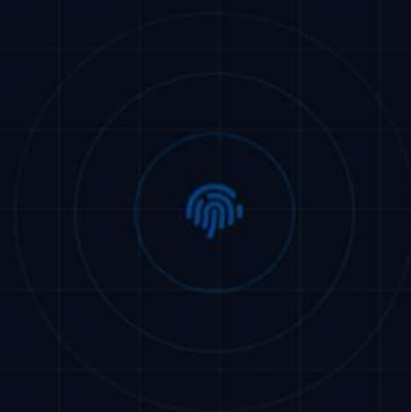

The Identity Infrastructure Imperative

Why fragmented security systems are failing enterprises and nations — and how unified biometric platforms are rewriting the rules of identity verification.



Inside This Report

01	Executive Summary	Key findings
02	The Fragmentation Problem	System failures
03	Threat Landscape	Aviation, defence, national ID
04	Unified Platform Architecture	Integrated approach
05	Technology Deep Dive	Biometric, AI, Edge
06	Deployment Scenarios	Airports, defence, enterprise
07	Ecosystem & Differentiators	Certifications, R&D
08	Case Study: Airport Transformation	Before & after
09	Future of Identity Infrastructure	Contactless, autonomous



Methodology

Findings derived from 40+ enterprise deployments, government procurement data, and third-party audit reports (2022–2025).

Executive Summary

The global identity verification market is undergoing a structural shift. Legacy systems — built for single-modality, single-site deployments — are structurally incapable of meeting the scale, speed, and security demands of modern infrastructure.



FRAGMENTATION

73%

of enterprises operate three or more disconnected identity systems with redundant data stores.



DELAY

4.2 min

average manual identity verification at critical checkpoints.



UNIFIED SPEED

<3 sec

end-to-end verification with integrated biometric platforms — 98% reduction.



MARKET

\$82B

projected biometric market by 2027.

→ Core Thesis

Organizations that consolidate onto a single multi-modal platform reduce security incidents by 60%, cut costs by 45%, and achieve compliance readiness 3x faster.

Fragmented Systems Create Compounding Risk

Most large-scale identity deployments were not designed — they were accumulated.
Organisations layered attendance systems without a unifying architecture



Access Control

Separate credential database,
no biometric cross-reference



CCTV Surveillance

Siloed recording, no real-time
identity correlation



Visitor Management

Paper-based or isolated digital
system



Biometric Capture

Proprietary format, no
interoperability



Manual Verification

Human-dependent, no
standardised audit



Identity Database

Fragmented records across
departments

THE COST

What Fragmentation Actually Costs

Security blind spots

High

No single view of identity events

Operational redundancy

High

Duplicate onboarding, multiple vendors

Compliance exposure

Critical

Inconsistent audit trails fail scrutiny

Scalability ceiling

Medium

Each new site needs full replication

3.7x

higher incident rate with fragmented systems

\$2.4M

annual cost of parallel identity infrastructures

"Every disconnected identity system is an unmonitored attack surface. Fragmentation is a structural vulnerability."

— Infrastructure Security Audit, 2024

Rising Threats Across Critical Sectors

Physical and digital threat convergence has exposed siloed security limitations.



Aviation

Surging volumes. Manual checks create bottlenecks.

- ▲ Document fraud up 34%
- ▲ Boarding delay: 8 min
- ▲ Zero watchlist automation



Defence

Perimeter breaches demand zero-trust at every layer.

- ▲ Credential cloning rising
- ▲ Clearance gaps
- ▲ Air-gapped systems at risk



National ID

1.4B enrolled globally. Privacy vs scale tension.

- ▲ Spoofing sophistication
- ▲ Connectivity limits
- ▲ Data sovereignty

Common Thread

All three sectors share the same failure mode: point solutions deployed in isolation, never architected for interoperability. The fix is structural.

Threat Evolution (2020–2025)

IDENTITY FRAUD INCIDENTS (THOUSANDS)



SPOOF ATTACK VECTORS (2024)



AVIATION BOTTLENECK

47%

of airports cite identity verification as primary passenger bottleneck

172%

deeptake fraud increase

\$9.2B

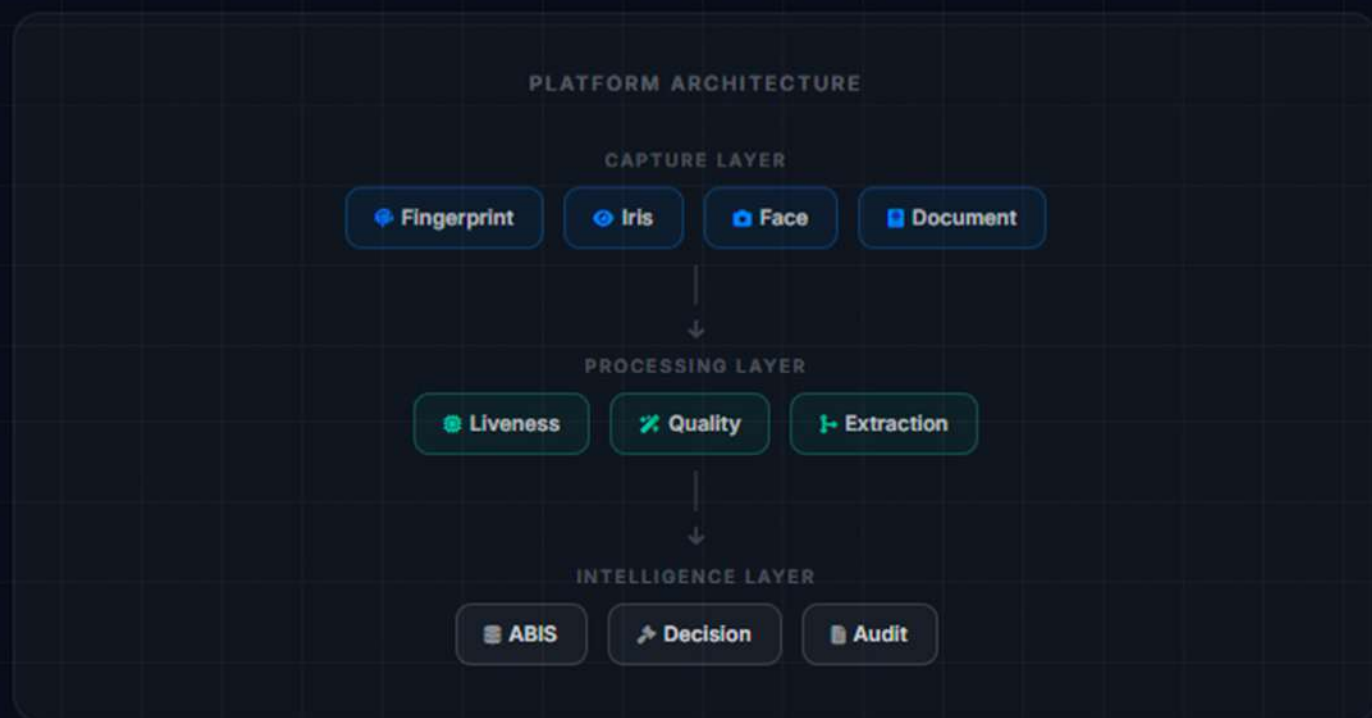
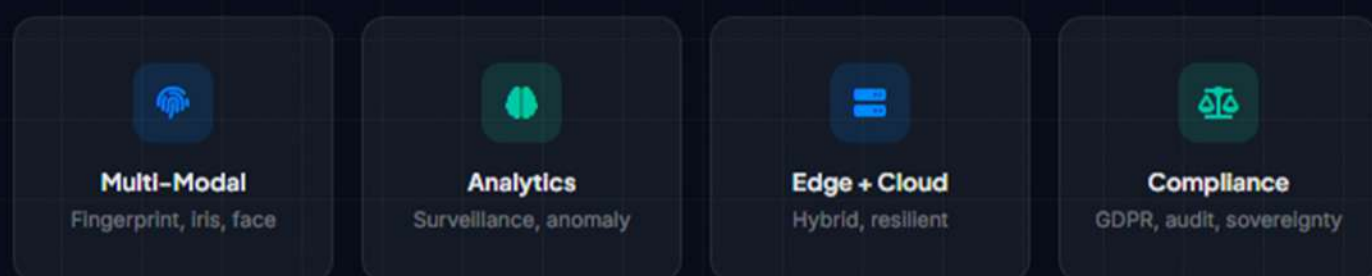
global verification failure cost

VERIFICATION RELIABILITY



A Unified Identity Platform

Not another point product — an integrated platform converging biometric capture, identity matching, surveillance analytics, and audit reporting into a single scalable architecture.



Architecture That Scales

Horizontal Scalability

Every component scales independently.
Microservices with containerised deployment.

Modal Independence with Fusion

Each modality operates independently. Fusion layer combines scores for multi-modal verification.

Edge-First Processing

Feature extraction on-device. Only encrypted templates traverse the network.

Zero-Trust Identity Chain

Every event cryptographically signed. Immutable and auditable end-to-end.

Compliance as Code

Regulatory requirements codified as policy rules, not manual processes.

Vendor-Agnostic Integration

REST/gRPC APIs, ANSI/NIST formats. Any compliant sensor, any downstream system.

Biometric Modalities



Fingerprint

Optical | Capacitive | Ultrasonic

FMR <0.001%

Speed <0.5s

Template ~500B

ANSI/NIST 378/400 compliant.



Iris

Near-Infrared | Active IR

FMR <0.0001%

Speed <0.8s

Template ~2KB

Highest entropy. ISO 19794-6.



Face

2D | 3D | NIR | Visible

FMR <0.002%

Speed <0.3s

Template ~1KB

512-d embedding.

Multi-Modal Fusion

Score-level fusion reduces FMR by 10x vs. best single modality.

Template Security

Irreversible. AES-256 at rest and in transit. Key rotation.

Liveness Detection

A biometric system is only as secure as its ability to distinguish a living subject from a presentation attack — defeating 3D masks, deepfakes, and synthetic fingerprints within sub-second latency.

DETECTION METHODS



Active Liveness

Challenge-response with randomized actions.
Defeats static attacks, adds ~1.5s latency.



Passive Liveness

Biophysical signals — micro-texture, rPPG, depth mapping. Zero friction.



3D Structured Light

IR dot pattern creates depth map. Hardware-assisted, highest reliability.

CERTIFIED PERFORMANCE

IBETA LEVEL 2 — PAD

100%

attack interception rate

<300ms

passive inference

0.01%

BPCER

Certifications

iBeta PAD L2

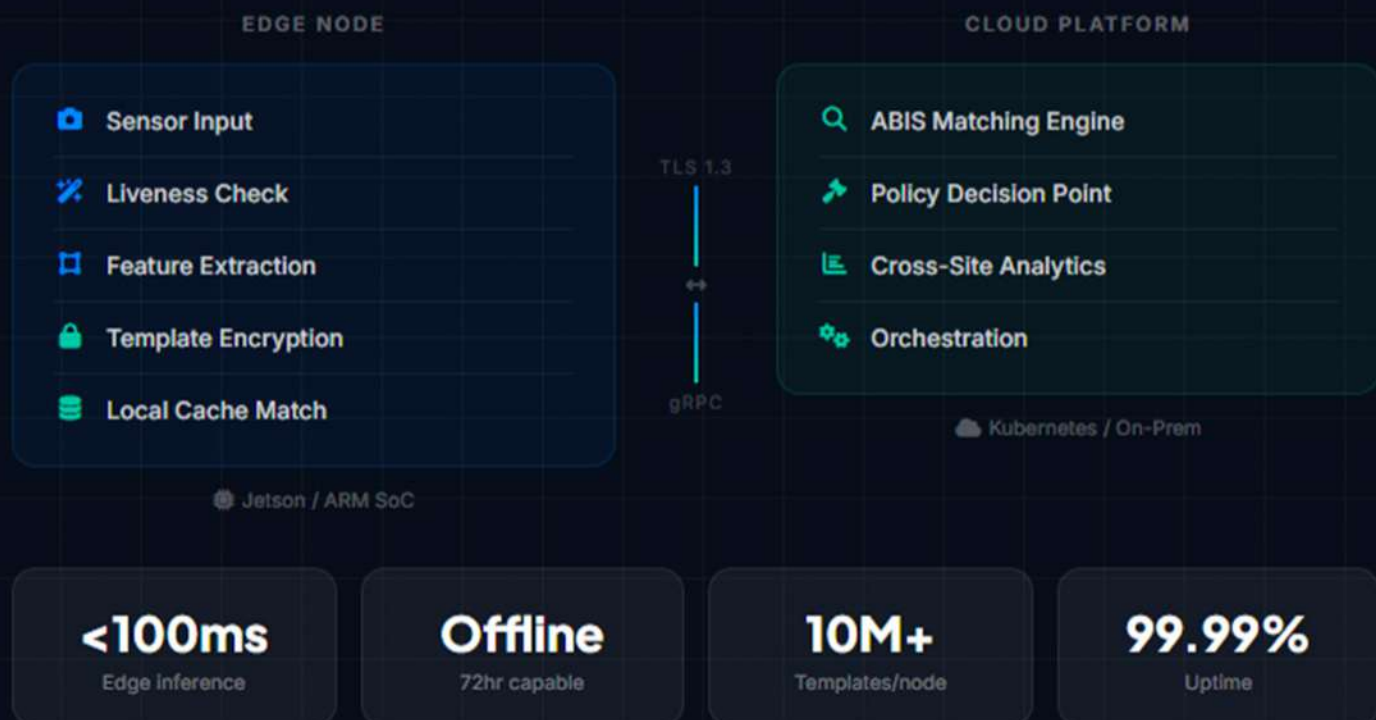
ISO 30107-3

STQC

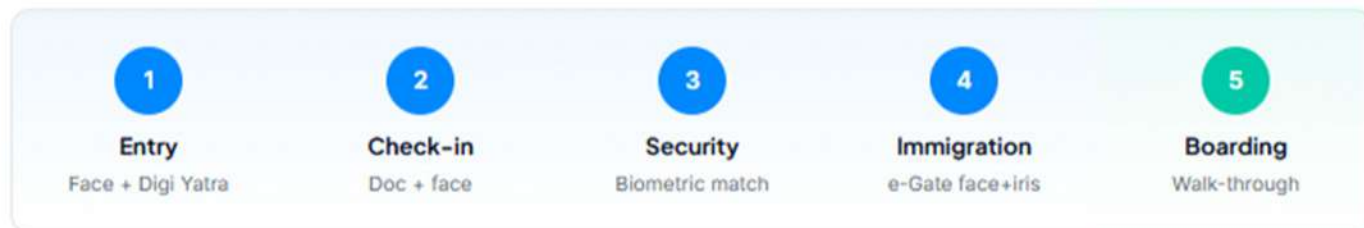
FIDO L2

Edge + Cloud Architecture

Edge handles real-time biometrics. Cloud handles orchestration and analytics. Neither fails alone.



Passenger Journey Transformation



DIGI YATRA INTEGRATION

Native integration with the Digi Yatra ecosystem for tokenised identity exchange.

- ✓ Token lifecycle management
- ✓ Self-service enrolment kiosks
- ✓ e-Gate API integration
- ✓ Real-time flow analytics

THROUGHPUT

2,400
passengers/hour/lane

85%

fewer manual
checks

15 min

saved per journey

Zero-Trust Secure Facilities

Multi-modal, real-time, cryptographically auditable identity at every checkpoint.

ACCESS ZONES

-  **Zone 1 — Perimeter**
Vehicle + face verification. ANPR.
-  **Zone 2 — Reception**
Multi-modal enrolment. Time-bound credentials.
-  **Zone 3 — Operational**
Continuous re-verification. Tailgating detection.
-  **Zone 4 — SCIF**
Dual-authority. Iris + fingerprint. Fully offline.



Air-Gap Operation

Full functionality without network.



Tailgating Detection

AI correlates access with cameras.



Crypto Audit Chain

TPM-signed. Tamper-evident to SIEM.

0

unauthorised access in 18 months

Enterprise Access

Frictionless biometric access replacing passwords and cards for hybrid workforces.

- ✓ Face at turnstiles
- ✓ Meeting room unlock
- ✓ Contractor auto-expiry
- ✓ HRIS onboarding
- ✓ Multi-site occupancy

60%

less overhead

3x

faster visitors

Connected Urban Spaces

Identity layer connecting transit, government services, and public safety.

- ✓ Transit fare validation
- ✓ Walk-in government services
- ✓ City watchlist screening
- ✓ Utility crew access
- ✓ Privacy management

50+

camera feeds

<2s

city-wide match

Why Mantra, Not Alternatives

CERTIFICATIONS



STQC Certification
Mandatory Indian standard for Aadhaar/National ID devices.



iBeta Level 2 PAD
International gold standard. 100% interception.



SOC 2 Type II
Independently audited security controls.

ADVANTAGES



Indigenous R&D
100% in-house algorithms. No third-party SDK dependency. Full IP.



Global Deployments
12+ countries. Aviation, defence, banking, government.



Unlimited Scale
Tested to 100M+ templates. Sub-second national-scale 1:N.

99.7%
Multi-modal accuracy

<3s
End-to-end verify

12+
Countries

500M+
Identities enrolled

Airport Transformation

Major Indian international airport (40M+ passengers). Mantra deployed across all touchpoints in 14 months.

✗ Before

- ✗ 6 separate systems with own databases
- ✗ Manual verification — 4.2 min avg
- ✗ No real-time watchlist screening
- ✗ Failed 2 BCAS audits in 3 years
- ✗ Peak queues exceeding 45 min

✓ After

- ✓ Single unified identity backbone
- ✓ Fully automated — 8 sec per passenger
- ✓ Real-time watchlist at every point
- ✓ BCAS audit passed — zero findings
- ✓ Peak processing under 7 min total

TIME
4.2 min

8 sec

QUEUES
45 min

<7 min

STAFF
120 FTE

42 FTE

COMPLIANCE
2-fails

0 fails

The Next Identity Paradigm

Three converging forces will reshape identity infrastructure over the next five years: contactless interaction, autonomous verification, and smart infrastructure integration.



Contactless Identity

Walk-through verification becomes the default. No stops, no tokens, no physical interaction. Presence alone triggers identity resolution.



Autonomous Verification

AI-driven risk scoring replaces binary pass/fail. Behavioural biometrics combined with physiological signals for continuous authentication.



Smart Infrastructure

Identity becomes a utility layer — like electricity — embedded into buildings, transport, and public spaces. Invisible until needed.

READINESS INDICATORS

Contactless tech maturity

85%

Edge AI capability

72%

Regulatory readiness

68%

Privacy-preserving tech

55%



Identity is not a feature. It is the foundation.

Every secure transaction, every controlled access point, every verified citizen interaction depends on identity infrastructure that is unified, scalable, and trustworthy.

99.7%

Accuracy

<3s

Verification

500M+

Enrolled

GET IN TOUCH

 www.mantratec.com

 info@mantratec.com

 Mantra Softech

© 2026 Mantra Softech. All rights reserved. This document contains proprietary information.