SATIN Creditcare Network Limited

Document Control

Document Name	Policy on Model Authentication Compliance
Document Reference No.	21
Version Number	1.2
Created by	Pravupada Pandit, Saurabh Mishra
Reviewed by	Vikas Umrao, Gaurav Gupta, Ashok Rawat
Approved by	Anil Kwatra, Dhiraj Jha
Effective From	01/04/2026

Revision History

Created Date	Ver	Description (First Release/Revision)	Created by	Reviewed by	Approved by	Board Approval
28/01/2026	1.2	Annual Policy Review	Pravupada, Saurabh	Vikas Umrao, Gaurav Gupta	Anil Kwatra, Vikas Wadhera	21/03/2026
18/12/2024	1.1	Annual Policy Review	Pravupada, Saurabh	Vikas Umrao	Anil Kwatra, Dhiraj Jha, Gaurav Gupta	12/03/2025
20/03/2024	1.0	Adoption/First Version	Ravi Anand	Vikas Umrao	Anil Kwatra, Dhiraj Jha	22/03/2024

Table of Contents

1. Abbreviation Table

For the purpose of this Policy, the following abbreviations shall have the meanings assigned to them below. Unless the context otherwise requires, these abbreviations shall be read consistently across this document.

Abbreviation	Description
ADV	Aadhaar Data Vault
API	Application Programming Interface
ASA	Authentication Service Agency
AUA	Authentication User Agency
BC	Business Correspondent
BGV	Background Verification
CERT-In	Indian Computer Emergency Response Team
CIDR	Central Identities Data Repository
CCTV	Closed-Circuit Television
e-KYC	Electronic Know Your Customer
FIPS	Federal Information Processing Standards
HSM	Hardware Security Module
IDS	Intrusion Detection System
IPS	Intrusion Prevention System
IT	Information Technology
KUA	e-KYC User Agency
NDA	Non-Disclosure Agreement
NTP	Network Time Protocol
OTP	One-Time Password
PID	Personal Identity Data
PoT	Point of Transaction
POS	Point of Sale
RCA	Root Cause Analysis
SCNL	Satin Creditcare Network Limited
SOP	Standard Operating Procedure
SPOC	Single Point of Contact
SSL	Secure Sockets Layer
STQC	Standardisation Testing and Quality Certification
UIDAI	Unique Identification Authority of India
UID Token	Unique Identification Token issued by UIDAI
UUID	Universally Unique Identifier
VA	Vulnerability Assessment
VID	Virtual ID
VPN	Virtual Private Network
WAF	Web Application Firewall
XML	Extensible Markup Language

and Services) Act, 2016 and includes any alternative virtual identity generated under sub-section (4) of that section.

Reference: Section 2(a) of the Aadhaar Act, 2016 and Section 3(i)(a) of the Aadhaar and Other Laws (Amendment) Act, 2019.

b) Aadhaar Data Vault (ADV)

"Aadhaar Data Vault" means a separate, secure database, vault, or system where Aadhaar numbers and any associated identity information are mandatorily stored, and which serves as the sole repository for such data.

Reference: UIDAI Circular No. 11020/205/2017 – UIDAI (Auth-I), dated 25 July 2017.

c) Anonymisation

"Anonymisation" means an irreversible process of transforming or converting personal data into a form in which an individual cannot be identified, directly or indirectly, and which meets the prescribed standards of irreversibility.

Reference: Section 3(2) of the Personal Data Protection Bill, 2019.

d) Authentication

"Authentication" means the process by which the Aadhaar number, along with demographic information, biometric information, or OTP of an individual, is submitted to the Central Identities Data Repository (CIDR) for verification, and such repository verifies the correctness or otherwise of such information based on its records.

Reference: Section 2(c) of the Aadhaar Act, 2016.

e) Authentication Service Agency (ASA)

"Authentication Service Agency" or "ASA" means an entity providing the necessary infrastructure and secure network connectivity to enable a requesting entity to perform Aadhaar authentication using the facilities provided by UIDAI.

Reference: Regulation 2(f) of the Aadhaar (Authentication) Regulations, 2016.

f) Authentication User Agency (AUA)

"Authentication User Agency" or "AUA" means a requesting entity that uses the Yes/No authentication facility provided by UIDAI.

Reference: Regulation 2(g) of the Aadhaar (Authentication) Regulations, 2016.

g) Authority

"Authority" means the Unique Identification Authority of India (UIDAI) established under sub-section (1) of Section 11 of the Aadhaar Act, 2016.

Reference: Section 2(e) of the Aadhaar Act, 2016.

h) Biometric Information

"Biometric information" means photograph, fingerprint, iris scan, or such other biological attributes of an individual as may be specified by regulations.

Reference: Section 2(g) of the Aadhaar Act, 2016.

q) Identity Information

"Identity information" in respect of an individual includes the Aadhaar number, biometric information, and demographic information.

Reference: Section 2(n) of the Aadhaar Act, 2016.

r) Limited KYC

"Limited KYC" means an Aadhaar-based service that does not return the Aadhaar number and provides only a UID Token and limited demographic information, as permitted to Local AUAs.

Reference: UIDAI Circular No. 1 of 2018, dated 10 January 2018.

s) PID Block

"PID Block" means the Personal Identity Data element comprising demographic information, biometric information, and/or OTP collected during Aadhaar authentication.

Reference: Regulation 2(n) of the Aadhaar (Authentication) Regulations, 2016.

t) Personal Data

"Personal data" means any data relating to a natural person who is directly or indirectly identifiable and includes any inference drawn for profiling purposes.

Reference: Section 3(28) of the Personal Data Protection Bill, 2019.

u) Personnel

"Personnel" means all employees, officers, directors, consultants, agents, and contractual staff engaged by the requesting entity.

Reference: Regulation 2(1)(f) of the Aadhaar (Data Security) Regulations, 2016.

v) Processing

"Processing" means any operation performed on personal data, including collection, recording, storage, use, disclosure, retrieval, restriction, erasure, or destruction.

Reference: Section 3(31) of the Personal Data Protection Bill, 2019.

w) Reference Key

"Reference Key" means an additional key mapped to an Aadhaar number stored within the Aadhaar Data Vault for secure referencing.

Reference: UIDAI Circular No. 11020/205/2017 – UIDAI (Auth-I), dated 25 July 2017.

x) Requesting Entity

"Requesting Entity" means an agency or person submitting Aadhaar number and related identity information to CIDR for authentication.

Reference: Section 2(u) of the Aadhaar Act, 2016.

y) Resident

"Resident" means an individual who has resided in India for a period of one hundred and eighty-two days or more during the twelve months immediately preceding the date of application for enrolment.

7.3. Training, Awareness and Access Lifecycle Management

SCNL shall ensure that comprehensive information security and Aadhaar compliance training is imparted to all relevant personnel at the time of induction and thereafter on a periodic basis. Such training shall cover the requirements of the Aadhaar Act, 2016, the Aadhaar Regulations, UIDAI information security policies, and all relevant circulars, advisories, and technical guidelines issued from time to time. In addition to general awareness programmes, specialised and role-based training shall be conducted for personnel involved in specific functions within the Aadhaar authentication ecosystem.

Training programmes shall be conducted at least on a half-yearly basis and additionally whenever there are material changes in the authentication ecosystem, regulatory requirements, or internal processes. Records of all training sessions shall be maintained for audit and compliance purposes.

Upon cessation of employment, transfer, or change of role of any personnel handling Aadhaar-related authentication data, all user credentials, system access rights, and associated privileges shall be revoked or deactivated within twenty-four hours. This requirement shall apply equally to employees, contractual staff, and third-party personnel and shall be periodically reviewed to ensure effectiveness.

8. Asset Management

SCNL shall maintain a comprehensive asset management framework for all information assets supporting Aadhaar authentication services. Given the sensitivity of Aadhaar-related information, all assets used for authentication including applications, systems, databases, networks, devices, and infrastructure shall be formally identified, labelled, classified, and protected throughout their lifecycle in accordance with applicable regulatory and security requirements.

8.1. Asset Identification, Ownership and Inventory Management

All information assets deployed for Aadhaar authentication purposes shall be clearly identified and recorded in a centrally maintained asset inventory. The inventory shall capture relevant details such as asset type, location, custodian, ownership, and classification and shall be updated on a regular basis or upon any material change.

Ownership and accountability for each authentication-related asset shall be clearly defined and documented to ensure appropriate control, maintenance, and oversight. Asset classification shall reflect the criticality and sensitivity of Aadhaar-related information processed or stored by the asset.

8.2. Asset Usage, Protection and Hardening Controls

SCNL shall implement appropriate technical and administrative controls to prevent unauthorised access, loss, damage, theft, or compromise of assets containing Aadhaar-related information. Aadhaar data, including identity information, shall not be transferred to or stored on personal devices or unauthorised electronic media or storage systems under any circumstances.

All devices and systems used for Aadhaar authentication, including point-of-sale devices, tablets, desktops, laptops, servers, and databases, shall be deployed only after completion of system hardening in accordance with approved baseline configurations. Where UIDAI has prescribed specific hardening or security standards, such requirements shall be strictly followed;

9.3. Privileged Access Controls and Operator Authentication

Administrative and privileged access to Aadhaar-related systems shall be strictly controlled and monitored. Procedures shall be established for the secure storage, handling, and management of administrative credentials for critical information systems. Where manual storage is unavoidable, credentials shall be secured in fire-resistant safes or approved password vaults, with access logs maintained and reviewed periodically.

Users shall not be granted local administrative rights on their systems as a default practice. In cases where administrative access is required for operational reasons, such access shall be time-bound, documented, and restricted from modifying local or system-level security configurations.

For assisted devices or applications where operators perform authentication-related functions on behalf of residents, robust operator authentication mechanisms shall be implemented. Such mechanisms may include password-based authentication, Aadhaar authentication, smart card–based authentication, or other secure authentication methods approved by SCNL, ensuring traceability and accountability of all operator actions.

10. Password Policy

SCNL shall implement a strong password management framework to protect access to Aadhaar authentication systems, applications, and information assets. Password controls shall form a foundational element of the Company's access security architecture and shall be enforced consistently across all Aadhaar-related environments.

10.1. Password Issuance, Confidentiality and Change Management

Initial passwords shall be issued through secure mechanisms and shall be mandatorily changed by users upon first login. All user credentials, including those of administrators and privileged users, shall be treated as confidential information and shall not be shared, displayed, transmitted, or otherwise disclosed in any form.

Passwords shall be changed immediately whenever there is any indication or suspicion of compromise, unauthorised disclosure, or system security breach. In addition, passwords shall be refreshed at defined intervals, with privileged and administrative accounts subject to more frequent change requirements than standard user accounts.

10.2. Password Complexity and Reuse Restrictions

Passwords used for accessing Aadhaar-related systems shall adhere to defined complexity standards to reduce the risk of guessing, brute-force, or credential-stuffing attacks. Such passwords shall have a minimum length of eight characters and shall not be based on easily identifiable personal information such as names, dates of birth, telephone numbers, or similar attributes.

Passwords shall be constructed to avoid predictable patterns, including consecutive identical characters or exclusively numeric or alphabetic sequences. Each password shall include a combination of uppercase and lowercase letters, numeric characters, and special characters. Reuse of the last five passwords shall be prohibited, and usernames shall not be used as passwords under any circumstances. Users shall also be restricted from using the same password across multiple UIDAI or Aadhaar-related access points.

11.3. Aadhaar Number Minimisation, Masking and Tokenisation

Where SCNL provides authentication services to Sub-AUAs, the client application used for Aadhaar authentication shall be developed, owned, and digitally signed by SCNL to ensure application integrity and regulatory accountability.

Aadhaar numbers shall be stored only within a secure Aadhaar Data Vault, where permitted, and the reference key used within the Aadhaar Data Vault shall be generated using a Universally Unique Identifier scheme to prevent guessing, correlation, or reverse engineering of Aadhaar numbers.

Display of full Aadhaar numbers shall be strictly restricted to the Aadhaar number holder or to authorised personnel with a demonstrable business requirement and appropriate approval. In all other cases, Aadhaar numbers shall be masked by default, with only the last four digits visible.

SCNL shall implement and progressively enhance the use of Virtual ID, UID Token, and Limited e-KYC mechanisms within its authentication systems to minimise direct handling of Aadhaar numbers and reduce the risk of data exposure. Integration of Virtual Tokens and UID Tokens into SCNL's services shall be undertaken in accordance with UIDAI specifications and applicable regulatory guidance.

12. Physical and Environmental Security

SCNL shall implement comprehensive physical and environmental security controls to protect Aadhaar-related infrastructure, information systems, and processing facilities against unauthorised access, damage, disruption, or loss. Such controls shall be commensurate with the criticality and sensitivity of Aadhaar-related information and shall align with UIDAI security requirements and industry best practices.

12.1. Data Centre Security and Access Management

All servers and infrastructure processing or storing Aadhaar-related information shall be housed within secure cabinets located in SCNL's designated Data Centres. Data Centres hosting Aadhaar-related systems shall be fully secured, access-controlled, and monitored at all times.

Physical access to Data Centres and other restricted areas shall be limited strictly to authorised personnel and shall be governed through pre-approval mechanisms. Entry and exit details, including the identity of the individual, date, time, and purpose of access, shall be recorded and retained for audit and regulatory review. Security personnel shall be deployed during and beyond office hours to ensure continuous monitoring and protection of critical infrastructure.

Closed-circuit television surveillance shall cover AUA and KUA servers and other critical Aadhaar-related infrastructure within the Data Centre. Signage clearly identifying restricted areas and entry requirements shall be prominently displayed at all relevant access points, particularly in areas where Aadhaar authentication servers are physically hosted.

12.2. Asset Protection, Movement Control and Environmental Safeguards

The movement of all incoming and outgoing assets associated with Aadhaar authentication within the Data Centre shall be formally documented and tracked. Lockable cabinets or safes shall be provided for secure storage of critical Aadhaar-related equipment, documents, and storage media.

13.3. Infrastructure Security, Patch Management and Monitoring

A formal patch management process shall be implemented to ensure timely application of security updates at both application and server levels. Periodic vulnerability assessments shall be conducted to identify and remediate weaknesses in Aadhaar-related infrastructure.

All systems and hosts connecting to Aadhaar authentication services or processing resident identity information shall be protected using endpoint security controls, including anti-virus and anti-malware solutions. Network security controls such as intrusion detection systems, intrusion prevention systems, and web application firewalls shall be deployed to safeguard Aadhaar infrastructure.

Event logging shall be enabled to capture critical user activities, system exceptions, and security events. Audit logs shall be monitored regularly, retained securely, and made accessible only to authorised personnel. All system clocks shall be synchronised using a centralised time source to ensure integrity of logs.

13.4. Data Handling, Logging and Aadhaar Data Vault Controls

SCNL shall comply fully with all consent-related requirements under the Aadhaar Act, 2016, Aadhaar Regulations, and UIDAI circulars. Aadhaar authentication transaction logs shall be maintained strictly in accordance with regulatory requirements and shall not contain Personal Identity Data.

Biometric data collected during Aadhaar authentication shall not be stored in client applications or terminal devices under any circumstances. No resident or transaction data shall be retained on endpoint devices after completion of authentication.

Where e-KYC data is received, such data shall be stored only in encrypted form and only after obtaining explicit consent from the resident. Sharing of e-KYC data with Sub-AUAs or other entities shall be undertaken only after obtaining specific approval from UIDAI and strictly in accordance with applicable regulations.

Where SCNL operates as a Global AUA or KUA, Aadhaar numbers and related data shall be stored only within a secure Aadhaar Data Vault located in a highly restricted and isolated network zone. All Aadhaar data stored in the Data Vault shall remain encrypted, and UIDAI-prescribed Data Vault guidelines shall be strictly followed.

13.5. Usage Restrictions, Session Controls and Hosting Requirements

Aadhaar numbers shall not be used as domain-specific identifiers within internal systems. Domain-specific identifiers shall be decoupled, revoked, or reissued as necessary to prevent correlation or misuse. Separate licence keys shall be generated for Sub-AUAs as prescribed by UIDAI, and SCNL's e-KYC licence key shall not be shared with any third party.

SCNL and its ecosystem partners shall ensure that Aadhaar-related identity information is not displayed, disclosed, or published to unauthorised persons or external agencies, nor mapped with unrelated datasets. Aadhaar authentication servers shall be hosted only in data centres located within India.

User sessions shall be terminated upon completion of authentication activity, and automated lock-out mechanisms shall be implemented for workstations, servers, and network devices to prevent unauthorised access due to inactivity.

15.1. Incident Identification and Regulatory Reporting

SCNL shall promptly identify, assess, and report any security weaknesses, suspected incidents, unauthorised access, misuse, or violation of Aadhaar-related security requirements. All reportable incidents shall be communicated to the Unique Identification Authority of India without delay and in the manner prescribed under applicable regulations.

Any confirmed or suspected confidentiality breach or security incident involving Aadhaar-related information shall be reported to UIDAI within twenty-four hours of detection, irrespective of whether the incident originates within SCNL's systems or within the ecosystem of its Sub-AUAs, Business Correspondents, or service providers.

15.2. Third-Party Incident Awareness and Accountability

SCNL shall ensure that all Sub-AUAs, Business Correspondents, and other third-party service providers involved in Aadhaar authentication are aware of, and comply with, prescribed Aadhaar incident reporting obligations. Contractual arrangements with such entities shall incorporate incident reporting requirements, escalation timelines, and cooperation obligations for investigation and remediation.

SCNL shall retain overall accountability for Aadhaar-related incident reporting and regulatory coordination, irrespective of whether the incident occurs within its own environment or that of an outsourced or partner entity.

15.3. Incident Investigation and Root Cause Analysis

For all material or significant Aadhaar-related security incidents, SCNL shall conduct a detailed Root Cause Analysis to identify underlying technical, procedural, or human factors contributing to the incident. Where incidents involve Sub-AUAs or third-party service providers, such entities shall be required to support the investigation and provide necessary information.

Based on the findings of the Root Cause Analysis, SCNL shall implement appropriate corrective and preventive actions to mitigate identified risks, strengthen controls, and reduce the likelihood of recurrence. Records of incidents, investigations, and remediation actions shall be maintained for audit and regulatory review.

16. Compliance

SCNL shall ensure continuous compliance with all applicable legal, regulatory, and contractual requirements governing Aadhaar authentication activities, supported by robust audit, oversight, and corrective action mechanisms.

16.1. Regulatory Compliance and Authorisations

SCNL shall comply at all times with the Aadhaar Act, 2016, the Aadhaar Regulations, 2016, the UIDAI agreement, and all circulars, advisories, technical specifications, and directions issued by UIDAI from time to time. Prior approval of UIDAI shall be obtained before appointment of any entity as a Sub-AUA, and necessary permissions shall be regularised for existing Sub-AUAs where applicable. All Aadhaar authentication applications deployed by SCNL and its Sub-AUAs shall clearly display the SCNL logo to ensure accountability and traceability in accordance with UIDAI requirements.

18. Policy Approval, Review, and Sign-Off Matrix

Author	Designation	Date	Signature
Pravupada Pandit	Sr. Associate - Operational Excellence & Customer Services	26/03/26	P.P. Pandit
Saurabh Mishra	Sr. Associate - Operational Excellence & Customer Services	26/03/26	

Reviewer	Designation	Date	Signature
Vikas Umrao	Lead - Operational Excellence & Customer Services	26/03/26	
Ashok Rawat	Chief Information Security Officer	30/03/26	
Gaurav Gupta	Head - Operational Excellence & Process Re-Engineering	30/03/26	

Approving Authority	Designation	Date	Signature
Anil Kwatra	Chief Business Officer	30.03.26	
Vikas Wadhera	Chief Risk Officer	30/03/26	

End***