

Codec Networks

Coding Threats. Decoding Solutions.

DIGITAL IDENTITY, TRUST & ESIGN

Prove Who Signed. Protect Who They Are.

Role-specific UIDAI assessments, eSign onboarding security, authentication and API testing, managed SOC and forensics for digital identity and trust services

Coding Threats. Decoding Solutions. · www.codecnetworks.com



What we will cover



The sector and its risks

Scale, players and the threats that matter most



What regulators now expect

Aadhaar Act, UIDAI audits and vaults, CCA eSign, RBI KYC, CERT-In and DPDP



How Codec Networks helps

Services, bundles and packages built for the sector



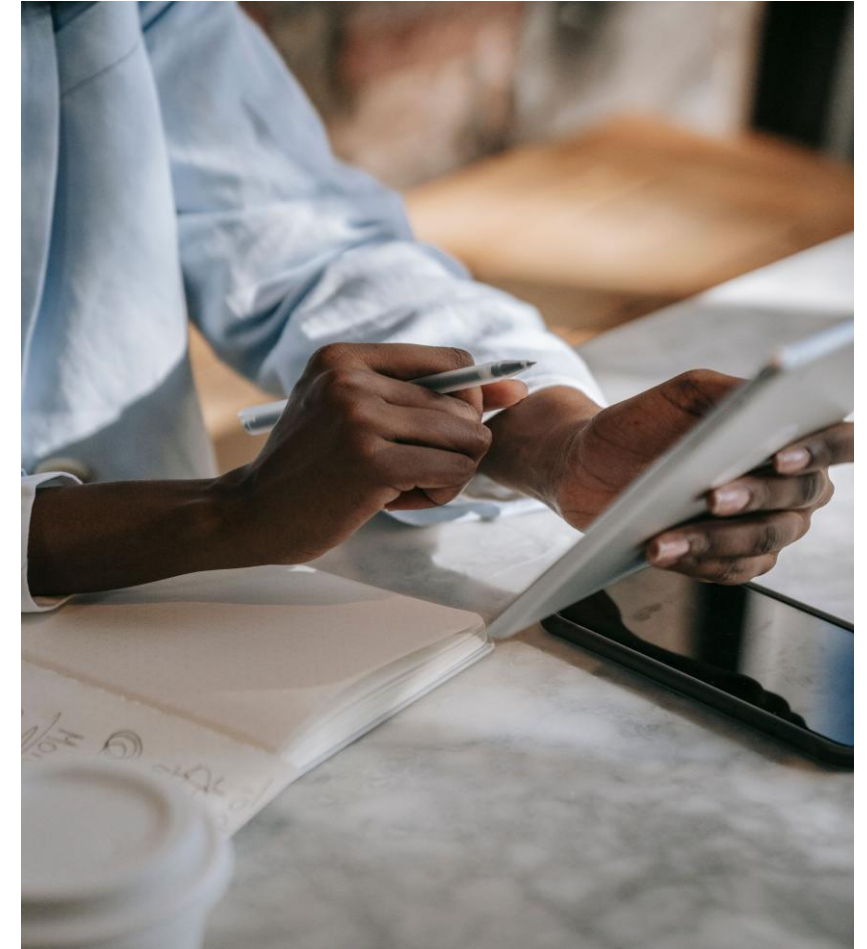
Proof in scenarios

Five new case studies and the controls that break the chain



Why Codec Networks and next steps

Our value add and how to start



Identity runs at national scale, and so does its attack surface

Official figures show the scale of what must be protected

134 crore

Live Aadhaar holders (PIB, 2026)

17,000 cr+

Aadhaar authentications
completed to date

47.19 crore

Aadhaar e-KYC transactions in
November 2025

6 hours

To report cyber incidents to
CERT-In

What this means: AUAs, KUAs, ASAs, enrolment agencies, certifying authorities, eSign providers and KYC platforms must stop cloned biometrics and deepfakes, keep Aadhaar numbers inside the vault, test every authentication and signing API, prove consent for every signature, pass UIDAI and CCA audits and report incidents within six hours.

Sources: PIB (MeitY) release of March 2026, UIDAI release on November 2025 transactions, CERT-In Directions (2022).

Who we serve across digital identity, trust and eSign



Aadhaar AUAs and KUAs

Banks, telecom, lenders, insurers



Authentication service agencies

Secure links to the CIDR



Enrolment agencies

Registrars, enrolment and update centres



Certifying authorities

Signature certificates and PKI



eSign service providers

Aadhaar e-KYC-based online signing



Application service providers

Apps and platforms integrating eSign



Video-KYC and IDV platforms

Onboarding, face match, liveness



DigiLocker issuers and requesters

Issued documents, verified sharing

The threats that cost identity and trust providers the most

Six priorities from our 18-threat digital identity and eSign assessment



Biometric spoofing and replay

Cloned prints, replayed captures



Deepfake video-KYC

Injected video, synthetic faces



Aadhaar data exposure

Numbers outside the vault



API and app abuse

Broken authorisation, scraping



Signing without consent

Swapped documents, OTP tricks



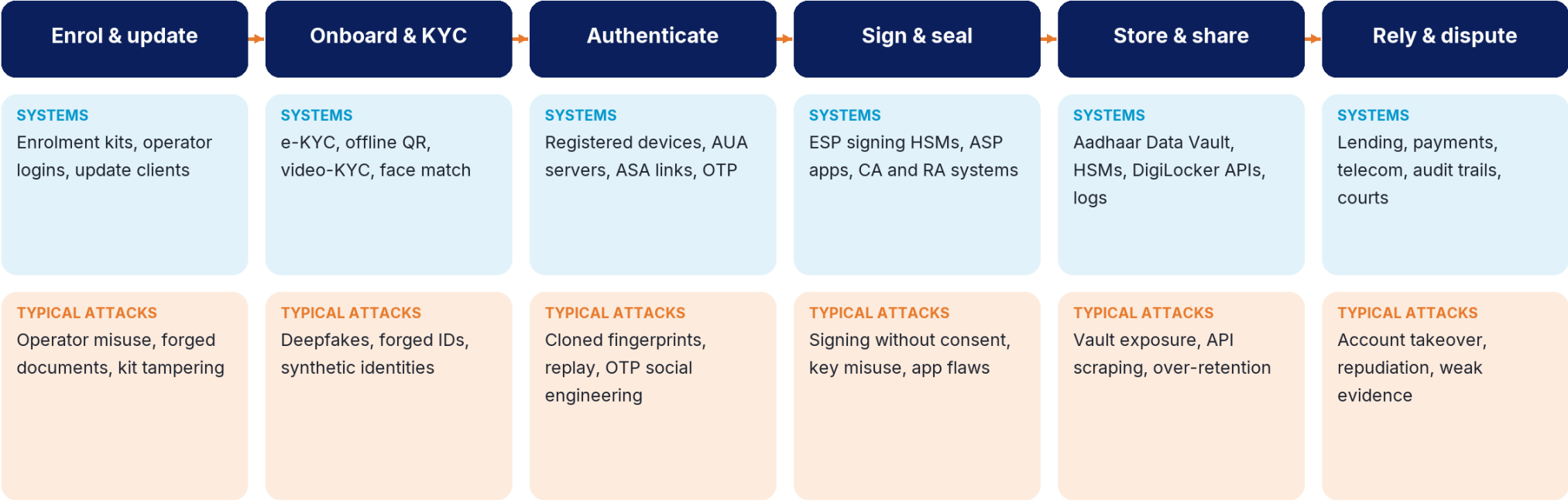
Key and CA compromise

HSMs, RA and admin access

Attacks target every step from enrolment to dispute

Where Cyber Risk Sits Across the Identity and Signing Lifecycle

Every step from enrolment to dispute carries its own attack surface



Identity and trust services sell a promise that a person is who they claim to be: one weak link makes every downstream account, signature and payment questionable.

Source: Codec Networks analysis

Codec Networks

What regulators now expect

Aadhaar Act, UIDAI audits and vaults, CCA eSign, RBI KYC, CERT-In and DPDP

The rules shaping digital identity and eSign security

Requirement	Frequency / deadline	Source
Annual IS audit	By a CERT-In empanelled auditor	Auth. Regulations 2021; UIDAI checklist
Aadhaar number storage	Only in an Aadhaar Data Vault; keys in HSMs	UIDAI Circular 14 of 2025
Core biometrics	Not stored; captured on registered devices	Aadhaar Act 2016; UIDAI specifications
Entity penalties	Civil penalty of up to ₹1 crore	Aadhaar Act, as amended in 2019
eSign service providers	Licensed CAs, empanelled after audit	IT Act Second Schedule; CCA
Video-KYC	Liveness, spoof detection, face matching	RBI KYC Directions, 2025
Cyber incident reporting	To CERT-In within 6 hours	CERT-In Directions, 2022
Synthetic content	Labelling; 3-hour takedown on orders	IT Rules amendment, 2026
Personal data	Safeguards and breach intimation	DPDP Act 2023; Rules 2025

Key dates on the regulatory timeline

Legal and Regulatory Timeline Shaping Digital Identity and eSign Security

Identity, signature, KYC and cyber instruments that reach Aadhaar ecosystem entities, certifying authorities, eSign providers and KYC platforms

● In force ● Upcoming (from Oct 2026)

2000	● IT Act, 2000 gives digital signatures legal force; the CCA becomes India's root of trust
2015	● Aadhaar e-KYC-based eSign added to the IT Act's Second Schedule; ESPs must be licensed CAs
Mar 2016	● Aadhaar Act, 2016 enacted, with consent, purpose limits and a bar on storing core biometrics
Feb 2017	● DigiLocker Rule 9A: documents issued into DigiLocker accepted at par with physical originals
Sep 2018	● Supreme Court upholds the Aadhaar Act but strikes down Section 57 on private-sector use
Jul 2019	● Aadhaar amendment adds offline verification and civil penalties of up to ₹1 crore on entities
Jan 2020	● RBI permits video-based customer identification (V-CIP) for onboarding under its KYC rules
Apr 2022	● CERT-In Directions: 6-hour incident reporting and 180-day ICT logs in India
Nov 2022	● UIDAI checklist V3.0: annual IS audits of requesting entities by CERT-In empanelled auditors
Jan 2025	● Good-governance amendment rules let approved private entities use Aadhaar authentication
Nov 2025	● UIDAI Circular 14 revises Aadhaar Data Vault and HSM hosting; DPDP Rules notified
Feb 2026	● IT Rules amended: labelling of synthetic content and 3-hour takedowns on official orders
Mar 2026	● Maximum publicly trusted TLS certificate validity cut to 200 days under CA/B Forum rules
May 2027	● Most DPDP Rules obligations, incl. security safeguards and breach intimation, apply

Sources: UIDAI, MeitY, CCA, RBI, CERT-In, Supreme Court of India, CA/Browser Forum, Gazette of India. Confirm against the official instruments.

Codec Networks

How Codec Networks helps

UIDAI audits · eSign security · Auth & API testing · Vaults & HSMs · KYC fraud & SOC · Forensics

One partner from enrolment to signature



UIDAI Role Audits

AUA, KUA, ASA, sub-AUA



eSign Onboarding Security

ASP, ESP and CA reviews



Auth & API Testing

Apps, APIs, SDKs, devices



Vaults, HSMs & Keys

ADV, keys, cloud hosting



KYC Fraud & 24/7 SOC

Liveness, anomalies, alerts



Privacy & Forensics

Consent, DPDP, investigations

Eleven bundles from the Codec Networks catalogue

Business-ready bundles instead of 180 separate services



Bundle numbers follow the Codec Networks Bundled Service Models. Scope, frequency and pricing are confirmed during scoping.

Three packages, sized to where you are

Foundation

Sub-AUAs, ASPs and KYC start-ups

- UIDAI checklist gap review (B4)
- ASP and e-KYC API test (B2, B1)
- Aadhaar data discovery (B6)
- Consent quick check (B6)

Assurance

AUAs, KUAs, lenders and IDV platforms

- Annual UIDAI IS audit (B4, B5)
- Vault, HSM and cloud review (B3)
- Video-KYC deepfake testing (B2, B11)
- 24x7 managed SOC (B7)

Continuous Resilience

ASAs, CAs, ESPs and large AUAs

- CCA and UIDAI audit readiness (B4)
- Signing, RA and key review (B3, B1)
- Red team and fraud scenarios (B1, B10)
- Crisis exercises and IR retainer (B10, B8)

Every obligation mapped to a bundle

Requirement	How Codec Networks helps	Bundle
Annual IS audit by a CERT-In empanelled auditor (UIDAI checklist)	Role-specific UIDAI audit	B4, B5
Aadhaar numbers only in a vault, keys in HSMs (UIDAI Circular 14)	Vault and HSM review	B3, B6
eSign by licensed CAs as ESPs; ASP terms (IT Act, CCA)	ESP, CA and ASP security reviews	B4, B1
Live V-CIP with liveness and face matching (RBI KYC Directions)	Video-KYC fraud testing	B2, B11
Incidents to CERT-In in six hours; 180-day logs (CERT-In)	SOC, IR retainer, reporting support	B7, B8
Informed consent and purpose limits for authentication (Aadhaar Act)	Consent flow and privacy review	B6
Safeguards and breach intimation for personal data (DPDP Act)	DPDPA programme	B6

Five new case studies, five broken chains

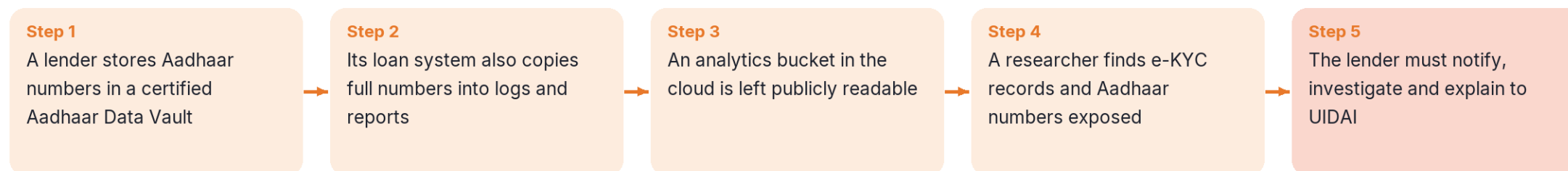
Illustrative composite scenarios written for 2026—not client engagements

1	The Fingerprints That Were Never There	Silicone copies of fingerprints beat older agent devices; liveness and anomaly monitoring stop it	B1 · B7 · B8
2	The Vault That Had a Back Door	Aadhaar numbers leak from logs and a public cloud bucket; masking and data discovery prevent it	B3 · B6 · B4
3	The Applicant Who Was a Video Feed	Deepfakes injected into video-KYC open mule accounts; injection detection and audits catch them	B2 · B11 · B7
4	The Document That Changed After Consent	An ASP app swaps documents after OTP consent; hash binding and ASP testing prevent it	B1 · B2 · B4
5	The Certifying Authority's Long Weekend	A phished RA officer approves rogue certificates; MFA, dual control and monitoring stop it	B3 · B7 · B8

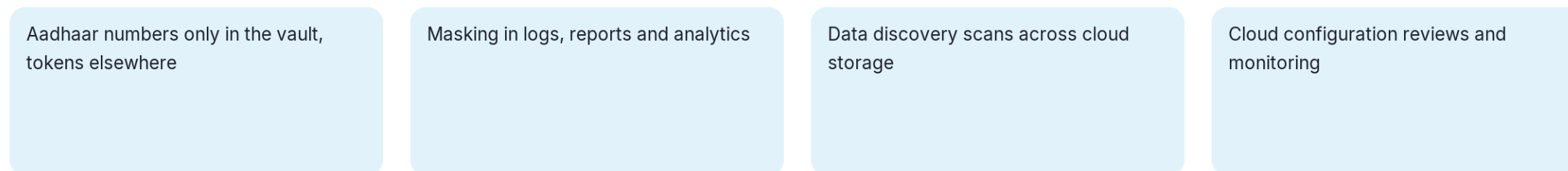
Example: closing a vault's back door

Case 2: The Vault That Had a Back Door

ILLUSTRATIVE ATTACK PATH



WHERE CONTROLS BREAK THE CHAIN



Illustrative composite scenario prepared by Codec Networks. Not a client engagement.

Codec Networks

What we test: where full Aadhaar numbers and e-KYC data actually sit across applications, logs, reports, backups and cloud storage, whether every system outside the vault uses reference keys or tokens, how vault keys are protected in the HSM, whether cloud storage is private and monitored, and how the lender would investigate, notify and report an exposure to CERT-In, UIDAI and affected customers.

Why identity and trust providers choose Codec Networks



CERT-In empanelled

For information security auditing services; NISCI empanelled for application audits



Certified

ISO 9001:2015, ISO/IEC 27001:2022, ISO/IEC 20000-1:2018



Regulation-mapped

Mapped to the Aadhaar Act and Regulations, UIDAI checklists and Circular 14, CCA eSign guidelines, RBI KYC Directions, CERT-In and DPDP



Tests the whole chain

Technical, process and monitoring tests together



Full stack, one partner

VAPT, audits, SOC, forensics, privacy and Board advisory connected



Specialist experts

CEH, OSCP, CPENT, CISA, ISO 27001 LA/LI, CHFI; OWASP, MITRE ATT&CK, NIST



How we deliver, and what you receive

Codec Networks Delivery Methodology

Nine stages, from scoping to continuous improvement



Source: Codec Networks project and service delivery methodology

Codec Networks

- Executive summary for the Board or its committee
- Technical findings with evidence and CVSS ratings
- Compliance gap matrix mapped to your obligations
- Prioritised remediation roadmap and retest reports
- Audit evidence tracker for regulators and partners
- SOC dashboards with MTDD and MTTR metrics

Let's start with a scoping session

1 Scoping session

Authentication servers and ASA links, registered devices, e-KYC and eSign integrations, Aadhaar Data Vaults and HSMS, video-KYC systems, APIs and SDKs, CA and RA systems, partners and sub-AUAs

2 Proposal

Regulation-mapped scope, methodology, timeline and deliverables

3 Kick-off

Testing, audit or SOC onboarding, with Board-ready reporting

 New Delhi: 507, 5th Floor, New Delhi House, Barakhamba Road, Connaught Place – 110001

 Gurugram: 707, 7th Floor, Silverton Tower, Golf Course Extension Road, Sector 50 – 122018

 011 430 496 96 · 011 437 522 99 · +91 99716 76124 · +91 88007 88220 · +91 88003 31124

 mktg@codecnetworks.com · www.codecnetworks.com

Regulatory references reflect public instruments as of October 2026; applicability depends on each entity's licence, category and activities.