AXON · SOVEREIGN TELECOM IDENTITY

NATIONAL SIM REGISTRY.

Every connection, linked to an accountable identity.

A sovereign national registry for verified subscriber identity, full SIM lifecycle control and audited access across participating operators.

350M+
SIMs Registered
Proven at national scale

15+
Countries Deployed
Complex regulatory markets

Up to 200M
Monthly Transactions
Validated against national records

100K+
Field Agents
Feeding verified registrations

Full Life
Lifecycle Governance
Stock · registration · SIM swap · recycling

WHY OPERATOR-LEVEL DEDUPLICATION ISN'T ENOUGH

One Operator Can Only See Its Own Subscribers.

A person blocked at one network simply registers at the next. Biometric deduplication only closes that gap when it runs **above the operator layer, at a registry every operator feeds into.**

SCOPE

What Operator-Level Dedup Can Answer

"Has this person registered with us before?" — nothing more.

- Blind spot: every subscriber of every *other* operator
- A blocked registrant simply moves to the next network and re-registers
- Each operator holds its own biometric silo, under its own policy
- Registration volume is a growth metric — deduplication works against it

SCOPE

What a National Registry Can Answer

"Has this person registered *anywhere in the country*, before?"

- The only blind spot left is an operator not yet integrated
- A blocked registrant is recognised at the next attempt, whoever they approach
- One registry, one published policy, one audit regime
- Not measured on subscriber growth — closing the gap *is* the mandate

Operator A
Registration blocked

→

Operator B
Registered, no cross-check

OUTCOME

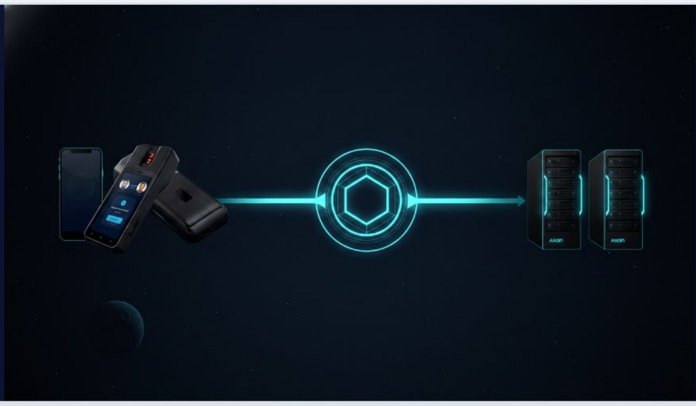
One registration, checked once, against everyone — not one registration, checked once, against one operator's own list.

For the full argument — the four ways ghost subscribers actually get created, and what to specify in a tender — see Axon's white paper, "Ghost Subscribers, and the Limits of Operator-Level Deduplication."

THE NATIONAL OPERATING MODEL

A Common Standard From Legacy Base to Live Event.

A programme can begin with existing subscriber records, add real-time control for high-risk events, and then move each operator, channel and lifecycle event onto one governed national standard — **without stopping the market to improve it.**



01 Controlled Integration

Every participating operator connects through defined, signed and audited interfaces for batch, real-time and exception workflows.

- A single national evidence and transport standard, with no informal side channels
- Format, identity evidence and transport are checked before a record reaches the registry

02 Policy and Decision Engine

National rules are versioned and applied consistently, with clear reasons for approve, decline, refer, provisional or remediate decisions.

- SIM limits, category rules, waivers and high-risk event checks are explicit policy, not hidden code
- Queues, retries and reconciliation support resilient high-volume operation

03 National Registry and Evidence

Verified subscriber, SIM, device, channel and decision evidence is held as a governed national record — not a merged guess.

- Connect civil identity, immigration, business and authorised security sources where policy permits
- Maintain a durable audit trail for registration, review, remediation and lawful access

OUTCOME

One national operating standard for registration and change events — with evidence that can be explained, audited and improved.

ONE PERSON, ONE IDENTITY, EVERY NETWORK

Cross-Operator 1:N Matching, Not Per-Operator Checks.

Every new registration is searched against the whole national registry — **every operator, not just the one being joined** — before it is accepted.

MATCHING

What Gets Matched

Fingerprint, face, or both, captured at the point of registration and matched against the full cross-operator record.

- ISO/IEC 19794 biometric record format — portable across operators and systems
- Batch and real-time deduplication, depending on the channel
- Independently benchmarked matching — a floor for accuracy, not a guarantee on its own

SCALE

Why Cross-Operator Matters

A person blocked at Operator A and waved through at Operator B is not a dedup failure — it's what happens when dedup stops at the operator boundary.

- Registered once, recognised everywhere — the same identity, whichever network is approached
- Closes exactly the loophole operator-level ABIS cannot see

OUTCOME

Deduplication that works across the whole market — because a person only has to be caught once.

Fingerprint

Face

Iris

3
Modalities
Fingerprint · Face · Iris

ISO/IEC
19794 Record Format
Portable across systems

Millions
of Subscribers
Batch & real-time

1:N
Cross-Operator Search
Not per-operator

THE PERSON, THE CREDENTIAL AND THE RIGHT TO REGISTER

Identity Assurance That Is Strong, Inclusive and Governed.

Verification does not stop at a name and document image. Combine biometrics, document evidence and authorised identity sources, with thresholds and exception pathways that fit **the country's own law and programme policy.**

Multi-Modal, Policy-Driven Checks

Face with liveness, fingerprint, document OCR, MRZ, PDF417, NFC and ePassport data can be combined for the assurance level required by the event.

- Use 1:1 comparison, 1:N duplicate search and watchlist checks where policy permits
- Every check produces an evidence-backed decision rather than an unexplained score

Designed for Inclusion and Adjudication

High assurance must not become an exclusion mechanism for people who need assistance or do not fit a standard biometric or document pathway.

- Support disability, failure-to-enrol, minor or guardian, non-ID, foreign visitor and corporate pathways
- Route exceptions through manual adjudication, appeal and provisional status with clear accountability

OUTCOME

The subscriber is not just registered — the identity decision is proportionate, explainable and backed by the evidence the programme trusts.

FROM SECURE STOCK TO SAFE RECYCLING

The Full SIM and Device Lifecycle, Governed.

A national registry must retain control as a connection changes. Track the identifiers and evidence behind every SIM event — **not only the initial registration.**

Stock, Activation and Active Use

Track SIM and eSIM stock allocation through distributor, agent and activation, then bind ICCID, IMSI, MSISDN and devices to an accountable subscriber record.

- Identify unregistered active SIMs and reconcile inventory and network events
- Apply national or operator policy limits with a clear effective date and reason

High-Risk Change Events

SIM swap, replacement, porting, transfer, suspension, dormancy, deactivation and recycling carry a different risk profile from first registration.

- Elevate re-verification and cooling rules when account takeover risk is highest
- Maintain an evidence trail for closure, deceased-person controls and safe number reuse

OUTCOME

A connection stays accountable after activation — through every change that can create fraud, consumer harm or regulatory risk.

SEE THE PATTERN BEFORE IT SPREADS ACROSS OPERATORS

Fraud Doesn't Respect Channel, Agent or Operator Boundaries.

SIM swap fraud, synthetic identity, channel abuse and SIM-box activity look different from inside one operator's data than they do **across the whole national registry.**

Identity, Agent and Device Risk

Evaluate a new or changed registration against reusable identity, document, agent, device and location signals — not only the subscriber record.

- Use agent accreditation, accountable-user logs, device registration and geofencing controls where policy requires them
- Surface repeated face, document, identity or device reuse for review
- Route alerts to a decision: block, flag, investigate, remediate or allow

National Analytics and Enforcement

Patterns that only appear once the programme can see across channels and operators become actionable cases, not just an interesting dashboard.

- Use registration funnels, data-quality, biometric performance and fraud-risk views to direct remediation
- Support statutory reporting, operator scorecards and evidence-led compliance action
- Apply analytics to an accountable case-management and appeal workflow

OUTCOME

Fraud detection that runs at the scale fraud actually happens — across every operator, not one at a time.

PRIVACY, DUE PROCESS AND EVIDENCE ARE PART OF THE PLATFORM

National Oversight With Boundaries That Hold.

A national registry must serve parties whose mandates do not always align. Privacy controls, auditable access and lawful-access governance make that possible **without any party seeing or doing more than its mandate allows.**

Privacy and Security by Design

Data residency, retention, deletion, masking, tokenisation, encryption, key management and biometric storage patterns are explicit programme choices.

- Choose central, federated or constrained biometric holding based on law, risk and operational needs
- Protect sensitive data in transit, at rest and through controlled operations
- Support subject access, correction, consent and breach-response processes where required

Auditable and Lawfully Governed Access

Regulator, operator, auditor and law-enforcement activity is scoped by role, purpose and authorisation, with evidence that can withstand review.

- Use warrant or authorisation workflows, tiered query, purpose coding and independent oversight where policy requires them
- Apply segregation of duties, privileged-access controls and digitally signed enrolment evidence
- Every access, query, decision and export is part of the tamper-evident audit trail

Regulator
Oversight & reporting across the whole registry

Operators
Own submissions only — never another operator's data

Law Enforcement
Scoped, logged access — not a standing open door

OUTCOME

Trust and integrity across the mobile ecosystem — because access, privacy and evidence are structured around who is accountable for what.

TWO SYSTEMS, ONE VERIFIED IDENTITY

Polaris Registers. The Registry Verifies Across Everyone.

These are deliberately separate systems, not one product wearing two names. An operator running Polaris gets omni-channel registration, agent tools and its own fraud controls. A regulator running the Government SIM Registry gets **a standalone, cross-operator view no single operator's system can provide** — even if every operator in the country is running Polaris.

OPERATOR SIDE

Polaris

Everything a telecom operator needs to register, verify and manage subscribers across every channel — online, agent, in-store.

- Omni-channel registration, dynamic number allocation, full SIM lifecycle
- Operator-level biometric deduplication and fraud control
- COMET hardware range for field capture, or bring-your-own-device

REGULATOR SIDE

Government SIM Registry

A standalone, cross-operator verification system for regulators — everything on the previous seven pages.

- Works whether operators are running Polaris, a competitor's system, or a legacy platform
- One verified identity per person, checked against every connected operator
- The registry a regulator needs precisely because no single operator can provide it

OUTCOME

Register with Polaris. Verify across the whole market with the Government SIM Registry. Independent systems that were built to work together.

WHY AXON

Proven Where It Matters.

Since 2005, Axon has delivered identity and enrolment platforms for tier-1 operators and national regulators, with deployments across Africa, the Middle East, and Asia.

350M+	15+	100K+	Up to 200M
SIMS REGISTERED	COUNTRIES DEPLOYED	FIELD AGENTS	MONTHLY TRANSACTIONS VALIDATED

TELCO SOLUTIONS TRUSTED BY

MTN · zain · ethio telecom · Zamtel · Nepal Telecom · Digitel · glo · ECONET Wireless · yas · MoMo from MTN · B · mauritius telecom · areeba

WHY THE GOVERNMENT SIM REGISTRY — EVERYTHING YOU JUST SAW

- **Closes the Cross-Operator Gap** — sees what no single operator's dedup can see
- **One Auditable Path** — every operator, one gateway, one validated record
- **Cross-Operator Deduplication** — one person, one identity, every network
- **National Database Integration** — verified against the records a government already trusts
- **Self-Service Regulator Reporting** — oversight that doesn't wait on an operator to send it
- **Fraud Control at Registry Scale** — patterns visible across operators, not one at a time
- **Role-Based, Multi-Tenant Governance** — regulator, operators and law enforcement, each in their own space
- **Built to Pair With Polaris** — the operator side and the regulator side, working together by design