VERTICAL EDITION 06 · CITIZEN, FIELD & DEPARTMENT APPS

Stop the claim that no citizen ever made.

Public money moves on assertions: an enrolment, a claim, a field inspection, an attendance mark. Each one has to be defensible to an auditor years later. NonaShield answers a deterministic question before the submission leaves the handset — was this exact request produced by the physical device holding the non-exportable key, and has it been altered since? Attestation, RASP, fingerprinting, behavioural intelligence, network defence, risk decisioning and forensic evidence run as one signed pipeline across citizen, field-operator and departmental apps.

400+	40+	9	1
Distinct threat vectors monitored across device, network and server	Behavioural vectors profiled per submission session, continuously	Architectural layers delivered as one cryptographically signed pipeline	Vendor, contract, integration and console — not four or five

IN THIS DOCUMENT

EX 1 The fraud that actually costs a department — eight vectors, and the layer that stops each

EX 2 One platform, nine layers — and only three permitted to make a binary decision

EX 3 Commercial & deployment model — one vendor instead of five, audit-ready evidence

HARDWARE ATTESTATION · RASP · FINGERPRINTING · BEHAVIOURAL BIOMETRICS · GRAPH INTELLIGENCE · NETWORK DEFENCE · API GATEWAY · RISK DECISION ENGINE · EVIDENCE & COMPLIANCE

EXHIBIT 1 — EIGHT VECTORS, ONE ARCHITECTURE

The vocabulary is entitlement. The question underneath is possession.

Every vector below reduces to the same test: was this request produced by the physical device it claims to come from, by the person entitled to hold it, in an environment that has not been tampered with? The architecture does not change per sector — what changes is the policy set in Layer 7 and the entity model in Layer 5.

VECTOR	HOW IT ARRIVES ON A CITIZEN OR FIELD APP	LAYER
Benefit & subsidy leakage	Device farms enrolling and claiming on behalf of many beneficiaries; one operator, hundreds of identities.	**1, 3, 5**
Identity duplication at enrolment	The same person enrolled repeatedly under altered particulars from cloned or emulated handsets.	**1, 3, 5**
Ghost beneficiaries & proxy claims	Claims filed for deceased, migrated or non-existent beneficiaries by an intermediary holding the device.	**3, 5, 7**
Field-operator & insider collusion	Departmental and CSC operator apps used outside mandate, shared handsets, back-dated field entries.	**1, 5, 8–9**
Tampered field submissions	Geo-tag, timestamp and photo evidence spoofed on inspection, survey and attendance apps.	**1, 2, 7**
Deepfake & liveness defeat at eKYC	Synthetic face and document submission through injected camera feeds during video verification.	**1, 3, 7**
Bank-mandate & DBT diversion	Beneficiary account details altered ahead of disbursement, often paired with SIM and contact changes.	**2, 3, 7**
Bot floods on citizen portals	Scripted clients hoarding appointment slots, application tokens and scarce entitlements at scale.	**2, 3, 6**

WHERE CRYPTOGRAPHY IS SILENT — STATED PLAINLY

When a genuine beneficiary on their own device is coached through a fraudulent claim, every cryptographic check passes correctly. That case belongs to graph, behavioural and intent analysis (Layers 4–6), which surface operator-linked clusters and repeat-facilitator patterns rather than penalising the citizen.

APPS COVERED ON ONE INTEGRATION

Citizen service apps, field-inspection and survey apps, CSC and operator apps, departmental consoles, eKYC and enrolment journeys — Android and iOS from one Kotlin Multiplatform SDK. Layers engaged for this vertical: **1–3, 5 and 8–9**, with Layers 6–7 engaged where entitlement volume warrants it.

EXHIBIT 2 — ONE PLATFORM, NINE LAYERS

Six procurements, one signed pipeline — and only three layers may say no.

Device trust, app logic, network gateways, identity, backend controls and forensic chain-of-custody are conventionally six disjointed purchases correlated after the fact. NonaShield delivers them as a single pipeline in which every signal is bound to the same cryptographic assertion at the moment of capture.

BAND A · LAYERS 1–3 **Deterministic device & payload truth**	**1 Mobile SDK** — runtime signal capture, RASP, on-device enforcement **2 API Gateway & Network** — edge enforcement, signed-payload validation on enrolment, claim and disbursement endpoints **3 Trust Verification** — server-side hardware key attestation	WHAT IT ESTABLISHES Binary authority. These layers may allow or block outright because their error rate justifies it.
BAND B · LAYERS 4–6 **Probabilistic risk enrichment**	**4 Fraud Intelligence** — risk modelling and scoring across entities **5 Graph Intelligence** — entity linkage, duplicate-identity and operator-cluster detection across beneficiaries **6 Behavioural Intelligence** — continuous interaction and submission-intent analysis	WHAT IT ESTABLISHES Graded risk only. These layers modulate friction; they never make a binary access decision alone.
BAND C · LAYERS 7–9 **Verdict & accountability**	**7 Decision Engine** — real-time rule and model enforcement: allow / step-up / block **8 Evidence Engine** — hash-chained, tamper-evident immutable record per enrolment, claim and disbursement **9 Compliance** — regulatory controls, WORM retention, regulator-mapped export	WHAT IT ESTABLISHES One graded, signed verdict — and non-repudiable accountability as a by-product of the transaction path.

DETECT ———▶ ENFORCE ———▶ DECIDE ———▶ HARDENED RULES PUSHED BACK TO THE SDK

THE SEPARATION MATTERS MORE THAN THE COUNT

Most platforms fail not because they lack signals but because they let weak signals make strong decisions. Segregating binary authority (Bands A and C) from probabilistic enrichment (Band B) keeps false positives out of genuine citizen journeys — a wrongly blocked entitlement is a service-delivery failure, not just a support ticket — while still allowing behavioural evidence to add friction the instant a session deviates from its own baseline.

EXHIBIT 3 — POINT SOLUTIONS VERSUS ONE UNIFIED PLATFORM

The stack you would otherwise assemble has four seams.

	FOUR TO FIVE POINT SOLUTIONS	NONASHIELD (UNIFIED)
Vendors to contract & manage	4–5 separate vendors	**1**
Integrations to build & maintain	One per vendor, each with its own SDK and API	**Single SDK + gateway + backend**
Signal correlation across layers	Manual or none — each tool sees only its own slice	**Fused into one explainable risk score**
Threat vectors covered	Varies per tool; gaps at the seams	**400+, continuously correlated**
Compliance & audit evidence	Assembled after the fact from disparate logs	**Native hash-chained evidence, regulator-mapped**
Time to deploy	Sequential vendor onboarding	**A single integration cycle**

DEPLOYMENT

01 Threat-surface review — map your current stack, seams and highest-loss journeys. Two weeks.

02 Pilot — one app, one journey, production citizen flow, measured against existing controls.

03 Production rollout — full journey coverage, policy tuning, evidence chain live for audit.

04 Continuous hardening — detect, enforce, decide, with hardened rules pushed back to the SDK.

COMPLIANCE & ASSURANCE

Aligned to MeitY / CERT-In guidelines and STQC audit expectations for government applications

ISO 27001 and DPDP alignment; on-premises and sovereign-cloud deployment

Five-year WORM retention under compliance lock

Court-admissible, dual-ECDSA-signed evidence for statutory and CAG review

Fail-closed queuing; zero backend exposure on blocked traffic

Post-quantum-ready cryptographic design

WHY DIMEAI

25 years of e-governance and banking-technology security experience behind the architecture

Patent-backed, tamper-evident evidence chain

Explainable ML risk scoring — decisions you can defend to a regulator

Android & iOS from one Kotlin Multiplatform SDK

Cloud, on-premises or hybrid — matched to your infrastructure posture

One commercial relationship, one console, one support line

NONASHIELD · E-GOVERNANCE & GOVERNMENT DEPARTMENTS

Stop the fraudster. Before the fraud.

contactus@diimeai.com
+91 85917 55427
DIIMEAI.COM