Indian Overseas Bank

UIDAI Data Privacy and Security controls for Aadhar Holders

Version 1.0

-Public-

Contents

Table of Contents

1. Preamble 3
2. Purpose 3
3. Data Privacy and Security controls 3
   a) Definition 3
   b) Data Privacy of Beneficiary Aadhaar Holder Introduction 5
   c) Aadhaar Authentication Services: 4
   d) Data Privacy on Aadhaar and Biometric details: 5
   e) Human Resource 6
   f) Asset Management 6
   g) Access Control 7
   h) Password Policy 8
   i) Cryptography 9
   j) Physical and Environmental Security 10
   k) Operations Security 11
   l) Communications Security 13
   m) Information Security Incident Management 14
   n) Compliance 14
   o) Change Management 16
   p) Application Security 16
   q) Supplier Security 16
4. Roles and Responsibilities 17
5. Metrics – UIDAI Policy 17
6. Terms and definitions 17

UIDAI Data Privacy and Security controls for Aadhar Holders

1. Preamble

Security of UIDAI information assets handled by the external ecosystem partners for providing services, is of paramount importance. The confidentiality, integrity, and availability of these shall be always maintained by these partners by deploying security controls in line with the Aadhaar Act 2016, Aadhaar Authentication Application Security Standards. "*Indian Overseas Bank*" will be referred as Bank in the below document.

2. Purpose

This policy outlines the Information Security Policy and Information Security Controls applicable to the Bank acting as Authentication User Agency (AUA)/KYC User Agency (KUA). In addition to the bank's Information Security Policy and Cyber Security Policy, the UIDAI security policy outlines the additional security controls and specific measures to protect Aadhaar data collected, stored, and processed by the bank.

Bank shall ensure the security of UIDAI information assets handled by bank as listed below:

1. Providing AUAs/KUAs with an approach and directives for deploying security controls for allinformation assets used by them for providing services.
2. Establishing review mechanism to ensure that the AUAs/KUAs adhere to all provisions of the UIDAI Information Security Policy for AUAs/KUAs.

1. Data Privacy and Security controls

a) Definition

1. **Authentication User Agencies (AUA):** Authentication User Agency is an organisation or an entity using AADHAAR authentication as part of its applications to provide services to residents.
2. **KYC User Agencies (KUA)**: KYC User Agency is an organisation or an entity using AADHAAR authentication and eKYC services from UIDAI as part of its

applications to provide services to residents.

An AUA sends authentication requests to enable its services / business functions. An AUA connects to the CIDR through an ASA (either by becoming ASA on its own or contracting services of an existing ASA). AUA/KUA uses demographic data, and/or biometric data in addition to the resident's UID. They use Aadhaar authentication to provide services such as opening of bank account, LPG connection, etc. to residents. Since the AUAs handle sensitive resident information such as the Biometric information, Aadhaar number, eKYC data etc. of the residents, it becomes imperative to ensure its security.

b) Data Privacy of Beneficiary Aadhaar Holder Introduction:

1. The Unique Identification Authority of India has been established by the Government of India with the mandate to the Authority is to issue unique identification number (called Aadhaar ID or UID) to Indian residents that is robust enough to eliminate duplicate and fake identities and can be verified and authenticated using biometrics in an easy and cost-effective manner.
2. The UID has been envisioned as a means for residents to establish their identity easily and effectively, to any agency, anywhere in the country, without having to repeatedly produce identity documentation to agencies.
3. The UIDAI offers an authentication service that makes it possible for residents to authenticate their identity biometrically through presentation of their fingerprints/ iris authentication or non-biometrically using a One Time Password (OTP) sent to registered mobile phone or e- mail address.

c) Aadhaar Authentication Services:

1. Aadhaar Authentication is defined as the process wherein, Aadhaar number along with the Aadhaar holder's personal identity information is submitted to the Central Identities Data Repository (CIDR) for matching following which the CIDR verifies the correctness thereof based on the match with the Aadhaar holder's identity information available with it.

2. The purpose of Authentication is to enable Aadhaar – holders to prove identity and for service providers to confirm the resident's identity claim to supply services and give access to benefits. To protect resident's privacy, Aadhaar Authentication service responds only with a "Yes/No" and no Personal Identity Information (PII) is returned as part of the response.

3. e-KYC Service: UIDAI also uses the e-KYC service, which enables a resident having an Aadhaar number to share their demographic information (i.e., Name, Address, Date of Birth, Gender, Phone & E-mail) and Photograph with UIDAI partner organization (called a KYC User Agency –KUA) in an online, secure, auditable manner with the residents consent. The consent by the resident can be given via a Biometric authentication or One Time Password (OTP) authentication.

4. The Bank has entered into a formal agreement with UIDAI to access Aadhaar authentication services, and e-KYC services. To protect the Aadhaar Beneficiary, the data privacy policy of the Bank has been defined and formulated.

d) Data Privacy on Aadhaar and Biometric details:

1. The submission of Aadhaar details by a customer to the Bank is voluntary and the Bank shall not assist on a customer to produce their Aadhaar details for availing any of the services. In cases where Aadhaar number is offered voluntarily by the customer to the Bank, the Bank shall seek a declaration by the customer towards the same.

2. For cases where e-KYC verification is required, the Bank shall get an explicit consent from the resident for download of resident demographic details from UIDAI mentioning the purpose for which the details are sought.

3. The consent shall be either in the form of an authorization letter or a provision to electronically record the consent in a software application.

4. Biometric details shall also be captured by the Bank for the purposes of authentication, for example to authenticate a customer before permitting transaction through a Micro ATM / any other device, as an AEPS (Aadhaar Enabled Payment System) transaction.

5. The biometric details whenever captured by the Bank shall be used only for

data exchange with UIDAI which validates the captured biometric data against the biometric data maintained in CIDR (Central Identities Data Repository) against the specific Aadhaar number.

6. The Bank shall use STQC certified devices for demographic details received from UIDAI will be stored for future reference, the biometric details shall not be stored by the Bank in any manner and form.

7. A system log wherever required shall be maintained to extract the details in case of disputes. The logs should capture Aadhaar Number, timestamp etc., but will not capture/store the PID (Personal Identity Data) associated with the transaction.

8. As per Regulation 12A of the Aadhaar (Enrolment and Update) Regulations, 2016, all Scheduled Commercial Banks have been mandated to offer Aadhaar enrolment and updating services. The services will be offered at select branches identified by the Bank.

9. Aadhaar enrolment and updating entails the process of capturing the personal information of the customers along with their Biometric details. To protect data privacy, the enrolment application sought by the Bank from the customer to assist in internal data entry process shall be returned to the resident / will be destroyed internally.

10. The data so captured will be sent to UIDAI as a straight through process. The Bank shall not store the data captured (both biometric and personal information) in any manner and form.

e) Human Resource

1. Bank shall appoint a SPOC/team for all UIDAI related activities and communication with UIDAI.

2. An induction as well as periodic functional and information security trainings shall be conducted for all Bank personnel for UIDAI related services. The training shall include all relevant security guidelines per the UIDAI information security policy for Authentication, Aadhaar Act, 2016 and Aadhaar Regulations, 2016.

3. All employees accessing UIDAI information assets shall be made aware of UIDAI information security policy and controls.

f) Asset Management

1. All assets used by the ASA (servers, network devices, etc.) for the purpose of delivering services to UIDAI shall be identified, labelled and classified. Details of the information asset shall be recorded.

2. The assets which are scheduled to be disposed must have a procedure as part of the disposal policy of the Bank. Information systems containing UIDAI

information shall be disposed-off securely only after obtaining approvals from UIDAI authorized personnel.

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

4. ASA shall implement controls to prevent and detect any loss, damage, theft or compromise of the assets.

5. Authentication devices used to capture residents biometric should be STQC certified as specified by UIDAI.

g) Access Control

1. Only authorized individuals shall be provided access to information assets (such as servers, network devices etc.) processing UIDAI information.

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

    a) Have least privilege access for information access and processing;

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

3. The systems should have auto lock out feature i.e. after a certain time of inactivity (15 mins or as specified in the Bank's Policy), the system should log out; Implement an equipment locking mechanism for workstation, servers and/ or network device

4. Access rights and privileges to information assets for UIDAI information shall be revoked within 24 hours separation of respective personnel or as mentioned in the exit management policy of the 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 audit purposes;

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

7. Procedures shall be put in place for secure storage and management of administrative passwords for critical information systems.

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 Bank should 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 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 Bank.

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

11. If the application is operator assisted, the operator shall first authenticate himself before authenticating the residents.

h) 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. Avoid keeping a paper record of passwords, 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 encrypted form.

5. Change passwords whenever there is any indication of possible system or password compromise;

6. Complex passwords shall be selected with a minimum length of 8 characters, which are:

   a. Not based on anything somebody else could easily guess or obtain using person related information, e.g. names, telephone numbers, and dates of birth etc.;

   b. Free of consecutive identical characters or all-numeric or all-alphabetical groups;

   c. Password should contain at least one numeric, one uppercase letter and one special character;

d. Passwords shall be changed at regular intervals (passwords for privileged accounts shall be changed more frequently than normal passwords);

e. System should not allow the use of last 5 passwords.

f. System should not allow the username and password to be the same for a particular user.

g. Users must not use the same password for various UIDAI access needs;

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 function key;

10. Three successive login failures should result in a user's account being locked; they should not be able to login until their account is unlocked and the password reset. The user should contact the System Administrators for getting the account unlocked;

i) Cryptography

1. The Personal Identity data (PID) block comprising of the resident's demographic / biometric data shall be encrypted as per the latest API documents specified by the UIDAI at the end point device used for authentication (for e.g., PoT terminal)

2. The PID shall be encrypted during transit and flow within the AUA / KUA ecosystem and while sharing this information with ASAs.

3. Encrypted PID block and license keys that came as part of authentication packet should never be stored anywhere in its system

4. The authentication request shall be digitally signed by either by Bank or ASA as per the mutual agreement between them.

5. While establishing a secure channel to the AADHAAR Authentication Server (AAS the bank 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 nor expired.
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 all ASAs 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.
7. HSM shall be deployed in bank`s network to store the encryption keys for the Aadhaar vault and other Aadhaar related key management process. Access to HSM shall be restricted and periodic access reviews must be conducted for HSM. HSM shall be working in FIPS 140-2 operational mode for all encryption activities.

j) Physical and Environmental Security

1. The Bank servers involved in Aadhaar authentication mechanism should be placed in a secure lockable cage in the Data Centre.
2. The facility should be manned by security guards during and after office hours
3. CCTV surveillance shall cover the data centres where Aadhaar data is collected, processed, stored, and disposed.
4. Access to the premises should be limited to authorised personnel only and

appropriate logs for entry of personnel should be maintained.

5. The movement of all incoming and outgoing items shall be documented;
6. Preventive maintenance activities like audit of fire extinguishers, CCTV should be periodically done.
7. Physical access to restricted areas or offices and facilities hosting critical equipment shall be preapproved and recorded along with the date, time and purpose of entry.
8. Controls shall be designed and implemented to protect power and network cables from unauthorized interception or damage;

k) Operations Security

1. Bank shall complete the AADHAAR AUA / KUA 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; The Operating System as well as the network services used for communication with the PoT terminals shall be updated with the latest security patches
3. 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;
4. The Test and Production facilities / environments must be physically and/or logically separated.
5. ASA personnel shall conduct integrity checks to verify the completeness of the data packet and authenticity of the authentication user agency before processing the authentication request. A formal Patch Management Procedure shall be established for applying patches to the information systems. Patches should be updated at both application and server level.
6. Periodic VA exercise should be conducted for maintaining the security of

the authentication applications. Reports shall be generated and shared upon request with UIDAI.

7. AUA / KUA 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.
8. All hosts that connect to the AADHAAR Authentication Service or handle resident's identity information shall be secured using endpoint security solutions. At the minimum, anti-virus / malware detection software shall be installed on such hosts.
9. Network intrusion and prevention systems should be in place – e.g., IPS, IDS, WAF, etc.
10. AUAs / KUAs shall ensure that the event logs recording the critical user-activities, exceptions and security events shall be enabled and stored to assist in future investigations and access control monitoring.
11. 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.
12. 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 ofauthentication
    e) Record of the consent of Aadhaar number holder for the resident
    f) Details of the authentication transaction such as API Name, AUA / KUA Code, Sub- AUA, Transaction Id, Timestamp, Response Code, Response Timestamp, and any other non-id entity information.
13. Aadhaar number, PID information, device identity related data and eKYC

response data shall not be retained in the ASA logs.

14. No data pertaining to the resident or the transaction shall be stored within the terminal device.
15. The logs of authentication transactions shall be maintained by Bank for a period of 2 years, during which an Aadhaar number holder shall have the right to access such logs, in accordance with the procedure as may be specified.
16. Upon expiry of the period of 2 years, the logs shall be archived for a period of 5 years or the number of years as required by the laws or regulations governing the Bank, whichever is later, and upon expiry of the said period, the logs shall be deleted except those records required to be retained by court or for any pending disputes.
17. 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.
18. The Authentication server host shall reside in a segregated network segment that is isolated from the rest of the network of the organisation; The Bank`s server host shall be dedicated for the Online AADHAAR Authentication purposes and shall not be used for any other activities.
19. Service Continuity and service availability shall be ensured.

I) 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 biometric reader 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 using some 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 transaction along with UIDAI assigned institution code

for the bank 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 transaction processed.
5. The network between Bank and ASA shall be secured. Bank shall connect with ASAs through leased lines or similar secure private lines. If a public network is used, a secure channel such as SSL or VPN shall be used.
6. The Bank Authentication server shall be hosted behind a firewall. The firewall rules shall block incoming access requests to the Bank`s Authentication server from all sources other than AUAs / KUAs PoT terminals.
7. Wherever ATM/kiosk-based authentication is used, the systems shall be secured at the device and communication level.
8. 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.
9. 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.

m) Information Security Incident Management

1. Bank shall be responsible for reporting any security weaknesses, any incidents, possiblemisuse, or violation of any of the stipulated guidelines to UIDAI immediately.
2. Bank's Incident Management Policy shall be adhered in the event of an incident.

n) Compliance

1. Bank shall comply with all terms and conditions outlined in the UIDAI AUA / KUA agreement and AUA / KUA compliance checklist.
2. Bank shall ensure that its operations are audited by an information systems auditor certifiedby a recognized body on an annual basis and on a need

basis to ensure compliance withUIDAI standards and specifications. The audit report shall be shared with UIDAI upon request

3. 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.
4. Bank shall use only licensed software for UIDAI related infrastructure environment. Record of all software licenses shall be kept and updated regularly.
5. Bank and its partners shall ensure compliance to all the relevant laws, rules, and regulations, including, but not limited to, ISO27001:2013 Standard, Information Technology Act 2000 and 2008 amendments, Aadhaar Act, 2016 and Regulations.
6. It is recommended that AUA / KUA shall deploy as part of its systems, a Fraud Analytics module that is capable of analysing authentication related transactions to identify fraud.
7. Ensure that 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;
8. eKYC should be used as a facility using only biometric and OTP modalities by the AUAs
9. Bank shall use only licensed software within the UIDAI network environment. Record of all software licenses shall be kept and updated regularly;
10. Bank must have their authentication servers routing to CIDR hosted in Data Centres within India. Bank shall adhere to all the notifications, guidelines and circulars published by UIDAI. Compliance team of bank shall be responsible for the communication of the published information by UIDAI to all its personnel.
11. ASA shall be responsible to the Authority for all its authentication related operations, even in the event the ASA sub-contracts parts of its operations to

other entities, the responsibility shall remain with the ASA.

o) Change Management

1. Bank shall document all changes to UIDAI Information Processing facilities/ Infrastructure/processes.
2. Bank shall implement only those changes related to Aadhaar which are approved by UIDAI forexecution.
3. Change log/ register shall be maintained for all changes performed.

p) Application Security

1. All of the applications developed by AUA/KUA or authentication applications being used by AUA/KUA developed by third party vendor must adhere to Aadhaar Authentication Application Security Standard (AAASS). The standard applies to all entities that performAadhaar authentication and store, process or transmit Aadhaar number holder data.
2. Application shall be certified by STQC or CERT-In empanelled.
3. Source code review shall be conducted on the application and the report of the same shall be maintained.
4. Aadhaar Authentication Application Security Standard includes technical and operational requirements set by the Unique Identification Authority of India (UIDAI) to protect Aadhaar number holder data. The standard also provides developers with standard best practices and testing requirements to build a secure application by leveraging other standards and best practices such as PA-DSS, OWASP Top 10, OWASP MASC, SANS 25 etc. The standard is applicable to web-based applications, mobile applications and thick client applicationsleveraging Aadhaar authentication.
5. Prior to deployment of the application in the production environment, a requesting entityshall ensure that the application meets all the requirements of the AAASS satisfactorily.

q) Supplier Security

1. Adherence to the Bank's IT Outsourcing Policy the service providers shall adhere to the compliance requirements of UIDAI application security standards and Bank's UIDAI security policy.

2. Roles and Responsibilities

The roles and responsibilities as defined in the Information Security Policy applies to the Bank's UIDAI Security Policy.

3. Metrics – UIDAI Policy

1. List of applications in scope for Aadhaar services
2. VAPT reports
3. Source code review reports
4. Internal audit reports
5. Notifications, advisories, and circulars from UIDAI
6. Access Reviews
7. Configuration assessment records
8. Approved Network architecture diagram
9. Application architecture diagram

4. Terms and definitions

S.No	Terms	Definitions
1.	AAS	AADHAAR Authentication Server
2.	ATM	Automatic Teller Machine
3.	API	Application Program Interface
4.	AUA/ASA	Authentication User Agency/Authentication Service Agency
5.	CA	Certifying Authority
6.	PA-DSS	Payment Application Data Security Standard
7.	PCI-DSS	Payment Card Industry Data Security Standard
8.	OWASP	Open Web Application Security Project
9.	CCTV	Closed Circuit Television
10.	CIDR	Central Identities Data Repository
11.	CN	Common Name
12.	eKYC	Electronic Know your customer
13.	GRC	Governance Risk and Compliance
14.	Asset	An asset is anything that has value to the

		organization. Assets can be classified into the following 5 categories: Paper assets: (Legal documentation, manuals, policies & procedures, organizational documents etc.) Physical assets: (computer equipment, communications, utility equipment, buildings etc.) Software assets: (database information, applications, software code, development tools, operational software etc.) People assets: UIDAI human resources and stakeholders. 5. Service assets: (Logistics, building management systems, communications, utilities etc.)
15.	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 architecture, infrastructure, network details etc.
16.	IDS	Intrusion Detection System
17.	IPS	Intrusion Prevention System
18.	ISO 27001	International Organisation of Standardization
19.	IT	Information Technology
20.	KUA	Know your customer user agencies
21.	NDA	Non-Disclosure Agreement
22.	NTP	Network Time Protocol
23.	OTP	One Time Password
24.	PID	Personal Identity Data
25.	PII	Personally Identifiable Information
26.	SPOC	Single Point of Contact
27.	SSL	Secure Sockets Layer
28.	STQC	Standard Testing and Quality Control
29.	TSU	Technical Support Unit
30.	VA	Vulnerability Assessment
31.	VPN	Virtual Private Network
32.	WAF	Web Application Firewall