TELCO & MOBILE MONEY

IDENTITY THAT DRIVES GROWTH — AND STOPS FRAUD.

Activate eSIMs online. Protect subscribers from SIM-swap fraud. Re-verify customers remotely with confidence.

IDToolkit SDK enables one trusted identity layer across every subscriber journey — from first activation to account recovery, upgrades, mobile money and ongoing authentication.

- More activations completed remotely
- Faster onboarding, less customer friction
- Stronger compliance and auditability
- No dealer commission on self-service activations
- Fewer SIM-swap and impersonation losses
- No repeated ID checks for trusted subscribers
- One layer across physical SIM, eSIM and digital

350M+	**500M+**	**15+**	**20+**
SIM Cards Registered	Identities Verified	Countries Deployed	Years in Telco
Across 20+ deployments	Registered or verified	Africa, Middle East & Asia	Registering subscribers for MNOs

WHAT REGISTRATION ALONE DOES NOT STOP

Registering a Subscriber Is Not the Same as Knowing Them.

Fraud does not announce itself. It looks like a normal activation — right up until the person, the document or the device turns out not to be what they claimed. And the attack that costs the most happens **after** registration closes.

Stolen Identities
A real document, presented by someone who is not its owner — at a dealer counter or uploaded to a digital journey.

Altered Documents
Edited fields, swapped portraits, or a document that was never genuine.

Screen & Print Replays
A photo of a photo — a screen, printout or photocopy held to the camera.

Deepfakes & Injection
Synthetic faces and fabricated video fed straight into the capture pipeline, bypassing the camera.

Duplicate Enrolments
The same person registering again under a different name or document, often at industrial scale.

Compromised Devices
Emulators, rooted devices and device farms built to file the same registration thousands of times.

SIM Swap & Takeover
The attack after registration — a replacement SIM obtained for someone else's number.

Where mobile money exists, a SIM swap is not a telco problem. The phone number is the account. The OTP is the authentication. A successful SIM swap is a bank account takeover executed through the operator — who carries the loss, the regulator's attention and the reputational damage.

PROOF

Axon examines the person, the document, the device and the identity history — before deciding who to trust.

ONE ENROLMENT, THREE USES

Enrol Once. Verify for Life.

Most operators treat subscriber identity as a registration cost — verify once, satisfy the regulator, file the record. That leaves the most valuable asset in the process unused. **The biometric captured at registration is a reusable key** that secures every high-risk event for the life of the account.

ACQUISITION	ENROLMENT	LIFETIME USE
Digital Dealer & agent Retail store Partner API Document · liveness · 1:N · screening · risk decision	**Identity verified** **Biometric enrolled** Bound to ICCID / MSISDN Bound to wallet identity Record sealed & hash-chained	**TELCO** SIM swap · Change of ownership · Port-out · Care & recovery **MOBILE MONEY** Wallet KYC · Tier upgrade · Transfers · Cash-out **AGENT & MERCHANT** Onboarding · Authentication · Transaction attribution

SAME RISK ENGINE · SAME AUDIT TRAIL · SAME ENROLLED IDENTITY

Part 1 — Acquisition

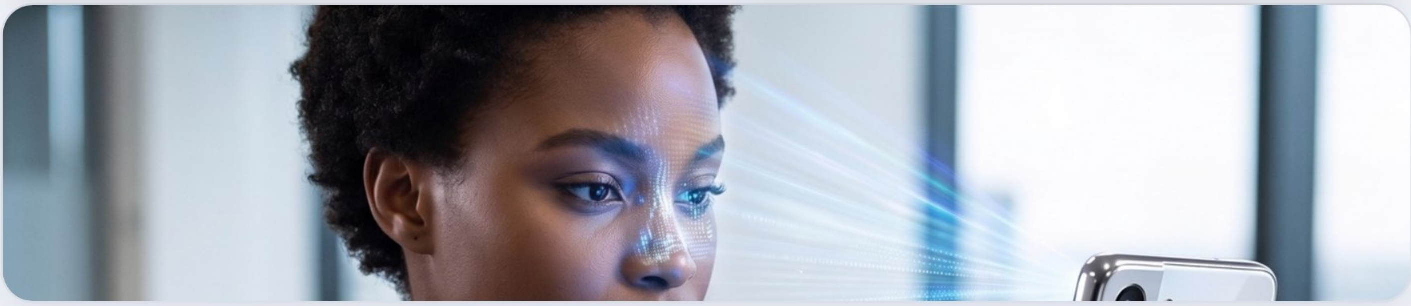
Problem: intent leaks before it becomes an active subscriber.

- Measured in conversion, time-to-live, cost per activation
- Owned by Digital, Growth and Distribution

Part 2 — Protection

Problem: account takeover, SIM swap and disputed ownership.

- Measured in fraud losses, care cost, regulatory exposure
- Owned by Fraud, Revenue Assurance and Compliance



THE POINT

The cost sits in acquisition. The value compounds across everything after it.

ONLINE eSIM ACTIVATION — THE REVENUE CASE

Sell Anywhere. Activate in Minutes.

eSIM removes the last physical step in acquisition — and identity is what unlocks it. A customer sees an offer, proves who they are, passes your risk rules, chooses a number and connects — no store visit, no courier, no "we'll activate you later" moment where the sale leaks away.

Every hour between wanting a SIM and having one is an hour the customer can change their mind — or buy from someone else.

WHERE ACTIVATION LEAKS

Verification and provisioning are separate
Identity confirmed, but the number and SIM handled later, in another system or another visit.

The digital lead goes back into a queue
A store, a dealer, a manual exception — at the moment intent was highest.

Every channel applies a different rule
A different decision and a different quality of record depending on which door was used.

Customer, SIM, MSISDN and evidence split
Making disputes, care escalations and fraud investigations expensive later.

THE JOURNEY

01 **Entry**
02 **Capture**
03 **Liveness**
04 **Document**
05 **Dedupe**
06 **Consent**
07 **Decision**
08 **Number**
09 **Provision**
10 **Enrol**

No physical SIM. No store visit. No dealer hand-off.

Step 10 is the one most operators skip.
Enrolment costs nothing extra at registration — and it is what makes every verification for the rest of that subscriber's life **instant.**

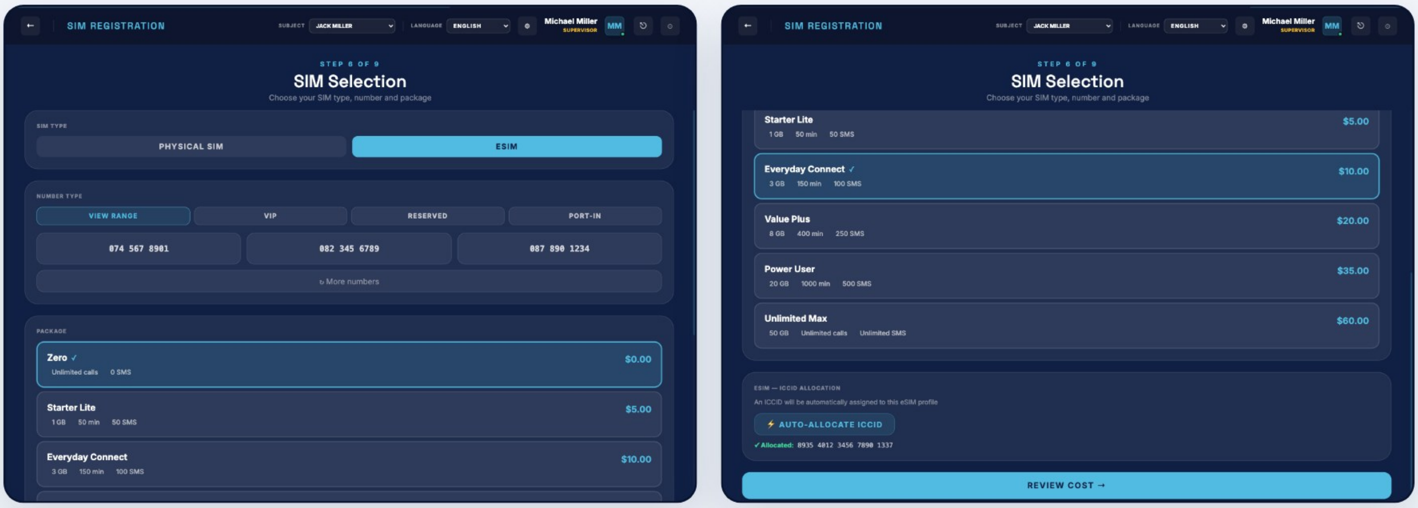
Self-service doesn't just move faster. It costs less.
A registration normally carries a dealer or agent commission — the channel cost of getting a subscriber signed up. A subscriber who self-activates through this journey never touches that channel, so **that commission is never paid on that registration.** And every eSIM activation is a SIM card never manufactured, shipped or distributed — **cutting plastic, logistics and carbon** alongside the cost.

PROOF
One journey from any channel — **with the same rules behind every door.**

THE HALF NOBODY ELSE DOES

Verification Is Half the Job. Activation Is the Other Half.

A verification decision is not an active subscriber. The operator still needs number allocation, provisioning, and the systems that own the subscriber updated — **and a reliable answer when one of those hand-offs fails.**



ESIM SELECTION WITH LIVE NUMBER INVENTORY · AUTOMATIC ICCID ALLOCATION

ICCID / MSISDN Binding

The verified identity bound to the SIM and the number at the moment of activation, so the registration record and the network record are one record. Running in production at operator scale.

Dynamic Number Allocation

Live inventory exposed in the journey — choose from an available range, take a premium or reserved number, or port in an existing one, without an agent re-keying the request.

eSIM Profile Delivery

Secure delivery as the final step of the same journey, so the customer connects in the same sitting.

CRM / BSS / OSS Hand-off

The verified record passed onward through provider-agnostic connectors, webhooks and status callbacks.

Exception & Reconciliation

If verification passes but provisioning fails, the operator sees the state, retries or refers — without asking the customer to start again.

Physical SIM or eSIM

The same journey and the same binding, whether the subscriber takes a physical SIM at a dealer or an eSIM profile on their own device.

PROOF

Identity, number and SIM bound in one transaction — and one auditable record.

THE ATTACK THAT COSTS OPERATORS MOST

Biometrically Secure SIM Swaps.

A replacement SIM issued to the wrong person is not a support ticket — it is **a drained bank account, a regulator's letter and a story in the press**. Every swap request is checked against the subscriber's enrolled 3D face **before the OTP is sent**. Once enrolled, proving a subscriber is who they claim takes seconds — no document, no store visit, no security questions an attacker can research.

SIM Swap & Replacement

The highest-value attack surface an operator has. A 3D:3D match against the enrolled template removes the attack at its root — the attacker cannot present the registered subscriber's face.

Change of Ownership

Both sides verified in one flow: the current owner authorises release against their biometric, the incoming owner is verified and enrolled — so the number's identity record stays continuous.

Port-Out

A port request that cannot produce the registered subscriber's face is stopped before the number leaves the network.

High-Value Transactions

Step-up verification at the moment of risk, on the operator's own thresholds — not a session authenticated hours earlier.

Care & Account Recovery

PUK release, PIN reset, disputed billing. Biometric re-verification replaces knowledge-based questions that stopped being secret years ago.

Dealer & Agent Assurance

Verifies the person *performing* the transaction, not only the customer — so agent-side and collusion fraud carries a biometric record of who did it.

1:125M	30107-3
3D:3D RE-VERIFICATION FAR	LIVENESS CERTIFIED · LEVELS 1 & 2

Approximately one false match in every 125 million comparisons.

Adaptive FaceMap

Each successful re-verification strengthens the enrolled template. The control gets **stronger** over the life of the account, not weaker.

PROOF

The match confirms *who*. Liveness confirms *now*. Neither is sufficient alone.

ONE IDENTITY, TWO PRODUCTS

The Same Enrolment Opens the Wallet.

Most operators verify the same person twice — once to register the SIM, again to open or upgrade a wallet, on a different system, often months later at an agent kiosk. **That is two costs, two records, and two different answers to the question of who this customer is.**

01 Wallet KYC and Tier Upgrade

Most markets tier KYC — a basic wallet with low limits, a full wallet with high ones. The boundary is enforced by friction: upgrading means visiting an agent with documents, so most customers never do. Remote upgrade changes that, from the customer's phone, in minutes.

This is a **revenue argument, not a compliance one.** Every customer moved off a capped wallet raises the transaction ceiling the operator earns against.

02 Agent & Merchant Assurance

The agent network handles cash and has the least direct supervision.

- Agents verified and biometrically enrolled before activation
- Agents authenticate before transacting — activity attributable to a person, not a shared login
- 1:N across the agent base catches ghost agents and terminated agents re-registering
- Merchants verified and screened before they can accept funds

03 Transaction Authorisation

The enrolled biometric secures the transactions that matter, at the moment they happen.

- High-value transfers — step-up above operator-set thresholds
- Cash-out at an agent — the customer proves identity to the system, not to the agent's judgement
- New beneficiary — verification before a first transfer to an unknown recipient
- Wallet and PIN recovery — biometric instead of knowledge-based questions

Why the economics work

The enrolment is already paid for by SIM registration. Every wallet KYC, tier upgrade, transfer approval and cash-out afterwards runs against a template that **already exists** — which is why securing a mobile money transaction costs a fraction of onboarding the customer, and a fraction of the loss it prevents.

PROOF

One enrolment satisfies SIM registration *and* wallet KYC. Stop paying twice to verify one person.

EVERY ROUTE TO YOUR NETWORK

One Platform. Every Verification Journey.

A subscriber does not care which door they came through, and neither should the record. **Every channel runs the same verification engine, the same thresholds and the same audit trail** — so a walk-in and an app signup produce the same quality of decision.

Self-Service, In-App

The subscriber completes it themselves, in your app or a browser, on their own device. No app install required for a web journey.

Dealer & Agent Assisted

Agent-guided registration at a dealer, with the same checks and the same thresholds. No separate "agent-grade" shortcut.

Retail Store

In-store activation on the same pipeline, so a walk-in produces the same registration record as a digital signup.

Mobile Money Agent

Wallet onboarding, tier upgrade and cash-out verification at the agent point — with the agent themselves authenticated.

Care & Contact Centre

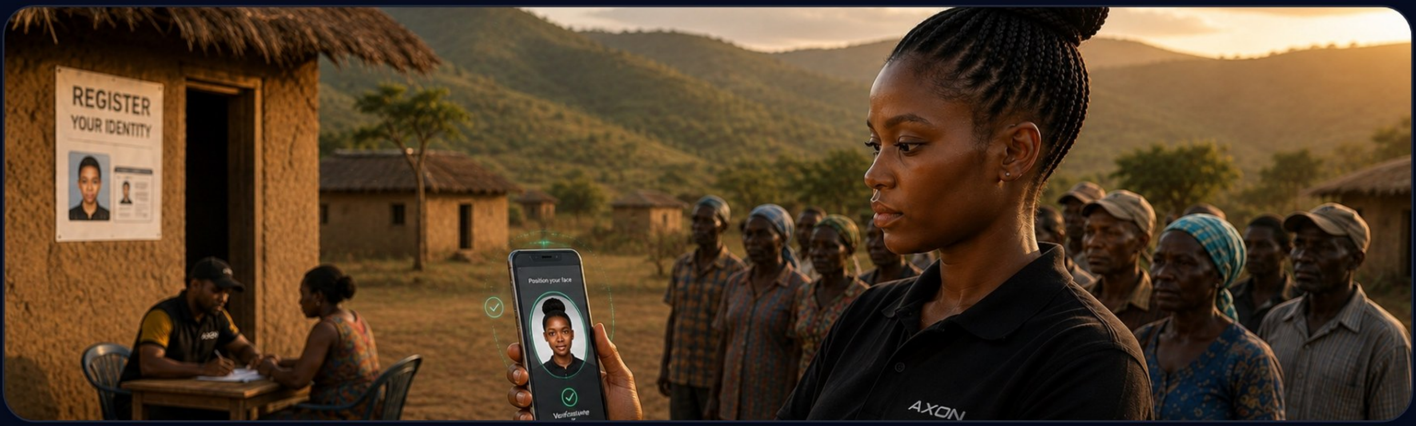
Re-verification during a support interaction — replacing knowledge-based questions that stopped being secret years ago.

Partner & Embedded

Banks, retailers, travel brands and fintech surfaces, through the API — acquisition wherever the customer already is.

Web, mobile and API integration.

All powered by **the same verification and risk engine.** The operator should not have to maintain a different verification policy for every route to market — or explain to a regulator why two channels produced different records for the same customer.



PROOF

Same engine, same rules, same audit trail — whichever door the subscriber came through.

AN SDK YOU EMBED — NOT A SERVICE YOU HAND OFF

Your Brand. Your Journey. Your Rules.

This is a software development kit you embed in your own apps and web journeys — not a third-party app your subscriber is handed off to. The subscriber never meets a vendor. The verification runs inside your experience, under your brand, on your rules: the screens they see, and the thresholds that decide when a journey is approved, referred or declined, configured per market and per channel.

- Your **logo, colours and customer experience**
- Your **activation and approval workflows**
- Your **language, prompts and consent wording**
- Your **verification thresholds**
- Your **market-specific document and policy rules**
- Your **risk decisions, review paths and audit trail**

ONE SDK · EVERY SCREEN

ANDROID
Android app
Embed the SDK in your existing Android application.

IOS
iOS app
Embed the SDK in your existing iOS application.

WEB
Browser journey
A responsive web flow — no app install for the subscriber.

API
REST API
Server-to-server integration into CRM, BSS and channel systems.

One verification engine behind all of them — the same journey, thresholds and audit trail whichever surface the subscriber uses.

AND RUN WHEREVER YOUR RULES REQUIRE

Axon-Hosted
Run as a managed service, with Axon operating the platform and its monitoring.

Private Cloud
Deployed inside your own tenancy, under your own cloud controls and network policy.

On-Premise
Fully inside your environment where data residency or sovereignty requires it.

Same product, same API, same console — the deployment model changes, the verification does not.

PROOF

You integrate it once — every screen your subscriber sees stays yours.

ONE PLATFORM, MANY OPERATORS

One Deployment. Many Tenants.

Group operating companies, MVNOs, channel partners and resellers can each run as an **isolated tenant on the same deployment** — with their own branding, journeys, thresholds and subscriber gallery — while the operator keeps central oversight of the whole estate.

Isolated by design

One tenant's subscriber gallery and 1:N watchlist are **never visible to, or matched against,** another tenant's. Data, users and audit trail stay separate.

Branded per tenant

Each tenant's SDK instance carries its own visual identity and OEM presentation — **configured, not rebuilt** for every brand you add.

Configured per tenant

Journey steps, document rules, approval thresholds, workflow rules and user access are set **independently for each tenant.**

WHAT EACH TENANT CONTROLS	WHAT STAYS CENTRAL
Its own brand — logo, colours and subscriber-facing journey	**Estate-wide oversight** — activity across every tenant in one console
Its own risk appetite — thresholds, approval and review rules	**One platform to operate** — a single deployment, support model and upgrade path
Its own data — subscriber gallery, watchlist, users and audit trail	**Usage and billing** — tracked by tenant, channel and service for cost allocation or partner billing

WHO RUNS AS A TENANT

- Other group operating companies
- Mobile money and fintech arms
- Resellers on-selling verification as a service
- MVNOs hosted on your network
- Dealers, distributors and channel partners
- Separate brands and sub-brands in one market

The second tenant costs less than the first.

Multi-tenancy, sub-OEM branding and per-tenant usage tracking are **platform capabilities, not a bespoke build.** Because tenants share the underlying infrastructure and support model, a second or third operator is materially cheaper and faster to bring live than the first — which is what makes on-selling the SDK commercially workable, not just technically possible.

HOW IT IS STRUCTURED

One deployment
Shared infrastructure, support model and upgrade path · central oversight and per-tenant usage tracking

TENANT A	TENANT B	TENANT C	TENANT D
Home market operator	**Second group opco**	**MVNO or fintech arm**	**Reseller or partner**
Own brand · own gallery · own rules	Own brand · own gallery · own rules	Own brand · own gallery · own rules	Own brand · own gallery · own rules

Tenants share the platform. They do not share data — galleries, watchlists, users and audit trails stay isolated.

SCALE

Isolation where it matters — shared economics where it counts.

WHERE A LICENCE CHANGES THE OBLIGATION

Screening That Finds the Name You Weren't Given.

Where regulation requires it, screening becomes a **central-bank and compliance obligation** — checked on every customer, maintained for the life of the account, and audited.

215+	**3,500+**	**50K+**	**2.6M+**	**80+**	**100K+**
SANCTION REGIMES	OFFICIAL WATCHLISTS	NEWS SOURCES	PEP PROFILES	LANGUAGES	DATA SOURCES

Beyond sanctions and PEP lists: PEP classification to Level 4, insolvent entities, historical biographies, shadow diplomats and high-risk businesses.

Name Matching That Survives Real Names

Most screening failures are matching failures, not database gaps — the right person is there under a spelling the system did not recognise. NLP, transliteration libraries and phonetic algorithms catch aliases, native-script variants and misspellings.

The Networks Behind the Named Individual

Sanctioned and politically exposed people rarely transact under their own name. Relatives, associates, financial-crime facilitators and shell-company operators are held as first-class records and linked by AI entity resolution — including local profiles global databases miss.

Hosted in country.

The screening database can be deployed **in country, inside your own environment.** No customer data leaves the jurisdiction to complete a check, and screening keeps working when cross-border connectivity does not. A cloud-only screening service cannot offer that.

Screening sources, thresholds and escalation rules are configured per market and regulator, and every hit is retained with the decision it informed.

PROOF

The AML score feeds the same composite decision as liveness and document checks — not a separate report read later.

THE CHECK A SIM SWAP CANNOT PASS

3D Facial Liveness. Virtually Unbreakable.

Backed by a $600,000 Spoof Bounty.

Every other check can be satisfied with something stolen — a real document, a real name, a real device. **Liveness is the only one that requires the actual person to be there**, proven to better than 99.999% confidence that they are physically present and the camera feed has not been tampered with.

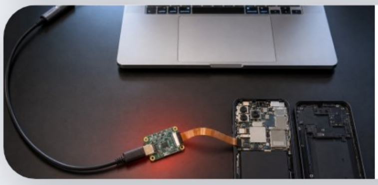
Not all liveness is comparable.

2D LIVENESS	3D FACIAL LIVENESS
Looks at the image.	**Challenges the capture.**
Analyses pixels and visible facial artefacts.	Analyses 3D session evidence, depth and capture-path integrity.

Five levels of attack. 3D Facial Liveness is built for all five.

01	Photos, screens and replayed video
02	Paper and human-worn masks
03	3D masks, dolls and lifelike replicas
04	**Synthetic data inserted into the FaceScan**
05	**Recorded or deepfake video injected into the camera path**

The first three attacks target the image. The last two target the capture itself.



When the camera feed is fake, the image can look perfect.

Software hooks and hardware adapters can replace a live camera feed with recorded or synthetic video — the rig pictured here. **In a 14-day European biometrics penetration test, nearly 1,000 injection attempts produced zero successful undetected injections.**

A certificate proves yesterday. A bounty challenges tomorrow.

The only liveness technology backed by a **$600,000 Spoof Bounty**. More than **110,000 attacks rebuffed in two years**, each analysed and any new method patched before it can scale into fraud. ENISA's 2023 report reaches the same conclusion: 3D data is needed in liveness assessment, and bounty programmes are the most effective way to test unknown threats.

A real subscriber. A trusted capture. A decision you can stand behind.

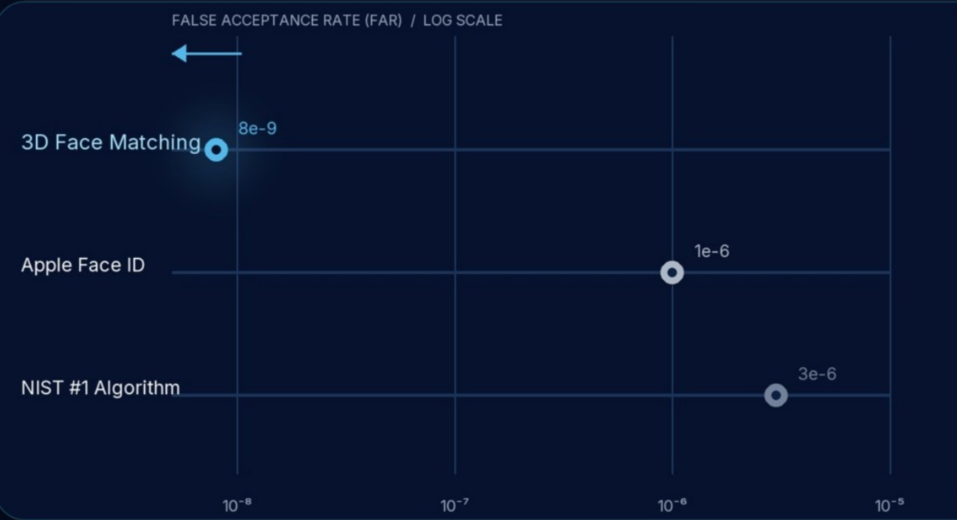
1B+	$600K	14 DAYS	0	iBeta
3D Liveness Checks	Standing Spoof Bounty	Video-Injection Testing	Undetected Injections	Level 1 & 2 PAD
Annually	Uncollected	European biometrics lab	In nearly 1,000 attempts	Independently certified

MATCHING PROOF

3D Face Matching. Up to 375× more accurate.

The right match. From the right source. A document tells you which identity is being presented. Face Matching confirms **who is presenting it** — and, for a returning subscriber, that it is the same person who registered.

THE GAP IS MEASURABLE



THE GAP IS NOT SUBTLE

125× more accurate in matching than Apple Face ID

375× more accurate in matching than NIST #1 Algorithm

3D Face Matching

0.000000008 FAR

More accurate means a lower false acceptance rate — fewer non-matches accepted as matches. Comparative values as supplied in the source material.

THREE WAYS TO MATCH

3D → 3D
Re-verification

`1 in 125 million FAR`

Approximately one false match in every 125 million comparisons. The check behind SIM swap, change of ownership and high-value approval.

3D → 2D NFC
From the chip

`1 in 2 million FAR`

The live face against the portrait extracted from the document's NFC chip. Strong assurance for chip-enabled passports and IDs.

3D → 2D ID Photo
Broad coverage

`1 in 500,000 FAR`

The live face against the portrait printed on the document. Widely deployable, strongest where the printed photo is clear.

Adaptive FaceMap

Each successful re-verification strengthens the subscriber's enrolled template. The control gets **stronger** over the life of the account, not weaker.

PROOF

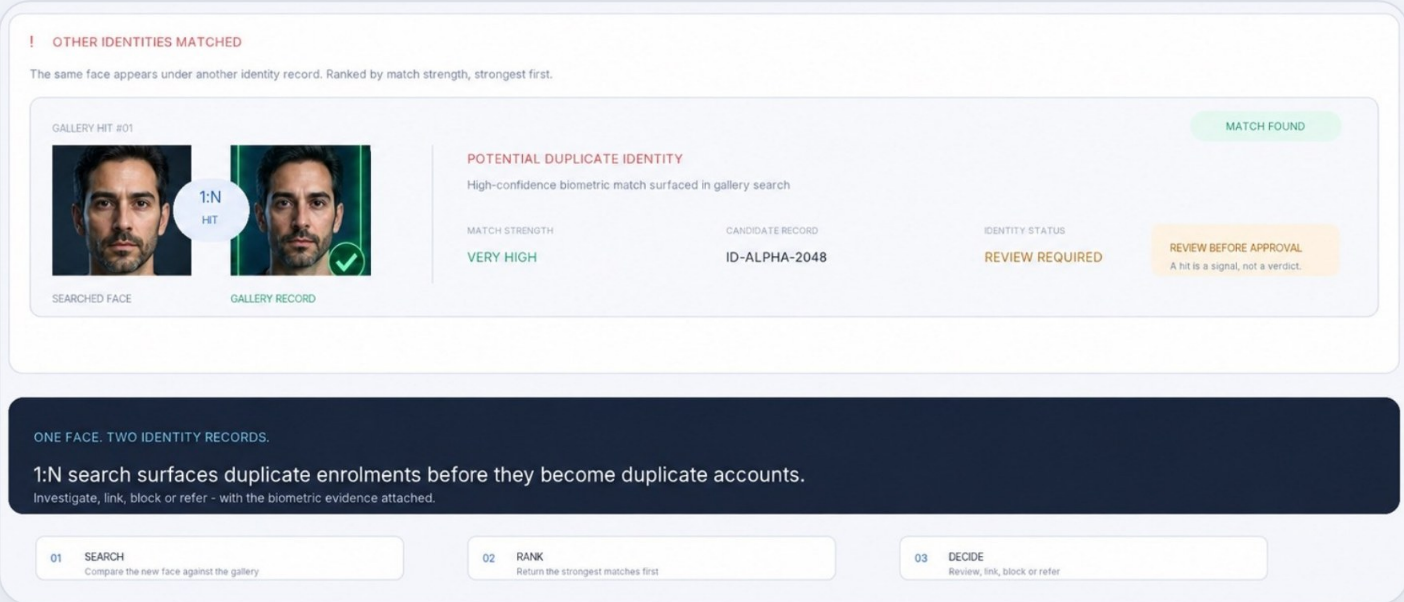
Match the subscriber to the identity. With confidence.

1:N FACE SEARCH

Same Face. Different ID.

Protection for the whole subscriber base, not one registration at a time.

A forged ID may look perfect. A real face cannot be replaced. 1:N search compares every new registration against your entire subscriber gallery, exposing when the same person attempts to register under a different identity — the check SIM registration regulation exists to require.



One person. One subscriber identity. Protect your base from:

- Duplicate registrations
- Synthetic identities
- SIM-farm enrolment
- Identity swapping
- Repeated use of the same face

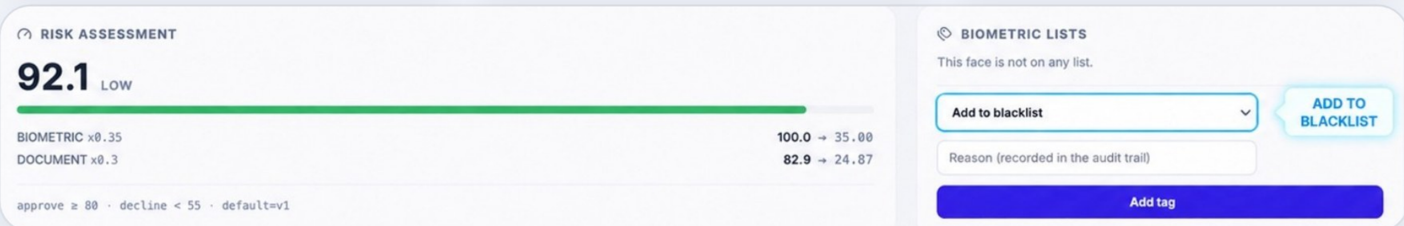
The operator keeps the policy decision — **legitimate shared, family and multi-SIM subscribers are a normal part of any base**, not fraud by default. A hit is surfaced with its evidence for review, not auto-rejected.

Built for decisive action. Configurable biometric lists.

Blacklists
Permanently block confirmed fraudsters from re-entering your subscriber base.

Grey lists
Flag suspicious identities for enhanced review, investigation or manual approval.

1:N alerts
Surface the strongest duplicate matches before a new activation is approved.



A PERFECT ID FORGERY STILL NEEDS A REAL FACE

When the same face appears under a different identity, the conflict is surfaced immediately — with the biometric evidence attached.

EIGHT SIGNALS, ONE SCORE

Eight Signals. One Defensible Decision.

Any one check can be individually defeated. **A composite score across all of them, at a threshold the operator controls, is what actually holds up.**

Capture Quality
Sharpness, framing and glare gates, so every other signal is scored from real evidence rather than a bad photograph.

Device & Network
Emulators, rooted devices, cloned hardware, VPN, proxy and anomalous-network detection.

Liveness
Spoof, injection and deepfake resistance, as a confidence score rather than a standalone gate.

Document Authenticity
OCR, MRZ, NFC and forensic checks combined into a single authenticity score.

Face-to-Document Match
Sub-second 1:1 scoring, weighted alongside liveness rather than evaluated in isolation.

Biometric Watchlists & Fraud Lists
Every applicant checked against known high-risk individuals; repeat attempts and associated identities detected, then blocked, escalated or referred.

Address & Geolocation
Session location and claimed address cross-checked in real time.

Duplicate Identity Search
1:N against the enrolled base, with ranked biometric evidence.

APPROVE
All required checks clear the configured threshold.

REFER
Borderline or conflicting signals route with their evidence.

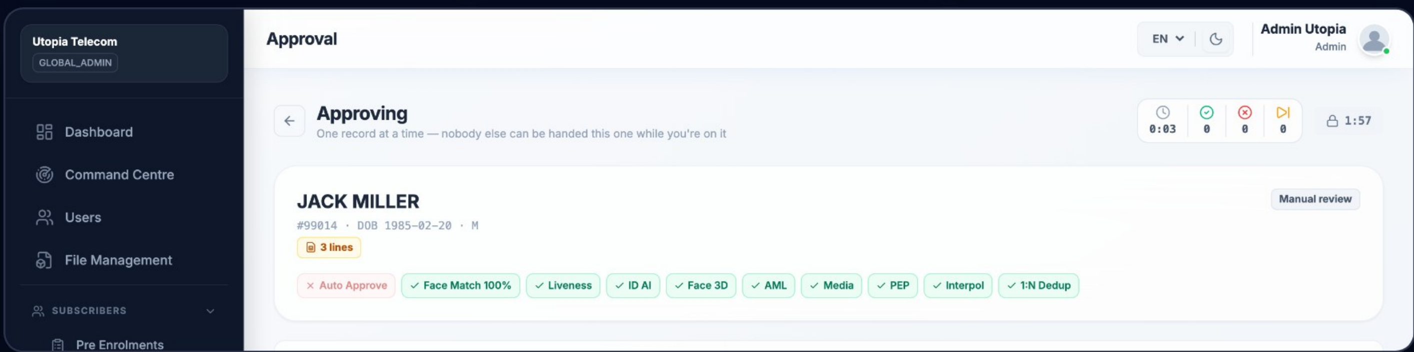
DECLINE
Hard failures and high-risk results stop the transaction.

ASSURANCE TIERS — THE OPERATOR SETS WHICH SIGNALS RUN WHERE

LOW FRICTION
Digital self-service
2D/3D liveness · document · device intelligence

BALANCED
Dealer & retail
3D liveness · document · 1:N · optional fingerprint

MAXIMUM
SIM swap & high value
3D liveness · 3D:3D · document + NFC · device signature



APPROVAL REVIEW — THE COMPOSITE DECISION, ITS CONTRIBUTING SIGNALS, AND THE REASON RECORDED AGAINST IT

PROOF
Approve, decline or refer — with a reason attached and the evidence retained.

THE PART THAT MATTERS EIGHTEEN MONTHS LATER

Every Action Recorded. Nothing Altered.

An activation or a SIM swap has to stand up later — in care, a dispute, a fraud investigation, an internal audit or a central bank review. **The evidence is created as part of the transaction, not reconstructed afterwards.**

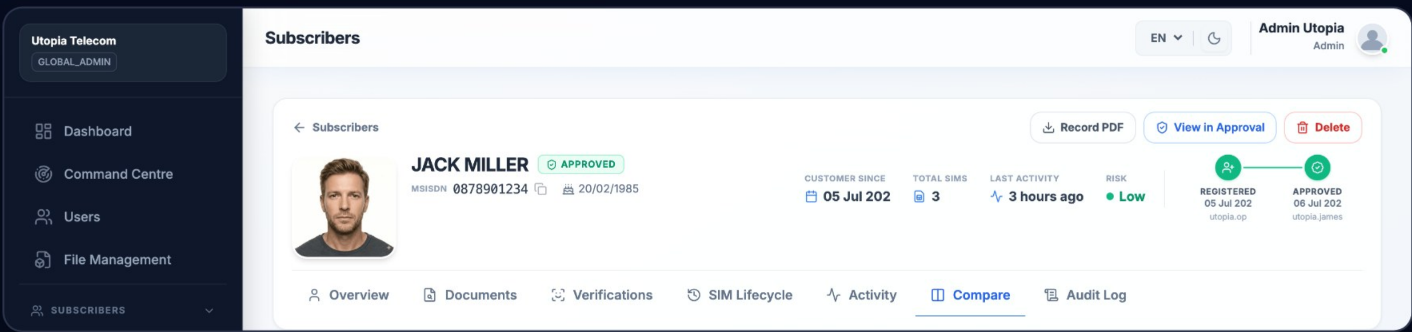
CONTROL	HOW IT WORKS
Complete record	Every check, result and piece of evidence kept against the subscriber record.
Append-only audit	Records cannot be updated or deleted. Each is hash-chained to the one before it, so a removal is detectable rather than merely forbidden.
Access is an event	Reading a subscriber's biometric is recorded like any other action, with the operator, the time and a stated reason.
Retention you set	Evidence and audit records each have their own retention period, applied automatically.
Role-based, tenant-separated	Scope resolved from the caller's own token — a dealer cannot widen its own view by asking differently.

Session View

The decision and the checks that produced it; evidence and confidence per check; document fields tagged by source; every 1:N gallery hit, not only the strongest; a timeline; and who has *seen* the result.

Search & Export

Filter by outcome, date, document type, dealer, branch or operator; open any session; export what a regulator or an internal audit has asked for.



OPERATOR CONSOLE — EVIDENCE, COMPARISON AND AUDIT AGAINST EVERY SUBSCRIBER RECORD

PROOF

Tamper-evident by design — the layer that gives compliance, risk and the regulator a reason to say yes.

WHY AXON

Proven at Subscriber Scale.

Running subscriber identity and registration programmes for mobile network operators since 2005 — across digital, dealer and field channels, where the identity decision has to become a live subscriber.

350M+	500M+	20+	15+	20+
SIM CARDS REGISTERED	IDENTITIES VERIFIED	OPERATORS & AUTHORITIES	COUNTRIES DEPLOYED	YEARS IN TELCO

That is subscriber-registration scale, not generic identity-verification scale.

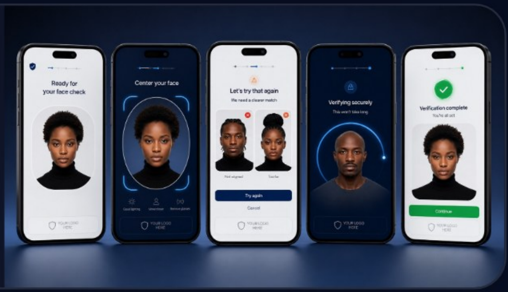
AFRICA · MIDDLE EAST · ASIA · TELECOMS · MOBILE MONEY · GOVERNMENT

ON-PREMISES & SOVEREIGN DEPLOYMENT

Built, Delivered and Supported by Axon.

Hosted, embedded through your app via API, private cloud, or fully on-premise where data residency requires it. **Same product, same API, same console** — the deployment model changes, the verification does not.

Branding, thresholds and approval rules are configured per market — see page 09.



WHAT THIS IS WORTH TO AN OPERATOR

- **More activations, completed remotely** — sell and activate wherever demand appears
- **Faster onboarding, fewer abandoned signups** — less friction between intent and revenue
- **One enrolment serving SIM and wallet** — stop paying twice to verify one person
- **Fewer SIM-swap losses and complaints** — and the reputational damage that follows them
- **No repeat ID checks for trusted subscribers** — servicing without a store visit
- **A base protected network-wide** — 1:N, lists and evidence across every registration

Activate More Customers. Reduce SIM-Swap and Impersonation Risk. Reuse Trusted Identity Across Every Subscriber Journey.

One trusted identity layer for eSIM activation, subscriber onboarding, account recovery, mobile money and ongoing authentication.

Book a demonstration or start an evaluation.

Scope, fees and deployment model are confirmed at solution design; pricing sits in the Axon commercial proposal.

sales@axonwireless.com · axonwireless.com