Data Protection Policy for Aadhar

Version 1.0

Dated : May 20, 2025

May 2025

PROFESSIONAL DIGISIGN PRIVATE LIMITED
Registered Address: Office No-209,2nd Floor, Patil
Plaza, Nr. Sarasbaug, Mitra Mandal Chowk,
Swargate, Pune-411009.
Email: info@prodigisign.in

Pro DigiSign

Document Control

Document Title	PRODIGISIGN_CA_ Data protection Policy for aadhar_v1.0
Document Classification	Confidential - Internal
Document Version No.	1.0
Document Number	PRODIGISIGN/CA/IS/021
Document Owner	Operations Head / CA
Distribution list	Employees of PRODIGISIGN and relevant vendors only
Document Release Date	May 20, 2025
Document Approved Date	May 20, 2025
Document Approved By	Board of Directors / Operations Head

Notice of Distribution	This document is available to all employees of PROFESSIONAL DIGISIGN PRIVATE LIMITED. Any request to update this document must be authorised by the PRODIGISIGN Management.
Notice of Confidentiality	This document contains proprietary and confidential information of PROFESSIONAL DIGISIGN PRIVATE LIMITED. The recipient agrees to maintain this information in confidence and not reproduce or otherwise disclose this information to any person outside of the PRODIGISIGN CA directly responsible for the evaluation of its contents.

Document Revision Record

Version No	Description of Change	Section Number	Approved By	Approved Date	Issued / Revision Date
1.0	Initial Release	NA	Board of Directors	May 19, 2025	May 20, 2025

Table of Contents

1. INTRODUCTION

Prodigisign provides all types of Digital Signatures (DSC), including Class 2, Class 3, DGFT, and Document Signer certificates. Prodigisign is system-ready to operate as a Certifying Authority authorized to issue digital signatures. Given the sensitivity of Aadhaar data, this policy outlines the mandatory security standards regarding Data Protection for Aadhar Data of the organization and also third parties engaged with Prodigisign in Aadhaar-based services.

2. PURPOSE

To ensure the secure collection, storage, processing, and sharing of Aadhaar data in compliance with UIDAI guidelines, the Aadhaar Act, 2016, and the Digital Personal Data Protection Act, 2023.

3. SCOPE

This policy applies to all employees, vendors, and systems that handle Aadhaar-related data within the organization.
This policy and procedure apply to:

- Authentication User Agencies (AUAs)
- Know Your Customer User Agencies (KUAs)
- Service providers
- Technology vendors who interact with Aadhaar data for Prodigisign’s e-KYC and digital signature issuance services.
- All CA personnel including IT, compliance, and verification officers.
- Aadhaar-based eKYC and e-authentication workflows for digital certificate issuance.
- All systems storing Aadhaar information (raw, tokenized, encrypted, or masked).

The procedure is applicable to all personnel, systems, and locations within the organization handling Aadhaar data. It includes but is not limited to:
- Storage media (e.g., hard drives, USB devices, backup tapes)
- Cryptographic devices (e.g., HSMs, smart cards)
- IT equipment (e.g., laptops, desktops, servers)
- Printed records and paper-based documentation
- Any other equipment used in Aadhaar authentication or e-KYC processing

4. REGULATORY REFERENCES

- Aadhaar Act, 2016
- Aadhaar (Authentication) Regulations, 2016
- Aadhaar (Data Security) Regulations, 2016
- UIDAI Circular: Storage and Usage of Aadhaar Data
- UIDAI IT & Security Guidelines
- CCA Guidelines for e-KYC and e-Sign
- Digital Personal Data Protection Act, 2023
- Any circulars or directives issued by UIDAI

5. AADHAAR DATA IN CA CONTEXT

As per UIDAI and CCA norms, Aadhaar data in CA workflows may include

Data Element	Reference
Aadhaar Number (UID)	12-digit number collected during KYC
e-KYC XML or PDF	Downloaded via UIDAI's authentication API
Encrypted UID Tokens	Used for mapping repeat users
e-Sign Metadata	UIDAI-authenticated identity linked to e-sign actions
Logs of Authentication	As required under Aadhaar Authentication Regulations

6. DATA CLASSIFICATION

- Personally Identifiable Information (PII): Aadhaar number, biometric data, demographic details.
- Sensitive Personal Data: Biometric information, e-KYC data.

7. DATA STORAGE AND RETENTION

- Aadhaar data must be encrypted at source and stored securely in compliance with UIDAI encryption standards.
- No Aadhaar data shall be stored beyond the permitted retention period.
- Masked Aadhaar numbers (only last 4 digits visible) must be used in all reports and displays.

8. Data Privacy on Aadhaar and Biometric details:

The submission of Aadhaar details by customers shall be entirely voluntary. Under no circumstances shall the organization compel or coerce any individual to furnish their Aadhaar number as a condition for availing services. In instances where a customer voluntarily provides their Aadhaar number, the organization shall obtain a formal declaration from the individual affirming the voluntary nature of such submission.

For services requiring Aadhaar-based e-KYC authentication, the organization shall obtain explicit and informed consent from the resident prior to initiating any request for demographic data from UIDAI. The purpose for which the data is being requested shall be clearly communicated at the time of consent collection. Such consent shall be documented either through a signed authorization letter or via secure electronic means integrated within the organization's software systems.

Biometric data, where required, shall be captured solely for the purpose of authentication through UIDAI. The organization shall ensure that biometric information is used exclusively for real-time validation against the Central Identities Data Repository (CIDR) and shall not be stored in any form, either temporarily or permanently.

Only STQC-certified biometric devices shall be used for capturing biometric data. While demographic information received from UIDAI may be retained for legitimate business or regulatory purposes, the organization shall strictly prohibit the storage, replication, or reuse of biometric data in any manner.

9. Access Control

Access to information assets processing UIDAI data—including servers, workstations, and network devices—shall be strictly restricted to authorized personnel only. The organization shall implement robust access control mechanisms to ensure the confidentiality, integrity, and availability of Aadhaar-related information.

All employees with access to UIDAI information assets must adhere to the following operational and technical safeguards:

Session Termination: Operators shall log out of all systems and applications immediately upon completion of their session. Unattended sessions are strictly prohibited.

Workstation and Device Locking: All endpoints, including servers and network devices, must be equipped with automatic locking mechanisms. Applications shall enforce an inactivity timeout, logging out users after 15 minutes of inactivity or as defined in the organization’s access control policy.

Login Failure Lockout: Applications shall implement an automatic lockout after three consecutive failed login attempts, with a lockout duration of 30 minutes or as specified in the organization’s password policy.

Centralized Policy Enforcement: All local security configurations shall be aligned with and enforced through centralized solutions such as Active Directory or equivalent group policy management systems.

10. Cryptography

All Personal Identity Data (PID) blocks, comprising residents’ demographic and/or biometric information, shall be encrypted at the point of capture using the latest UIDAI-specified API protocols. Encryption must be enforced at the endpoint device used for authentication to ensure data confidentiality from the outset.

The encrypted PID shall remain protected during transmission across the Authentication User Agency (AUA) / e-KYC User Agency (KUA) ecosystem and while being shared with Authentication Service Agencies (ASAs). Under no circumstances shall the encrypted PID block be stored, except in cases of buffered authentication, where temporary storage is permitted for a maximum of 24 hours. Post this duration, the data must be securely and irreversibly deleted from all local systems.

All authentication requests shall be digitally signed either by the organization or the designated ASA, in accordance with the mutually agreed terms. When establishing a secure connection with the Aadhaar Authentication Server (AAS), the organization shall validate the following:

The digital certificate presented by the AAS is issued and signed by a trusted Certifying Authority (CA).

- The certificate is valid, not expired, and has not been revoked.
- The Common Name (CN) on the certificate matches the fully qualified domain name of the AAS (currently auth.uidai.gov.in).

Organization shall implement comprehensive key management practices to safeguard cryptographic keys throughout their lifecycle. These practices shall include:

- Secure key generation and distribution
- Encrypted key storage

- Designation of key custodians with dual control mechanisms
- Prevention of unauthorized key substitution
- Timely replacement of compromised or suspected keys
- Key revocation procedures
- Logging and auditing of all key management activities

To support these operations, a Hardware Security Module (HSM) shall be deployed within the organization’s network for secure storage of Aadhaar-related encryption keys, including those used in the Aadhaar Data Vault. The HSM must operate in FIPS 140-2 compliant mode, and access to it shall be strictly controlled. Periodic access reviews and audits shall be conducted to ensure continued compliance and operational integrity.

11. Operations Security

- Onboarding Compliance

The organization shall ensure completion of the Aadhaar AUA/KUA onboarding process in accordance with UIDAI guidelines prior to initiating any formal authentication operations.

- Standard operating Procedures

Comprehensive SOPs shall be documented and maintained for all information systems and services associated with UIDAI operations. These SOPs must define operational workflows, maintenance protocols, and contingency actions in the event of system failures. All operating systems and network services interfacing with PoT (Point of Transaction) terminals shall be updated with the latest security patches to mitigate vulnerabilities.

- Vulnerability Assessment

Periodic vulnerability assessments shall be conducted to evaluate the security posture of authentication applications. Detailed VA reports shall be generated and made available to UIDAI upon request, in accordance with audit and compliance requirements.

- Code Integrity and Malicious Activity Prevention

AUA/KUA personnel are strictly prohibited from authoring, compiling, or deploying any code that may compromise the performance, integrity, or accessibility of Personal Identity Data (PID) or related systems.

- Endpoint Security Controls

All systems interfacing with the Aadhaar Authentication Service or processing resident identity data shall be protected with industry-standard endpoint security solutions. At a minimum, anti-virus and anti-malware software must be installed and regularly updated.

- Network Security Infrastructure

Intrusion detection and prevention mechanisms—including but not limited to IDS, IPS, and Web Application Firewalls (WAF)—shall be deployed to monitor and defend against unauthorized access and network-based threats.

- Event Logging and Monitoring

AUAs/KUAs shall ensure that logging mechanisms are enabled to capture critical user activities, exceptions, and security events. These logs shall be retained in a secure manner to support forensic investigations and access control audits.

- Audit Trail Governance

Continuous monitoring of audit logs shall be performed to detect and respond to unauthorized activities. Access to audit trails and event logs shall be restricted to authorized personnel only, with access rights reviewed periodically.

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 the resident

f) Details of the authentication transaction such as API Name, AUA / KUA Code, SubAUA, Transaction Id, Timestamp, Response Code, Response Timestamp, and any other non-id entity information.

- Logs shall not, in any event, retain the PID, biometric and OTP information.
- Resident or transaction data shall not be stored on terminal devices. Authentication logs shall be retained for two years, during which residents may request access. Post this period, logs shall be archived for five years or as per applicable legal requirements, and then securely deleted unless subject to legal hold.
- All system clocks must be synchronized using a Network Time Protocol (NTP) server or managed centrally, with procedures in place to correct deviations.
- The Aadhaar Authentication Server shall be hosted in a segregated network segment, and the designated KVB server shall be exclusively used for Aadhaar authentication activities.

12. Compliance

Contractual and Compliance Obligations

The organization shall comply with all provisions outlined in the UIDAI AUA/KUA Agreement and its Compliance Checklist.

Audit Governance

Annual and ad-hoc audits shall be conducted by a certified Information Systems Auditor to assess conformity with UIDAI standards. Audit findings shall be shared with UIDAI upon request.

Non-Compliance Management

Any audit-identified non-conformity shall be addressed through root cause analysis, preventive action planning, implementation, and post-action review.

Software Controls

Only licensed software shall be deployed in UIDAI infrastructure. License inventory shall be regularly maintained.

Legal and Regulatory Conformance

Full compliance with applicable statutes and standards including ISO/IEC 27001:2013, IT Act (2000 & 2008), Aadhaar Act (2016), and UIDAI Regulations is mandatory for the organization and its partners.

Fraud Analytics

AUA/KUA shall deploy fraud detection capabilities to monitor authentication anomalies.

eKYC Usage

AUAs shall perform eKYC solely through biometric and OTP modalities.

Sub-AUA License Key Generation

Separate UIDAI-issued license keys shall be obtained by AUAs for each Sub-AUA.

Infrastructure Hosting

Authentication servers shall route through CIDR and be hosted within India-based Data Centres.

UIDAI Communication and Adherence

The organization shall implement all UIDAI-issued directives. KVB's Compliance Team shall ensure institutional communication and awareness.

13. VIOLATIONS AND PENALTIES

Non-compliance with this policy may result in:

- Internal actions: Disciplinary proceedings up to dismissal
- Regulatory actions: Fines or revocation of CA license by CCA
- UIDAI actions: Suspension or revocation of API access

14. POLICY REVIEW

This policy shall be reviewed:
- Annually, or
- Immediately following any relevant UIDAI circular, guideline, or regulatory update