UNIFIED PLATFORM · CROSS-INDUSTRY EDITION · 2026

The World's First End-to-End Mobile Cryptographic Infrastructure Shield

Stop the Fraudster, Before the Fraud.

Every mobile fraud control on the market answers a probabilistic question. NonaShield answers a deterministic one: **was this exact request produced by the physical device holding the non-exportable key, and has it been altered since?** Hardware attestation, RASP, device fingerprinting, behavioural intelligence, network defence, risk decisioning and forensic evidence run as one signed pipeline — in any industry where a mobile app carries money, identity or regulated data.

IN THIS DOCUMENT

400+
Distinct threat vectors monitored across device, network and server

9
Architectural layers delivered as one cryptographically signed pipeline

40+
Behavioural vectors profiled per session, continuously

1
Vendor, contract, integration and console — not four or five

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

EXHIBIT 1 — THREE QUESTIONS, ONE OF THEM DECISIVE

Mobile fraud products answer one of two questions. Neither produces a proof.

Buyers evaluate mobile fraud tooling on feature counts. The more useful test is what class of assertion the product can make when a disputed transaction has to be defended — to a risk committee, a regulator, or a court.

APPROACH 01 · PROBABILISTIC

Does this resemble a device we have seen before?

Device fingerprinting assembles an identifier from software-reported device attributes. Every attribute is client-declared — and defeating them is a mature commercial market, not a theoretical risk.

OUTPUT: A SIMILARITY SCORE

APPROACH 02 · CONDITIONAL

Is this environment compromised right now?

RASP instruments the application runtime to detect rooting, hooking, tampering and instrumentation. It is essential, and it is a permanent arms race — every detection invites a new bypass.

OUTPUT: A THREAT INDICATOR

APPROACH 03 · DETERMINISTIC

Was this exact request produced by this physical device, unaltered?

NonaShield is a cryptographic possession proof with the detection signals sealed inside it. The question is deterministically bounded, and the answer is binary — with RASP and fingerprinting carried as inputs, not as the verdict.

OUTPUT: A SIGNED PROOF

WHY THIS IS THE EVALUATION CRITERION

A similarity score and a threat indicator are inputs to a judgement. A possession proof is a different class of assertion: it does not estimate, it excludes. An adversary who has stolen every credential, cloned the app, and replayed a valid session still cannot sign from hardware they do not physically hold.

AND WHERE IT IS SILENT — STATED PLAINLY

The same property that makes the proof decisive renders it silent when the adversary physically holds the genuine device — a customer talked into authorising the transfer themselves, for instance. NonaShield does not hide that boundary: it covers it with continuous behavioural profiling, graph intelligence and intent analysis (Layers 4–6), applying friction the moment a session deviates from its own baseline. Any vendor claiming cryptography alone solves it is describing marketing, not architecture.

THREE QUESTIONS WORTH PUTTING TO ANY MOBILE FRAUD VENDOR

QUESTION 01

Can you prove possession, or only resemblance? If the answer rests on device attributes the client reports about itself, the vendor is scoring a guess — however good the model.

QUESTION 02

Were the signals captured under one assertion, or stitched together afterwards? Signals reconciled across vendors post-hoc cannot prove they describe the same device at the same instant.

QUESTION 03

What does your architecture explicitly not cover? A vendor who cannot name the boundary has not mapped the threat model — and the unmapped part is where the loss will land.

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 from six vendors, 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 3 **Trust Verification** — server-side hardware key attestation	WHAT IT ESTABLISHES **Binary authority.** These layers are permitted to 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, mule and coordinated-network detection 6 **Behavioural Intelligence** — continuous interaction and intent analysis	WHAT IT ESTABLISHES **Graded risk only.** These layers modulate friction. They are never permitted to 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 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) is what keeps false positives out of the ~99% of traffic that is legitimate, while still allowing behavioural evidence to add friction the instant a session deviates from its own baseline.

EXHIBIT 3 — THE WORLD'S FIRST UNIFIED MOBILE TRUST PLATFORM

Eight defence pillars, 400+ threat vectors, one signed pipeline — the first of its kind.

No other platform delivers hardware attestation, RASP, fingerprinting, behavioural intelligence, network defence, API gateway enforcement, risk decisioning and compliance evidence as a single end-to-end cryptographic pipeline. Eight independently verifiable pillars monitor **400+ distinct threat vectors** across device, network and server — and because every signal is captured under one assertion, they are correlated by construction rather than reconciled afterwards from four vendors' logs.

#	PILLAR	WHAT IT DOES
1	**Hardware Attestation**	Non-exportable keys generated inside the device's TEE / StrongBox / Secure Enclave; native attestation (Play Integrity, App Attest) proves binary and device integrity to the backend before any trust is extended.
2	**RASP**	Detects debugging, hooking frameworks (Frida, Xposed), repackaging, cloning, overlay and tapjacking attacks, keylogging and malware — and terminates on critical violation without waiting for a network round-trip.
3	**Device Fingerprinting**	Composite identity from hardware, OS, network and install markers; flags cloned installs, emulators, device farms and SIM/device cloning indicators.
4	**Behavioural Intelligence**	Navigation timing, input rhythm and micro-jitter validation distinguish a genuine human session from a scripted, automated or remote-controlled one.
5	**Network Defence**	Certificate-pinned TLS with anomaly detection on the transport channel; blocks MitM interception, disguised routing, nonce reuse and header tampering.
6	**API Gateway**	Edge enforcement validates attestation tokens and signed payloads, applies device/user/IP rate limiting, and filters bot and API abuse — with zero backend exposure on blocked traffic.
7	**Risk Decision Engine**	Centralised server-side fusion of every layer into one explainable risk score, enforcing allow / step-up / block. Includes synthetic-identity, account-stacking and SIM-swap correlation before OTP release.
8	**Evidence & Compliance**	Tamper-evident, hash-chained evidence with dual ECDSA signatures, fail-closed queuing, audit logging and regulator-mapped export for supervisory review.

CARRIED ON THE SAME PIPELINE, AT NO ADDITIONAL INTEGRATION COST

SIM-swap correlation before OTP release · replay-resistant transaction authorisation · deepfake and liveness-defeat signals at onboarding · synthetic-identity and multi-accounting detection · screen-share, remote-access and social-engineering indicators · mule and coordinated-network graph detection · agent, partner and insider-channel scoring · bot and emulator-farm suppression.

EXHIBIT 4 — FOUR PROPERTIES, FOUR MECHANISMS

Each claim resolves to a mechanism. If it does not, it is not in this document.

Security marketing is dense with adjectives. The four properties below are stated as mechanism and consequence, so a technical evaluator can verify each one against the implementation.

#	PROPERTY	MECHANISM	CONSEQUENCE
1	**Possession proof**	Non-exportable EC P-256 key pair generated inside StrongBox / Secure Enclave, with server-side validated hardware key attestation.	An adversary holding **every** credential still cannot sign from their own hardware. Credential theft stops being sufficient.
2	**Sealed at origin**	Threat, identity and behavioural signals are bound into one enclave-signed assertion at the moment of capture.	Provable co-origin — cryptographic proof that every signal describes the same device at the same instant, not three vendors' timestamps stitched together later.
3	**Tiered assurance**	Hardware assurance level is measured per device and transmitted as a live risk input.	Assurance degrades gracefully with the handset; service does not stop. Older and low-end devices are scored, not excluded — critical in mass-market and emerging-market portfolios.
4	**Evidence by construction**	Hash-chained record with dual ECDSA signatures and five-year WORM retention under compliance lock.	Non-repudiation is a by-product of the transaction path, not a reporting project. Dispute and regulatory evidence exists before anyone asks for it.

THE PRECISE CLAIM

NonaShield is **cryptographically tamper-evident and replay-resistant**, contingent on the signing device not already being compromised. A signature proves two things: the payload was not altered between device and server, and it was not replayed. It cannot prove the device was uncompromised *before* it signed — that residual belongs to runtime integrity, which is precisely why hardware binding and RASP are complements rather than alternatives, and why both ship in one platform.

WHAT NONASHIELD DOES NOT CLAIM

It does not claim to read intent. When a legitimate customer, on their own enrolled device, is talked into authorising a transfer, every cryptographic check passes correctly — because every check is correct. That case is addressed by behavioural baselining and intent analysis (Layers 4–6) applying surgical friction, not by the possession proof — which is precisely why those layers ship inside the same platform rather than as a second purchase.

EXHIBIT 5 — ONE ARCHITECTURE, TEN FRAUD VOCABULARIES

The architecture does not change by industry. Only the name of the fraud does.

Wherever a mobile app carries money, identity or regulated data, the underlying question is identical: 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? NonaShield answers it once, at the platform level — the industry-specific work is policy configuration, not re-architecture.

SECTOR	FRAUD THAT ACTUALLY COSTS THEM	LAYERS ENGAGED
Capital markets, broking & wealth	Unauthorised order placement, account takeover, pump-and-dump via compromised accounts, API manipulation of trade parameters, mule-account layering	**1–3, 5–9**
NBFC & digital lending	Synthetic identity at onboarding, loan stacking, bot-driven loan floods, EMI & OTP replay, DSA-agent and insider-enrolment fraud, cloned lending apps	**1–7**
Retail banking & payments	RAT-driven account takeover, SIM swap before OTP release, credential stuffing, authorised push payment fraud, overlay and accessibility abuse	**1–9**
Insurance	Policy and claim fraud from cloned or emulated devices, agent-channel collusion, fabricated identity and document submission, duplicate-claim networks	**1–3, 5, 7–9**
Crypto, wallets & neobanks	Key-extraction and device-cloning attacks, automated withdrawal scripting, deepfake onboarding, rapid multi-account creation	**1–4, 6–8**
Government & e-governance	Benefit and subsidy fraud from device farms, identity duplication at enrolment, tamper-evident audit for statutory and supervisory review	**1–3, 5, 8–9**
Healthcare & digital health	Tele-consult and prescription identity fraud, regulated-record access from compromised handsets, provider-credential misuse	**1–3, 6, 8–9**
Gaming, wagering & rewards	Emulator and bot farms, multi-accounting, promotion and bonus abuse, collusion rings, automated play	**1, 3–6**
Mobility, gig & marketplaces	Driver and rider account farming, GPS and app-tamper manipulation, incentive and referral fraud, seller-account takeover	**1–4, 6–7**
Telecom & connected services	SIM-swap and port-out abuse, subscription and device-financing fraud, eSIM provisioning abuse	**1, 3, 5, 7**

THE PORTABILITY TEST

A fraud platform is only genuinely industry-agnostic if adding a new sector requires no new integration. NonaShield's device, network and evidence layers are invariant; what changes per sector is the policy set in Layer 7 and the entity model in Layer 5. That is a configuration exercise measured in weeks — not a second procurement cycle.

EXHIBIT 6 — POINT SOLUTIONS VERSUS ONE UNIFIED PLATFORM

The stack you would otherwise assemble has four seams. Fraud arrives at the 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

- **Android & iOS** from one Kotlin Multiplatform SDK
- Customer, agent, partner and collections apps on the same integration
- **Cloud, on-premises or hybrid** — matched to your infrastructure and compliance posture
- Fail-closed queuing; zero backend exposure on blocked traffic

COMPLIANCE & ASSURANCE

- Aligned to **ISO 27001, PCI DSS, DPDP** and the **RBI Cyber Security Framework**; SEBI-ready
- Five-year **WORM retention** under compliance lock
- Court-admissible, dual-signed transaction evidence
- **Post-quantum-ready** cryptographic design

WHY DIMEAI

- **25 years** of banking-technology and e-governance security experience behind the architecture
- Patent-backed, tamper-evident evidence chain
- Explainable ML risk scoring — decisions you can defend to a regulator
- One commercial relationship, one console, one support line

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

STEP 02
Pilot
One app, one journey, production traffic. Measured against your existing controls.

STEP 03
Production rollout
Full journey coverage, policy tuning, evidence chain live for audit.

STEP 04
Continuous hardening
Detect → Enforce → Decide, with hardened rules pushed back to the SDK.

Stop the fraudster.
Before the fraud.

JRAJESH@DIIMEAI.COM · +91 85917 55427
DIIMEAI.COM