

Codec Networks

Coding Threats. Decoding Solutions.



INDUSTRY BROCHURE · 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 Aadhaar ecosystem entities, certifying authorities and eSign providers, video-KYC and identity verification platforms and DigiLocker-integrated organisations.

UIDAI Role Audits

eSign Onboarding

Auth & API Testing

Vaults & HSMs

KYC Fraud & SOC

Privacy & Forensics

THE CHALLENGE

In identity, a cyber incident is fraud in someone's name.

Aadhaar has passed 17,000 crore authentications and DigiLocker 72 crore users, and approved private entities can now use Aadhaar authentication. Every AUA, KUA, ESP and KYC platform faces cloned biometrics, deepfakes and API abuse, while UIDAI, CCA and CERT-In expect audited proof of control.

What keeps leadership teams awake

- Cloned fingerprints and biometric replay
- Deepfakes injected into video-KYC
- Aadhaar numbers stored outside the vault
- API flaws exposing identity and KYC data
- Documents signed without real consent
- UIDAI, CCA and CERT-In audit findings



17,000 cr+

Aadhaar authentications to date (PIB, 2026)

231 crore

Aadhaar authentications in November 2025 alone

72.43 crore

DigiLocker users (Rajya Sabha, Aug 2026)

6 hours

To report cyber incidents to CERT-In

The rulebook has changed

Instrument	What it means for you
Aadhaar Act and Authentication Regulations (2016, 2021)	Consent and purpose limits; no storage of core biometrics; annual IS audits under UIDAI's compliance checklists
UIDAI Circular 14 of 2025 (2025)	Aadhaar numbers and e-KYC data only in an Aadhaar Data Vault; keys in HSMS; approved hosting
IT Act Second Schedule and CCA eSign (2015)	Aadhaar e-KYC-based eSign by licensed CAs acting as ESPs; CCA guidelines, audits and API specifications
CERT-In Directions and RBI KYC Directions (2022, 2025)	6-hour incident reporting, 180-day logs; video-KYC with liveness and face matching

One partner from enrolment to signature

Built around our primary proposition for the sector: **role-specific UIDAI assessments, eSign onboarding security and authentication and API testing.**

UIDAI Role Audits

- AUA, KUA, sub-AUA and ASA audits
- UIDAI compliance checklist evidence
- Registrar and enrolment agency reviews
- Remediation and closure tracking

eSign Onboarding Security

- ASP application security assessments
- ESP and CA control reviews
- Consent and document-binding tests
- CCA audit readiness support

Authentication & API Testing

- Authentication and e-KYC API testing
- Mobile app and SDK security
- Registered device integration checks
- DigiLocker issuer and requester APIs

Vaults, HSMs & Keys

- Aadhaar Data Vault architecture review
- HSM, key and token management
- Cloud hosting and access reviews
- Data discovery for stray Aadhaar data

KYC Fraud & 24/7 SOC

- Video-KYC deepfake and injection tests
- Authentication anomaly monitoring
- Mule and account takeover detection
- 6-hour CERT-In reporting support

Privacy & Forensics

- Aadhaar consent and DPDP programmes
- Identity fraud investigations
- Breach response and evidence handling
- Root cause and regulator reporting

Who we serve: Aadhaar AUAs, KUAs, sub-AUAs and ASAs · registrars and enrolment agencies · certifying authorities and eSign service providers · application service providers integrating eSign · video-KYC and identity verification platforms · DigiLocker issuers and requesters.

Packaged for how identity and trust providers buy

Eleven Codec Networks bundles apply directly to Aadhaar ecosystem entities, certifying authorities, eSign providers and identity verification platforms:

B1

Cyber Assessment & VAPT Assurance

B2

Application, API & DevSecOps Security

B3

Cloud, Infrastructure & Zero Trust

B4

Regulatory Cyber Audit & Compliance

B5

GRC, ISO, SOC 2 & PCI DSS Maturity

B6

Data Privacy & DPDPA Program

B7

Managed SOC, MDR & Threat Monitoring

B8

Forensics, Incident Response & Malware RCA

B9

Third-Party & Supply-Chain Risk

B10

Cyber Simulation, Awareness & Tabletop

B11

Emerging Tech, AI & Web3 Security

Foundation

Sub-AUAs, ASPs and KYC start-ups

- UIDAI checklist gap review
- ASP and e-KYC API security test
- Aadhaar data discovery scan
- Consent and privacy quick check

Assurance

AUAs, KUAs, lenders and IDV platforms

- Annual UIDAI IS audit
- Vault, HSM and cloud review
- Video-KYC deepfake testing
- 24x7 managed SOC

Continuous Resilience

ASAs, CAs, ESPs and large AUAs

- CCA and UIDAI audit readiness
- Signing, RA and key control review
- Red team and fraud scenario tests
- Crisis exercises and IR retainer

Mapped to your obligations

Requirement	How we help	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

Why identity and trust providers choose Codec Networks

CERT-In empanelled

Eligible for the IS audits UIDAI's checklist calls for.

Identity-aware testing

Authentication, e-KYC, eSign and video-KYC flows tested end to end.

Role-specific audits

AUA, KUA, sub-AUA, ASA and enrolment checklists applied by role.

Certified and accountable

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

Full stack, one partner

Audit, testing, SOC and forensics connected from finding to closure.

Certified experts

CISA, ISO 27001 LA/LI, CEH, OSCP and CHFI professionals.

How we engage

Discover & scope

Authentication servers and ASA links, registered devices, e-KYC and eSign integrations, Aadhaar Data Vaults and HSMS, video-KYC and face-match systems, APIs and SDKs, CA and RA systems, partners and sub-AUAs, and the UIDAI, CCA, RBI and CERT-In obligations that apply to you.

Assess & test

Threat-led testing and regulatory audits executed by certified specialists.

Report in business terms

Findings, risk ratings and a compliance gap matrix for the Board and regulators.

Remediate

Practical, prioritised fixes with technology and compliance teams.

Validate & prove

Retesting and an evidence tracker for auditors, regulators and partners.

Monitor & improve

Managed SOC, recurring testing and quarterly governance reviews.

What you receive: executive summary for the Board or its committee · technical findings with evidence and CVSS ratings · compliance gap matrix · prioritised remediation roadmap · retest reports · audit evidence tracker · SOC dashboards and MTTD/MTTR metrics.



START WITH A SCOPING SESSION

Let's make your next UIDAI audit, eSign go-live and KYC review a non-event.

Tell us your role in the ecosystem, your integrations, your partners and your obligations. We will propose a practical assurance, testing and monitoring plan.

New Delhi

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

Gurugram

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

Call

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

Write

mktg@codecnetworks.com
www.codecnetworks.com

Codec Networks

Coding Threats. Decoding Solutions.

Secure Today. Innovate Tomorrow. Regulatory references reflect public instruments as of October 2026; applicability depends on each entity's licence, category and activities. Packages are proposed groupings of Codec Networks bundles, finalised through scoping. Services support risk reduction and assurance and do not guarantee prevention of all incidents or regulatory compliance. Sources: PIB (MeitY) release of March 2026, UIDAI release on November 2025 transactions, Rajya Sabha reply of August 2026, CERT-In Directions (2022). Confirm obligations against the official instruments.