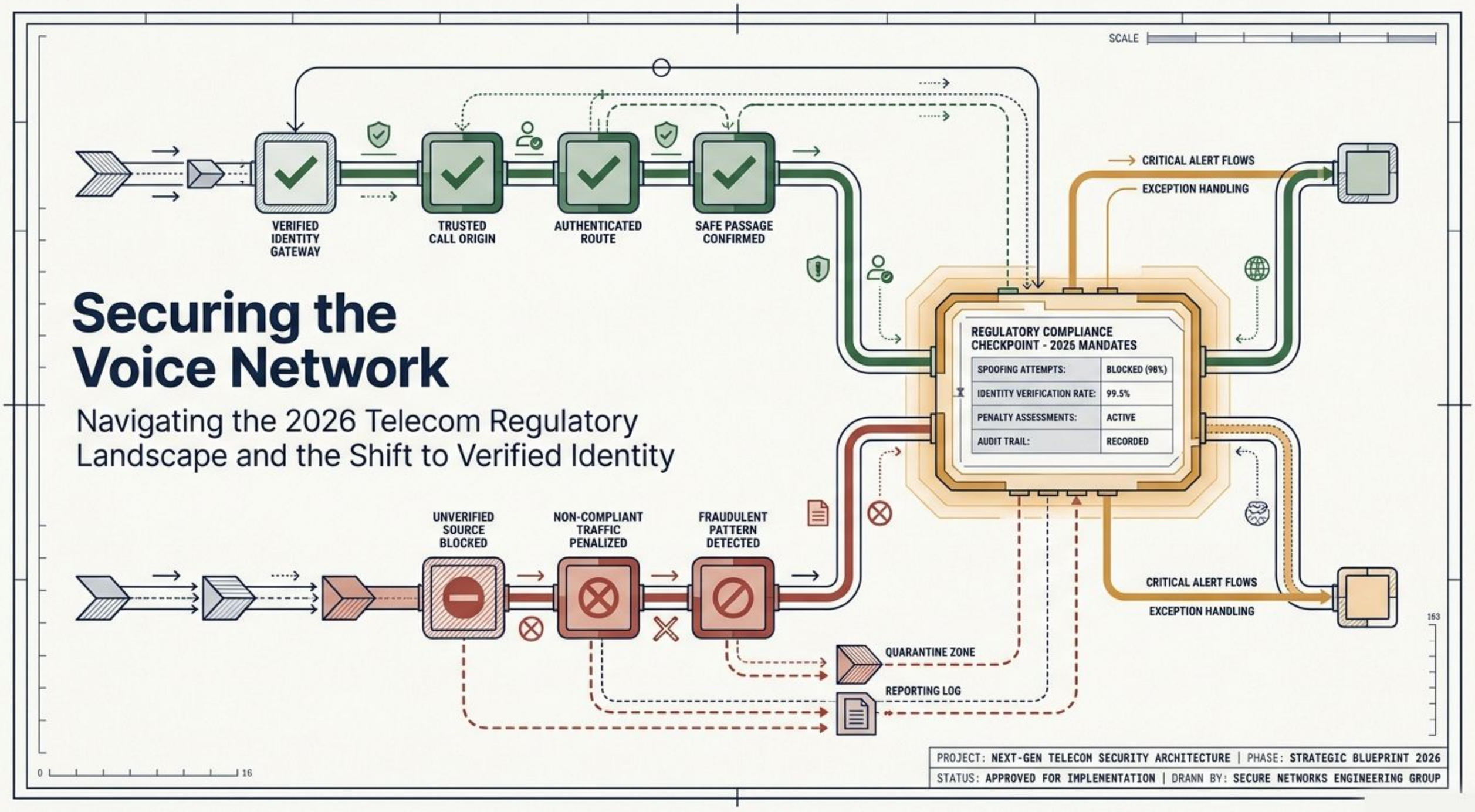
VERIFIED VOICE

Restoring Trust in Voice Communications:
A Solution Blueprint for Identity Security in Telecommunications


SCALE
VERIFIED IDENTITY GATEWAY
TRUSTED CALL ORIGIN
AUTHENTICATED ROUTE
SAFE PASSAGE CONFIRMED
CRITICAL ALERT FLOWS
EXCEPTION HANDLING
Securing the Voice Network
Navigating the 2026 Telecom Regulatory Landscape and the Shift to Verified Identity
REGULATORY COMPLIANCE CHECKPOINT - 2025 MANDATES
SPOOFING ATTEMPTS: BLOCKED (98%)
IDENTITY VERIFICATION RATE: 99.5%
PENALTY ASSESSMENTS: ACTIVE
AUDIT TRAIL: RECORDED
UNVERIFIED SOURCE BLOCKED
NON-COMPLIANT TRAFFIC PENALIZED
FRAUDULENT PATTERN DETECTED
CRITICAL ALERT FLOWS
EXCEPTION HANDLING
QUARANTINE ZONE
REPORTING LOG
0
16
153
PROJECT: NEXT-GEN TELECOM SECURITY ARCHITECTURE | PHASE: STRATEGIC BLUEPRINT 2026
STATUS: APPROVED FOR IMPLEMENTATION | DRANN BY: SECURE NETWORKS ENGINEERING GROUP

Restoring Trust in the Voice Channel: The Shift to Verifiable Identity

THE TRUST GAP: WHY CURRENT SYSTEMS FAIL

Knowledge-Based Authentication is Obsolete

Traditional security questions force users to disclose sensitive data, creating privacy risks and liability.

$1 TRILLION
Global Annual Losses

Industrialized fraud and scams caused massive financial damage in 2024, with only 4% recovered.

Caller ID is Easily Spoofed

Modern interconnected networks allow attackers to impersonate brands, eroding consumer trust in voice calls.

THE VERIFIABLE SOLUTION: SECURE & SEAMLESS

SIM-Based Root of Trust

Telcos use real-time network signals (like SIM swap detection) to anchor digital identities.

Decentralized "Yes/No" Verification

Users share cryptographic proofs from digital wallets without revealing unnecessary personal information.

Two-Way Authentication (VVP)

The Verifiable Voice Protocol allows both callers and callees to prove their identities simultaneously.

OPERATIONAL EFFICIENCY & SECURITY COMPARISON

Metric	Traditional Authentication	Verifiable Voice Future
Average Verification Time	4 – 5 Minutes ✗	Seconds ✓
Estimated Call Center Cost	$0.75 – $1.50 per minute ✗	Significantly Lowered ✓
Primary Security Vector	Stolen Data & Spoofing ✗	Cryptographic Proof (DID) ✓

Trust Under Siege: The Catalyst for Aggressive FCC Action

THE THREAT:

1 in 4 Americans hit by AI deepfake voice calls.

THE PERCEPTION:

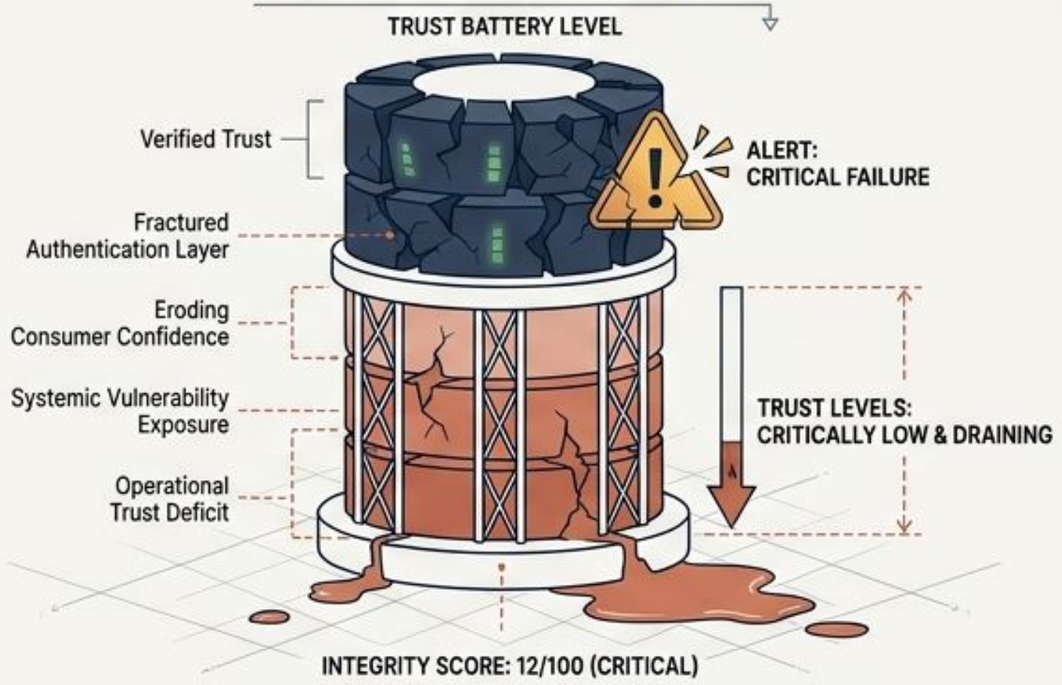
Consumers report scammers are beating mobile network operators

2-to-1.

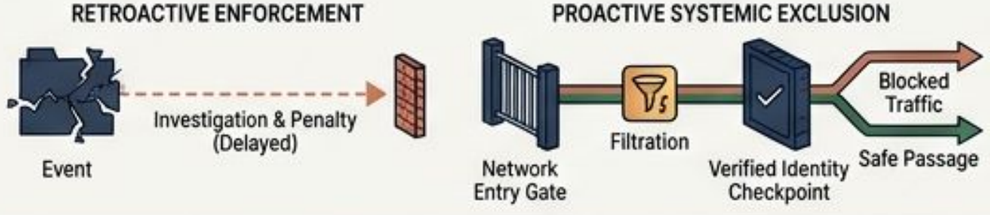
THE BUSINESS IMPACT:

38% of consumers are ready to switch providers due to frustration.

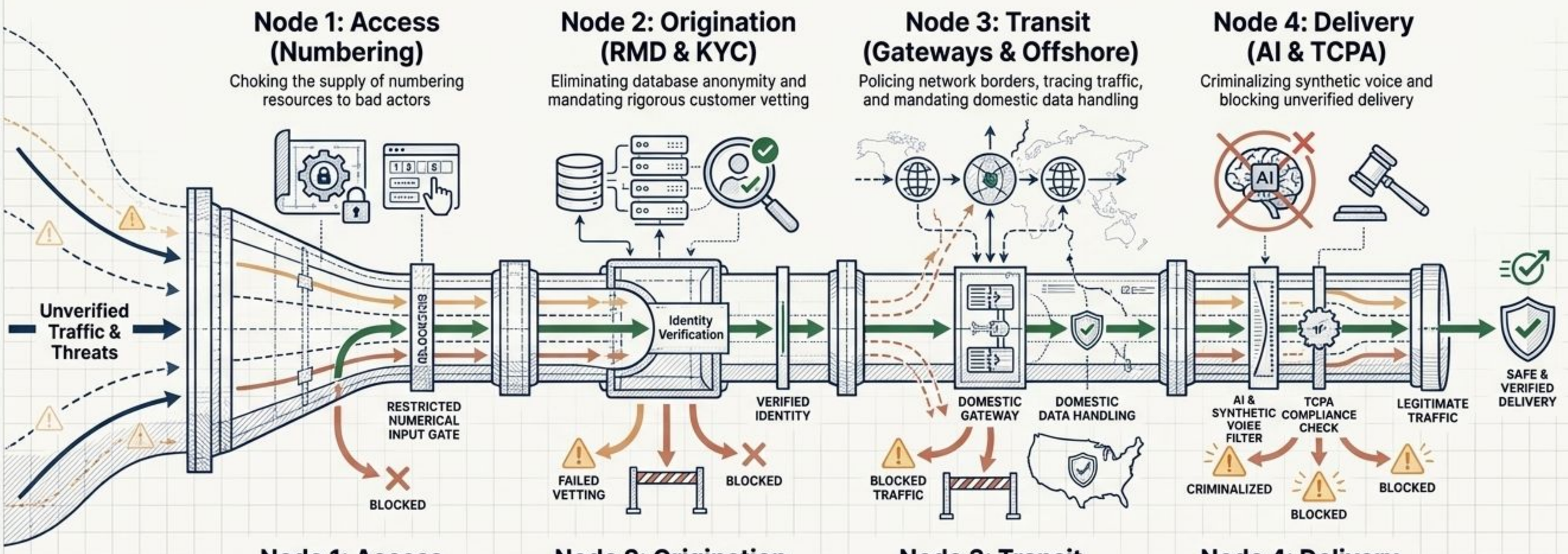
NETWORK INTEGRITY METER



The FCC's response is a **total architectural overhaul**—shifting from retroactive enforcement to proactive, systemic network exclusion.



Defense in Depth: The Four-Node Regulatory Gauntlet



Node 1: Access (Numbering)
Choking the supply of numbering resources to bad actors

Node 2: Origination (RMD & KYC)
Eliminating database anonymity and mandating rigorous customer vetting

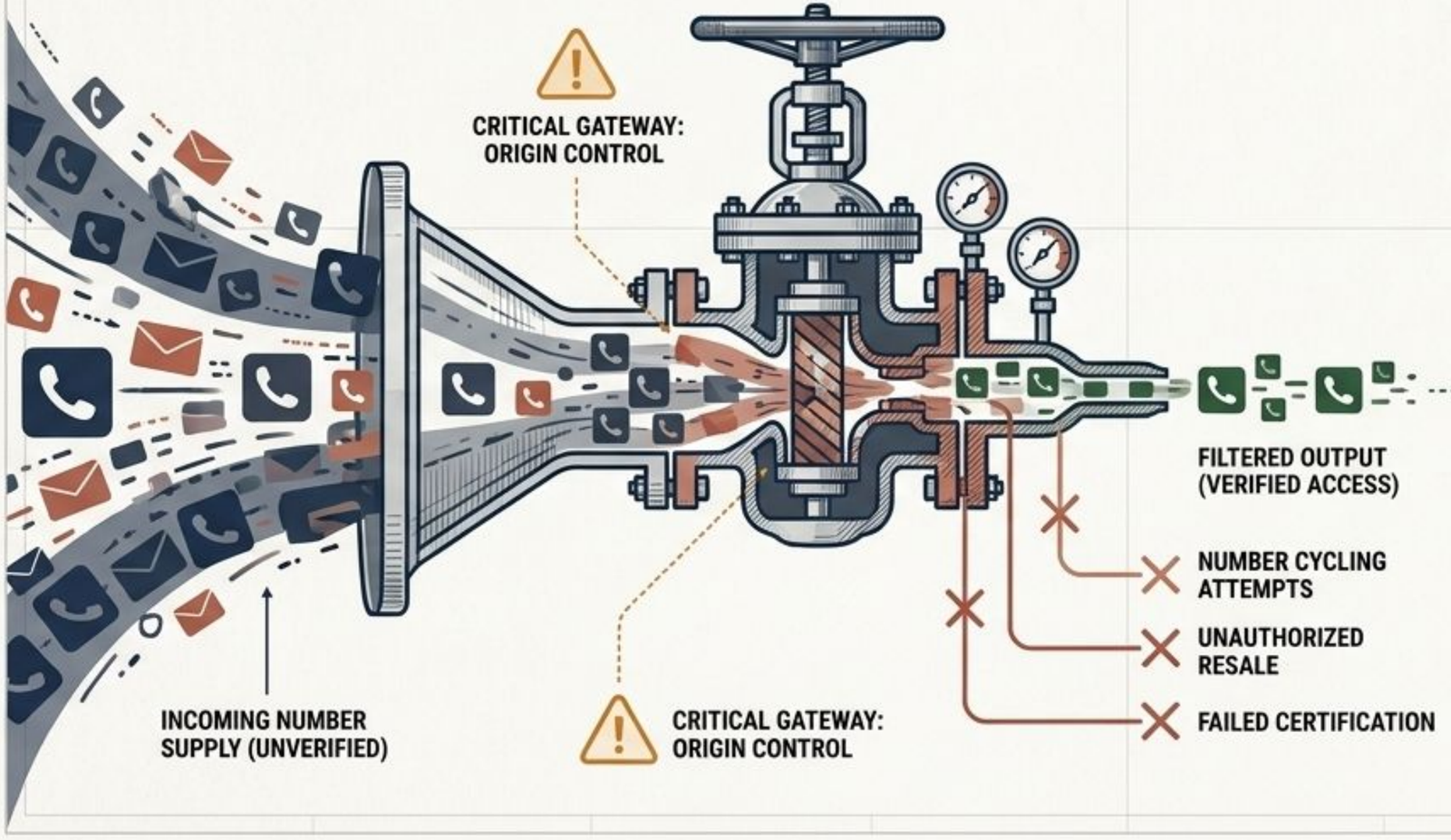
Node 3: Transit (Gateways & Offshore)
Policing network borders, tracing traffic, and mandating domestic data handling

Node 4: Delivery (AI & TCPA)
Criminalizing synthetic voice and blocking unverified delivery

Deep Forest Green: Verified Identity & Safe Passage
Muted Terracotta: Blocked Traffic & Penalties
Architectural Amber: Alerts & Critical Checkpoints

NEWS FROM THE FEDERAL COMMUNICATIONS COMMISSION

Node 1: Access — Choking the Supply of Telephone Numbers



The Target: Number Cycling

The FCC is cracking down on scammers churning through large quantities of numbers on a rotating or single-use basis to evade detection.

The Mechanism: Expanded Certification

Robocall certification requirements are now extended to all providers receiving numbering resources, including indirect recipients and resellers.

The Impact: Absolute Origin Control

Enhanced reporting forces transparency into exactly how numbers are resold and utilized, attacking the illegal robocall lifecycle at its absolute origin.

Node 2: Origination — The End of Database Anonymity

Strict Time Limits

Filers must update any information in the CORES registration system system within 10 business days of a change.

Annual Recertification

Providers must actively recertify annually by March 1, accompanied by a $100 filing fee.

Hardened Access

Mandatory two-factor (or more) authentication (2FA) for RMD access to validate email addresses and tie corporate policies to individuals.

Red-Light Rule

RMD access is conditional; providers with non-tax debt to the FCC face rescission of their filing capability.

Node 2: Origination — Enhanced Know-Your-Customer (KYC)

Baseline KYC Requirements

- Name, Physical Address (no virtual offices/PO boxes).
- Government Issued ID Number.
- Alternative Telephone Number.

High-Volume / Foreign Caller KYC

- Intended use of service (marketing, education, political).
- Customer's IP address from which calls are placed.
- Proof of good standing/corporate formation records.

The Retention Rule: Providers must retain KYC information and supporting records for four years following the termination of the customer relationship to allow for statute of limitations investigations.

The Penalty Ledger: Monetizing Compliance Failures

Violation	Penalty
Submitting false or inaccurate information to the RMD.	**$10,000** base forfeiture (assessed on a continuing daily basis until cured).
Failure to update RMD/CORES information within 10 business days.	**$1,000** base forfeiture (continuing violation).
Violation of KYC verification rules (originating illegal traffic).	**$2,500** base forfeiture per call.

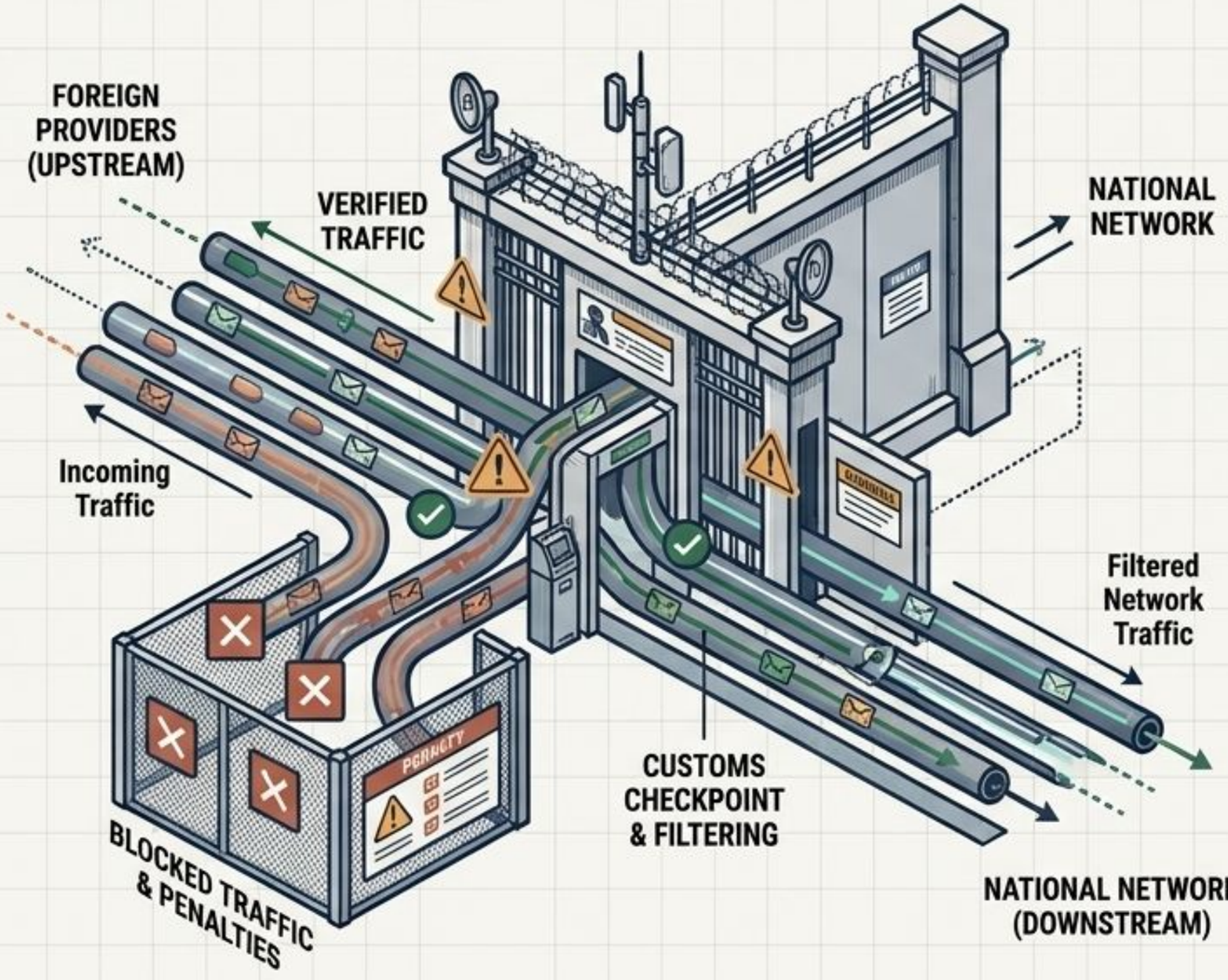
Key Insight: By shifting to a per-call forfeiture for KYC failures, the FCC ensures penalties scale destructively with the volume of illegal traffic, eliminating the cost of doing business loophole for non-compliant providers.

Node 3: Transit — Policing the Borders (Gateway Providers)

PUBLIC NOTICE

Federal Communications Commission
45 L Street NE
Washington, DC 20554

News Media Information 202-419-6300
Internet: www.fcc.gov



1. Traceback Mandate

Gateway providers must respond to robocall traceback requests within 24 hours.

2. Know Your Upstream

Mandatory reasonable steps to ensure immediate upstream foreign providers are not transmitting illegal robocalls, formalized in mitigation plans.

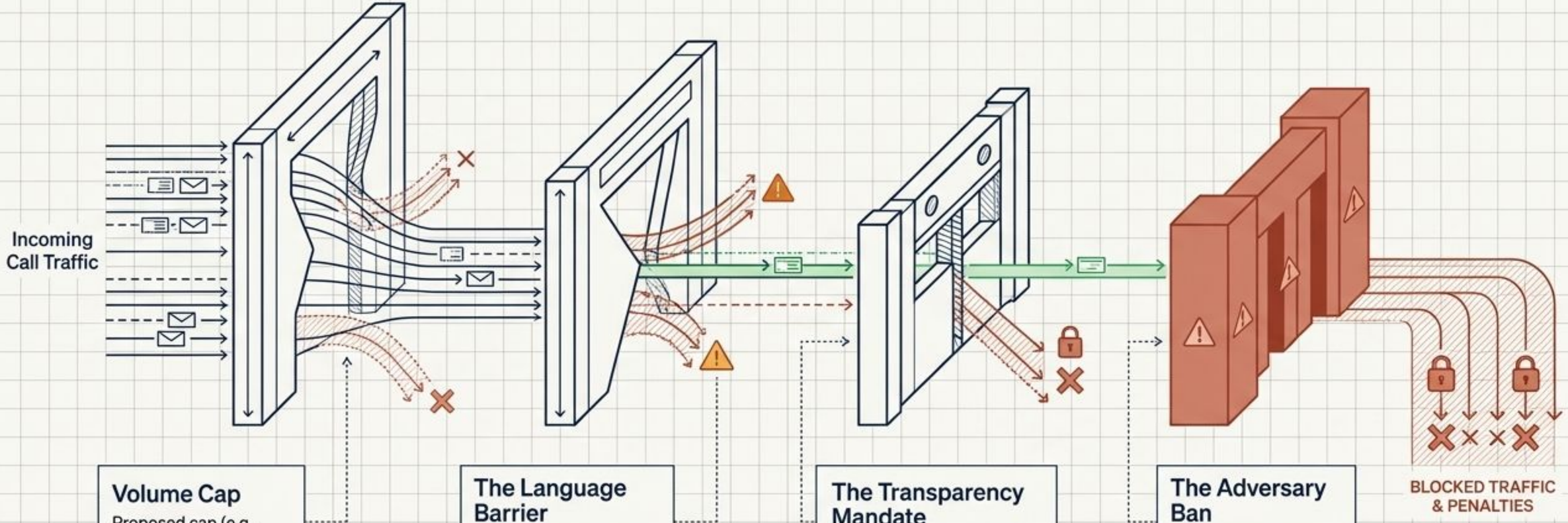
3. Mandatory Blocking

Must block illegal traffic within 14 days of an FCC Notification of Suspected Illegal Traffic and utilize a reasonable Do-Not-Originate list.

4. Authentication Limits (Sept 2025)

Providers must make their own STIR/SHAKEN attestation decisions and sign calls using their own certificate, not a third party's.

Node 3: Transit — The Offshore Call Center Squeeze



Volume Cap

Proposed cap (e.g., 30%) on the percentage of customer service calls routed to foreign centers.

The Language Barrier

Mandatory proficiency in spoken and written American Standard English, including tone and cultural context.

The Transparency Mandate

Required up-front disclosure of the foreign location and the immediate right to transfer to a U.S.-based representative.

The Adversary Ban

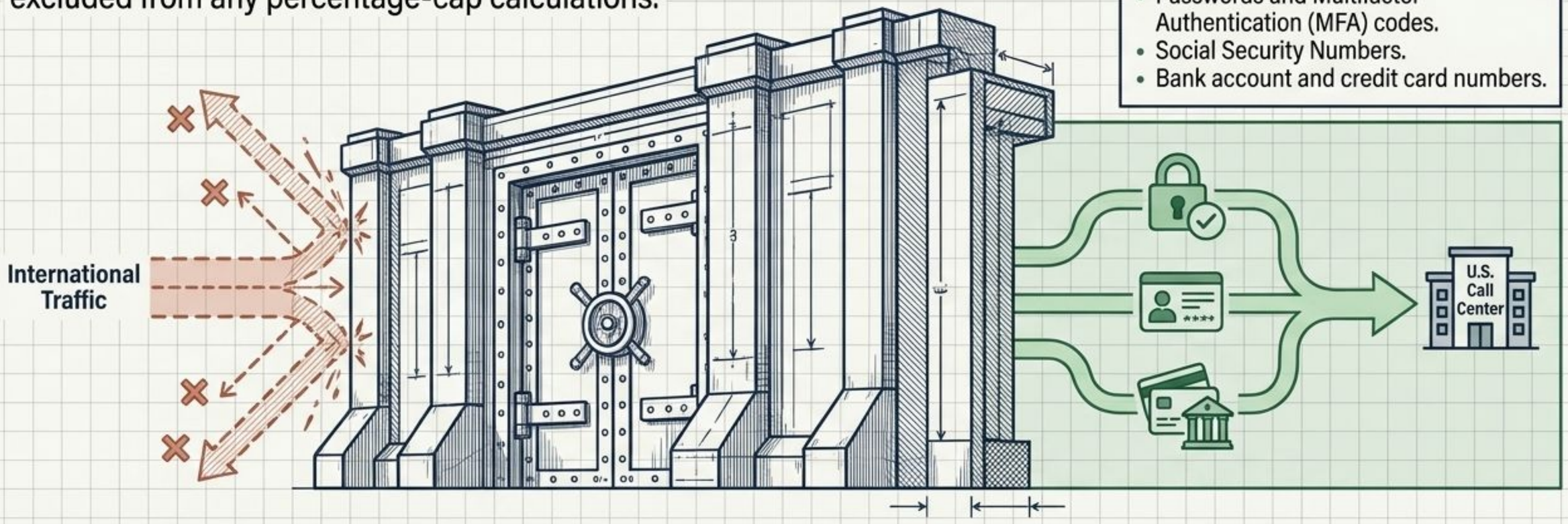
Complete prohibition on using call centers located in, or employing citizens of, foreign adversary nations (e.g., China, Russia, Iran).

The Data Sovereignty Firewall

The Mandate: U.S.-based call centers must exclusively handle customer interactions involving sensitive data. This is an absolute requirement, excluded from any percentage-cap calculations.

Covered Data Includes:

- Passwords and Multifactor Authentication (MFA) codes.
- Social Security Numbers.
- Bank account and credit card numbers.



Omnichannel Scope: This requirement is not just voice—it applies across chat, email, text, and video conferencing.

Node 4: Delivery — Criminalizing Synthetic Voice

FCC NEWS from the Federal Communications Commission

The Ruling

AI-generated voices are officially classified as artificial under the Telephone Consumer Protection Act (TCPA).

The Mechanism

Voice cloning technology used in common robocalls requires prior express written consent from consumers before calling.

The Enforcers

Empowers 48 State Attorneys General with civil enforcement authority, expanding legal avenues to target the technology used rather than just the fraud perpetrated.

The Judicial Twist: Legal Consent vs. Network Access

The Legal Win (TCPA)

January 24, 2025: The 11th Circuit vacates the FCC's 1-to-1 consent rule.

Result:
Consumers do not need to independently consent to every individual seller. Lead generation and comparison shopping models are preserved.

The Network Reality (FCC)

2025-2026: FCC drastically tightens numbering, KYC, and transit rules.

Result: Network borders are closing.

Legal consent to market is useless if you cannot access the network. Bare-minimum compliance will no longer guarantee call delivery.

The Identity Imperative: A Paradigm Shift

FCC NEWS from the Federal Communications Commission

The Old Paradigm

Identity Standard
Database Anonymity & Basic Vetting.

Call Authentication
Relying on 3rd party STIR/SHAKEN certificates.

Reputation Management
Reactive spam label remediation (Whack-a-mole).

Consumer Experience
Unknown 10-digit numbers.

The New Paradigm

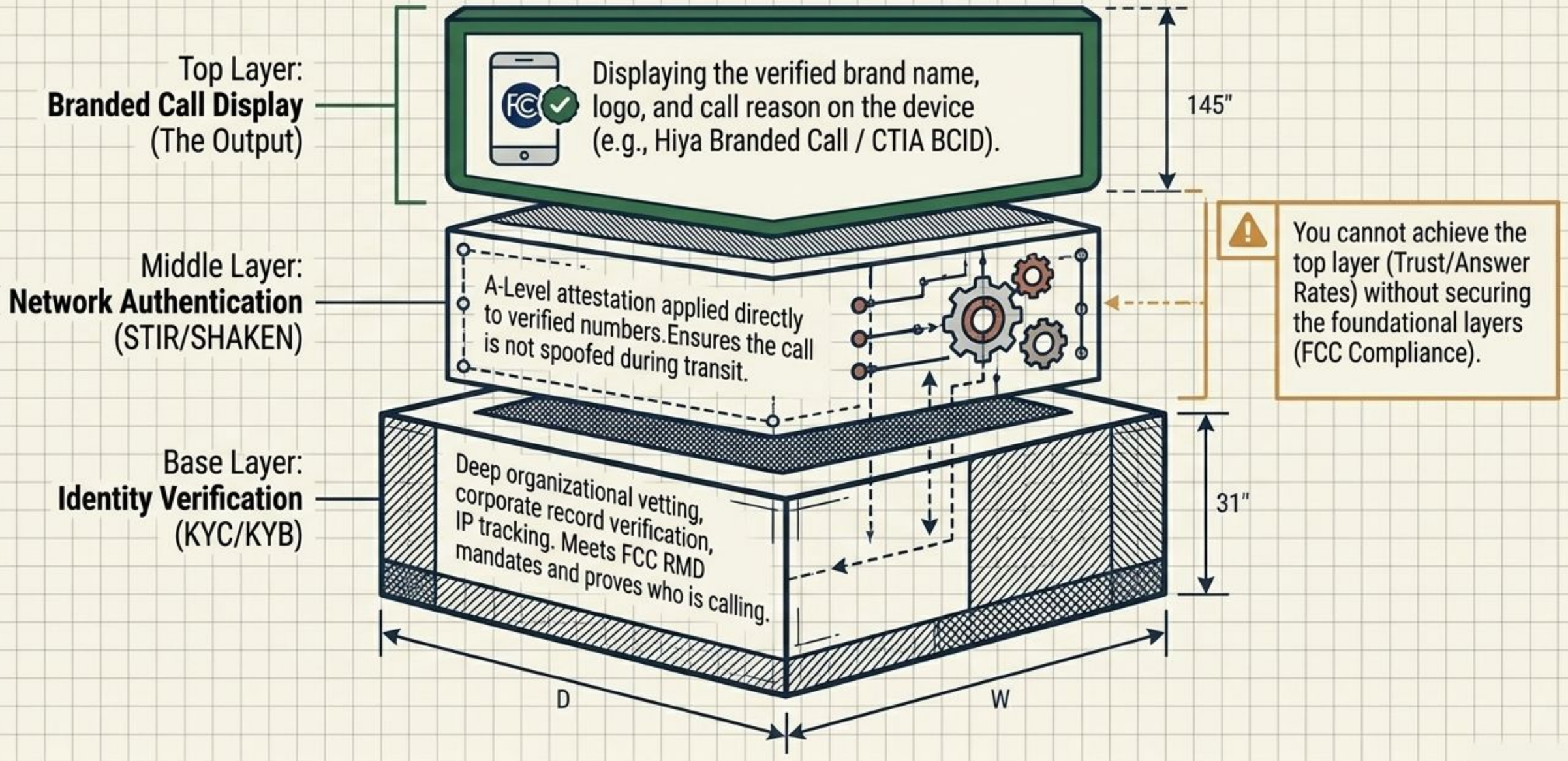
Identity Standard
KYC as a Service (KYCaaS) & Verified Entity Identity.

Call Authentication
Direct, 1st-party STIR/SHAKEN attestation.

Reputation Management
Proactive Caller Reputation monitoring (Credit score for business calls).

Consumer Experience
Secure Verified Identity Presentation (sVIP) & Branded Calling.

The New Identity Stack: From Compliance to Connection



Strategic Imperatives for 2026

1. Audit Your RMD Stance

Prepare for annual March 1 recertifications, $100 fees, 2FA implementations, and ensure 10-day CORES updates are automated.

2. Implement KYCaaS

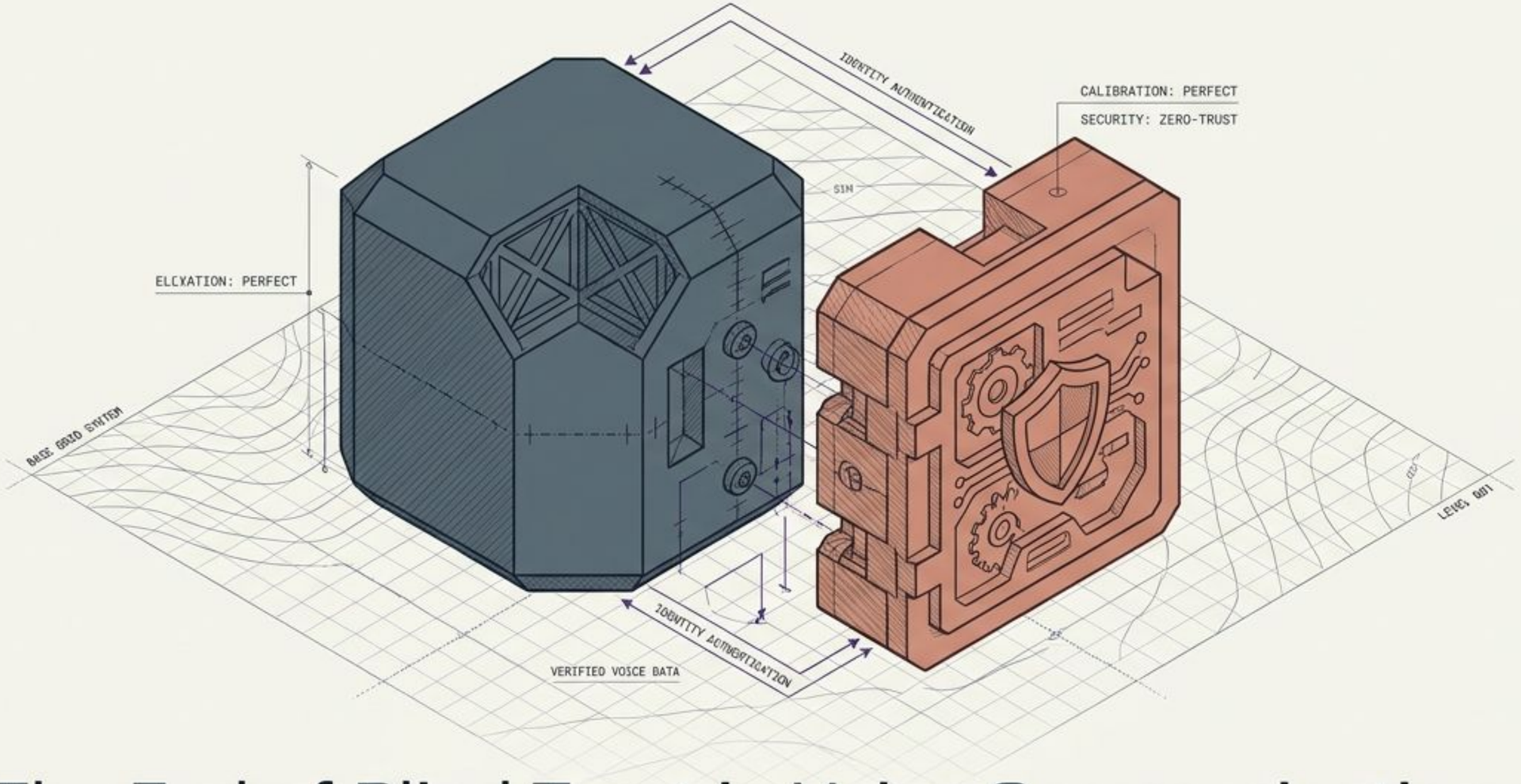
Transition from basic vetting to rigorous identity verification. Standardize collection of intended use and IP addresses for high-volume callers.

3. Audit Your Call Centers

Map your offshore routing. Prepare for 30% caps, English proficiency testing, and strictly enforce the US-based Sensitive Data Firewall.

4. Deploy Branded Calling

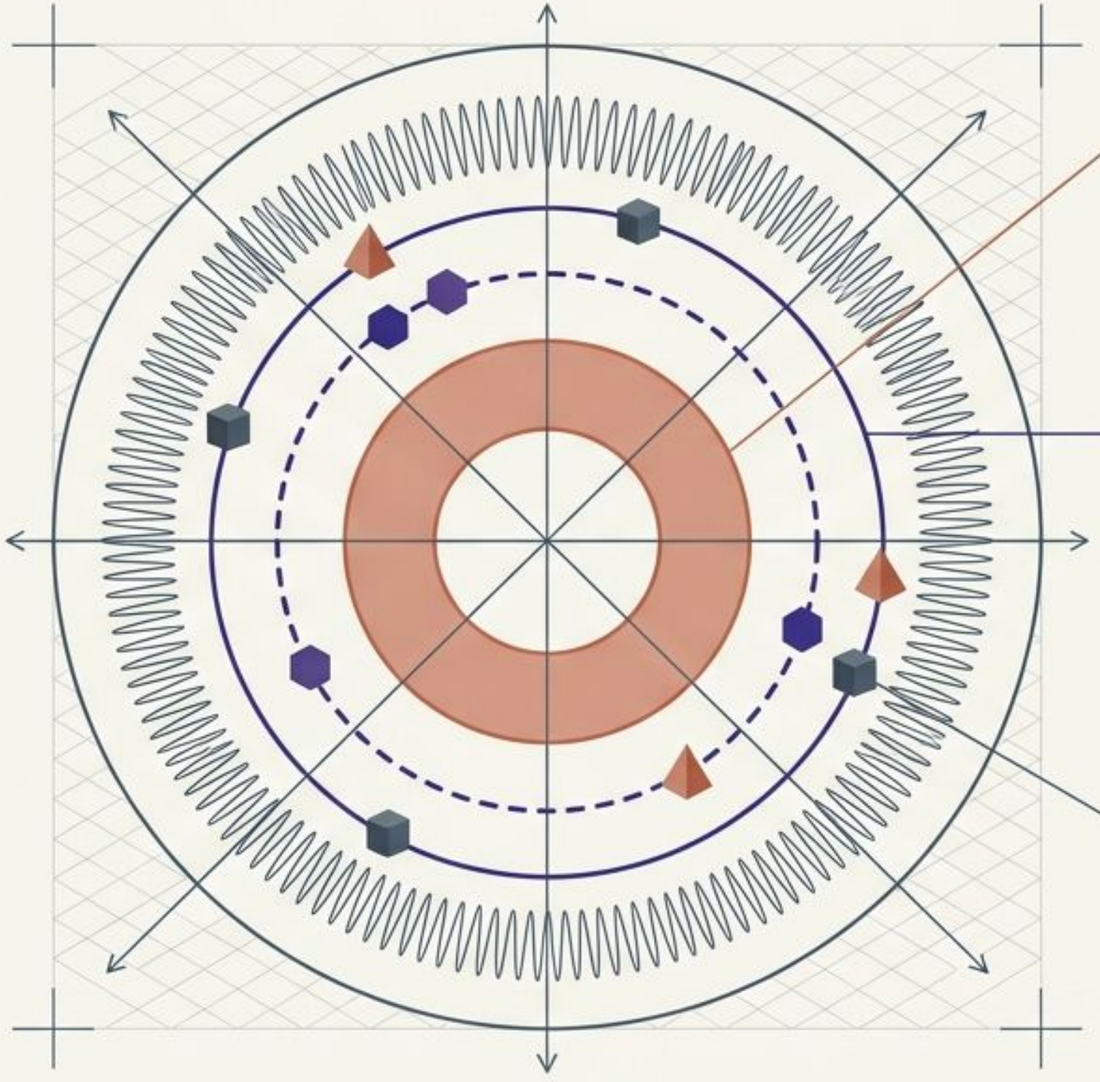
Upgrade outbound strategies from raw 10-digit dials to Branded Calling ID to bypass spam filters, restore consumer trust, and drastically improve answer rates.



The End of Blind Trust in Voice Communications

A strategic blueprint for restoring the integrity of the voice channel through Telco-rooted identity, decentralized wallets, and the Verifiable Voice Protocol.

Industrialized fraud and Generative AI have transformed voice channels into the most exploited attack surface in the world.



1. Financial Impact

> $1 Trillion global losses in 2024 (GASA estimate)

Only **~4%** of financial losses are successfully recovered.

2. Industrialized Operations

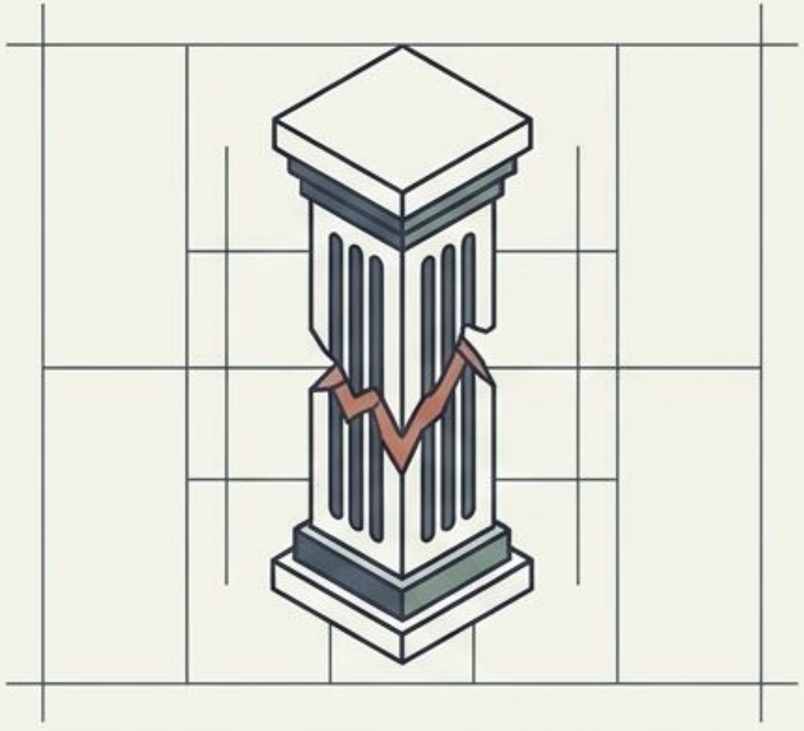
Call center fraud operations are highly organized, frequently tied to human trafficking in Southeast Asia.

Severe psychological harm impacts **>50%** of targeted adults globally.

3. AI Acceleration

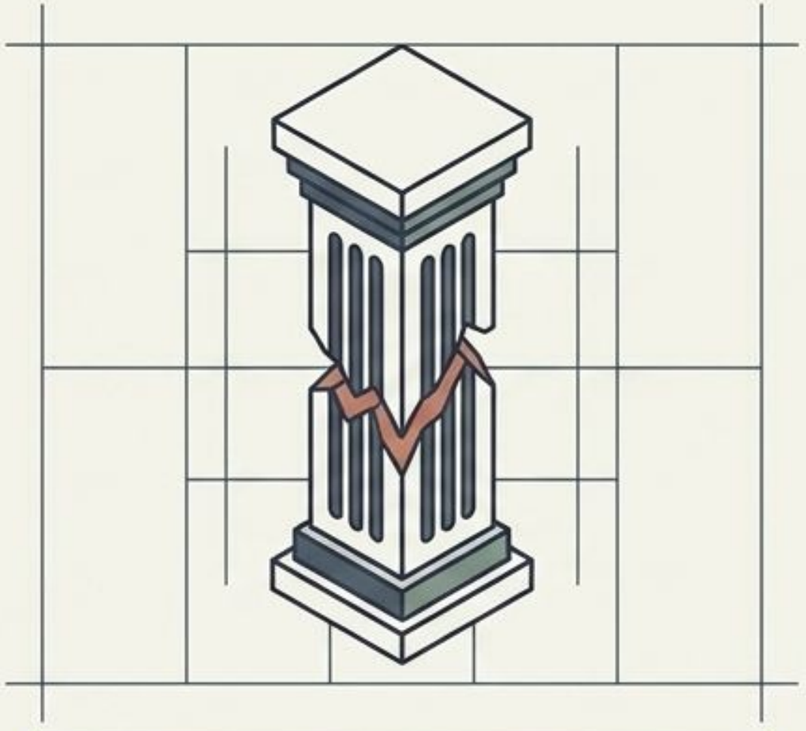
Synthetic Identity Proliferation via Generative AI allows malicious actors to iterate rapidly on real-looking synthesized voices and identities.

Legacy authentication relies on easily spoofed signals and forces mass data exposure, turning security into a profound corporate liability.



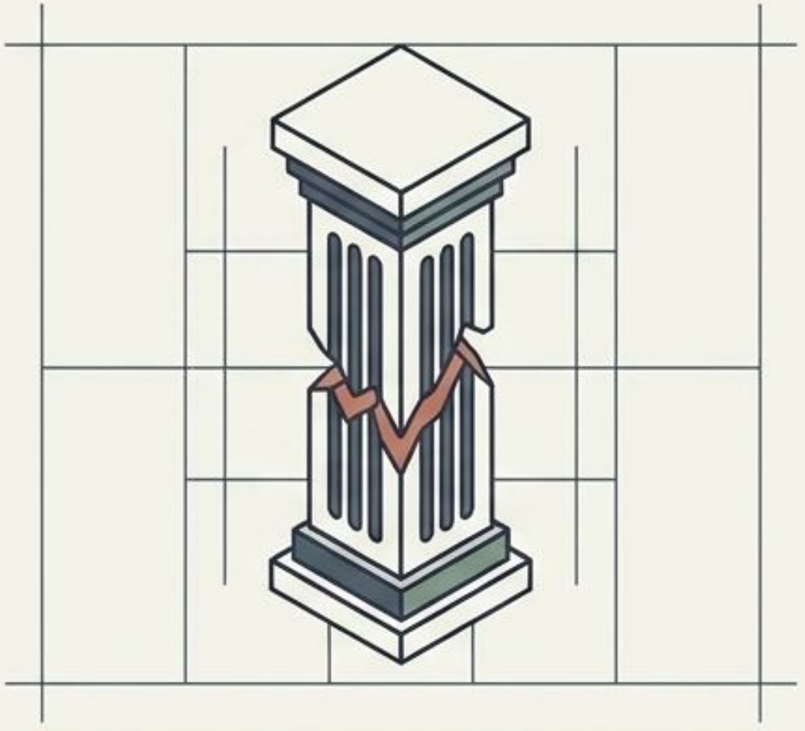
Caller Line Identity (CLI)

The Fault: CLI was designed for a closed system. On modern interconnected networks, it is easily spoofed, enabling mass impersonation without friction.



Knowledge-Based Authentication (KBA)

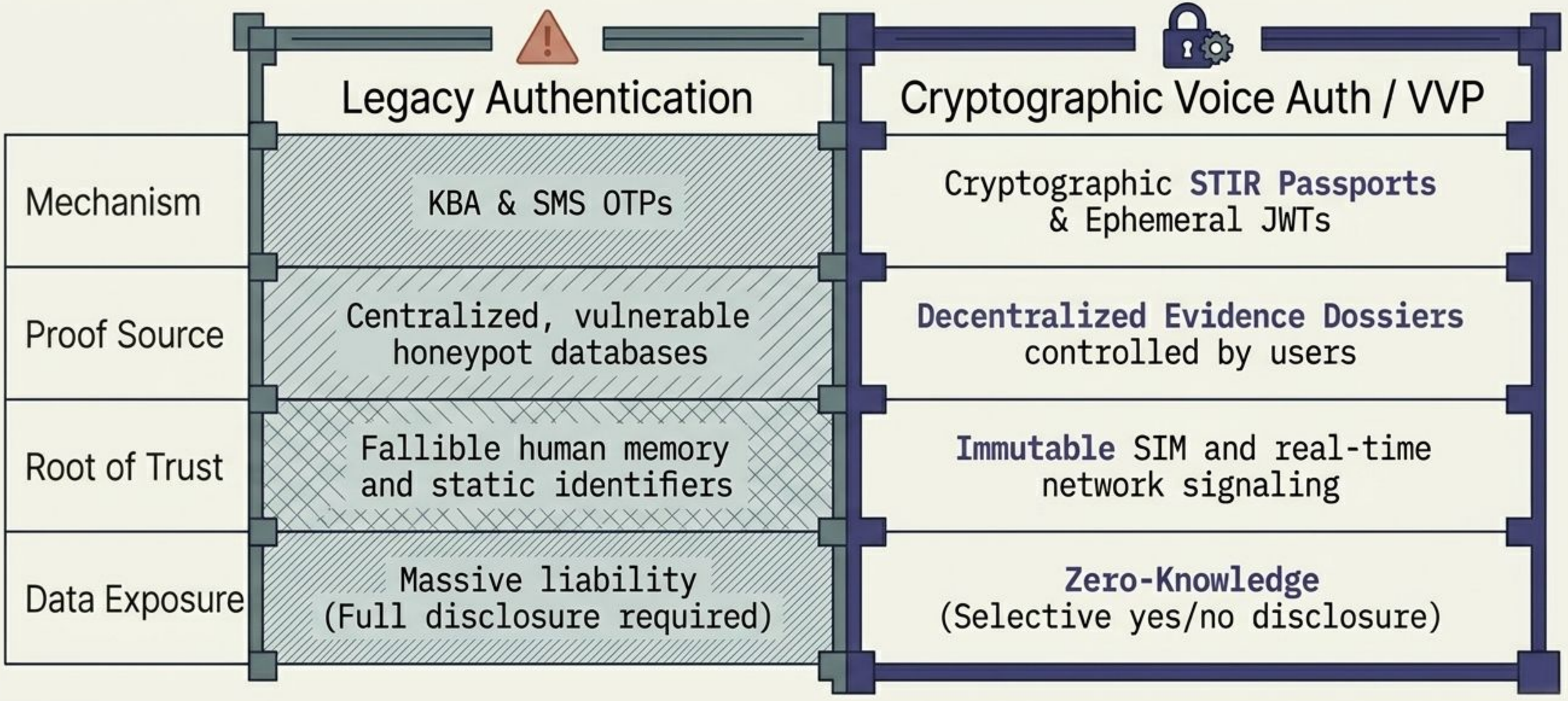
The Fault: Forces consumers to disclose sensitive data (e.g., Mother's maiden name), turning call center databases into massive honeypots and creating immense enterprise liability.



SMS One-Time Passwords (OTPs)

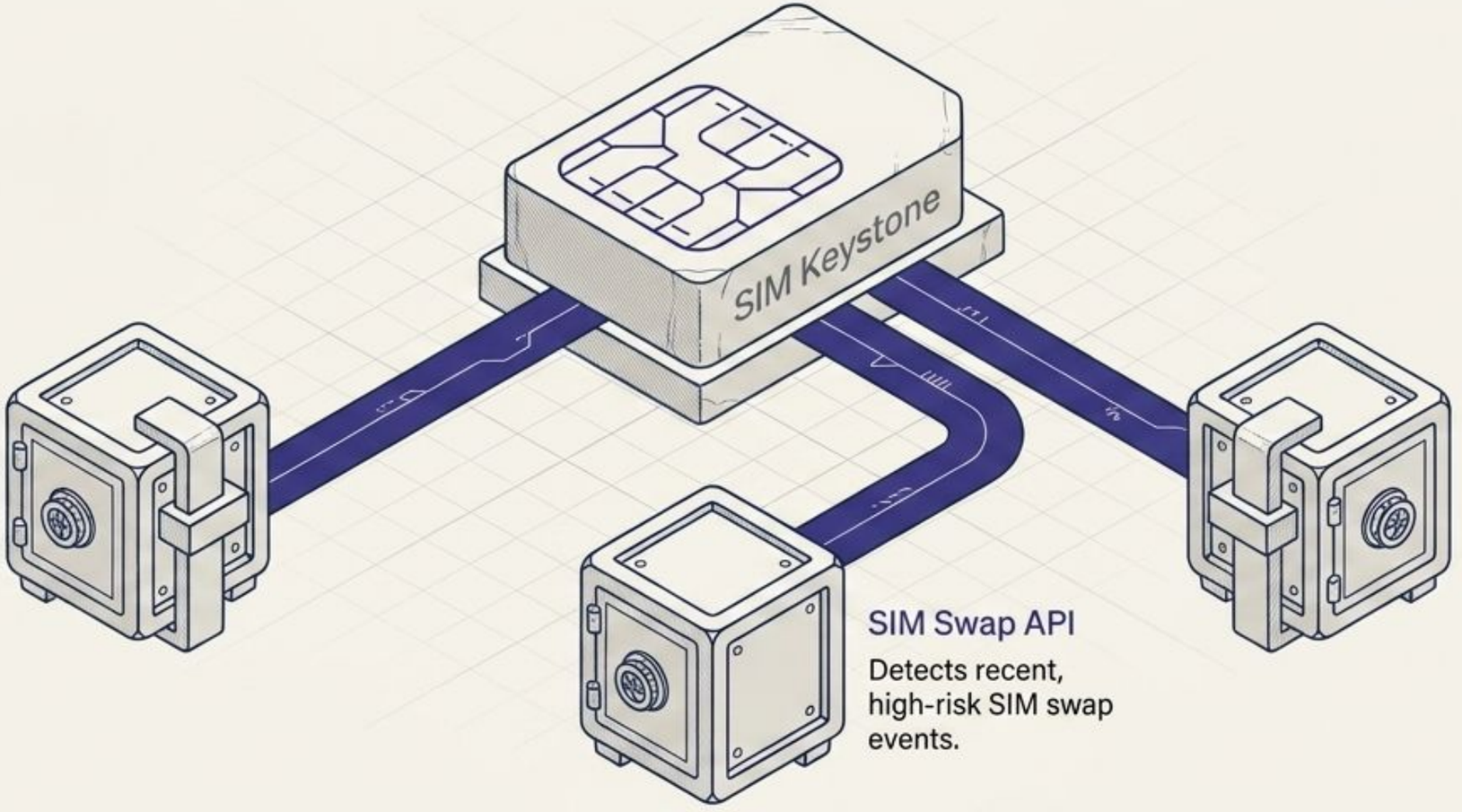
The Fault: Introduces high friction to the user experience and is increasingly vulnerable to network interception and targeted social engineering.

To secure the voice channel, the industry must transition from centralized data silos to decentralized cryptographic trust.



Mobile operators authenticate devices hundreds of times a day, making the SIM the definitive anchor for real-time digital identity.

Unlike static databases, Telcos process dynamic lifecycle events. If a number is recycled or ported, APIs instantly revoke the associated digital credentials, updating trust conditions in real-time.



Number Verification API

Confirms the user currently possesses the device and number.

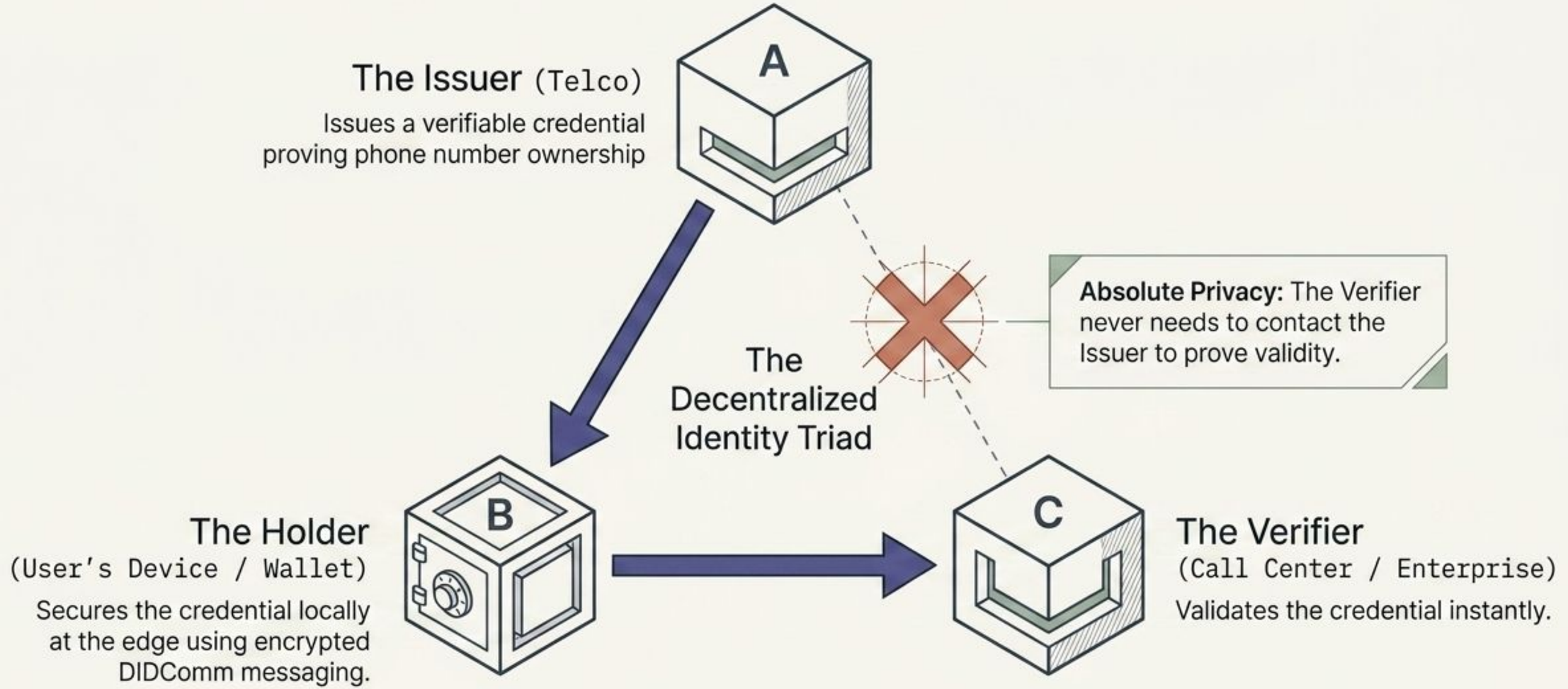
SIM Swap API

Detects recent, high-risk SIM swap events.

Network Lifecycle Events

Monitors real-time port-outs, disconnects, and number recycling.

Decentralized identity empowers users to hold their credentials locally, allowing instant verification without pinging central servers.



Under the hood, the Verifiable Voice Protocol (VVP) binds stable, cryptographic evidence directly to an ephemeral SIP INVITE.

Anatomy of a Passport

Plate 1: Cryptography

Mandates EdDSA or quantum-proof FN-DSA-512. Replay attack window clamped to an aggressive exp expiration of 15-60 seconds.

Plate 2: kid Header

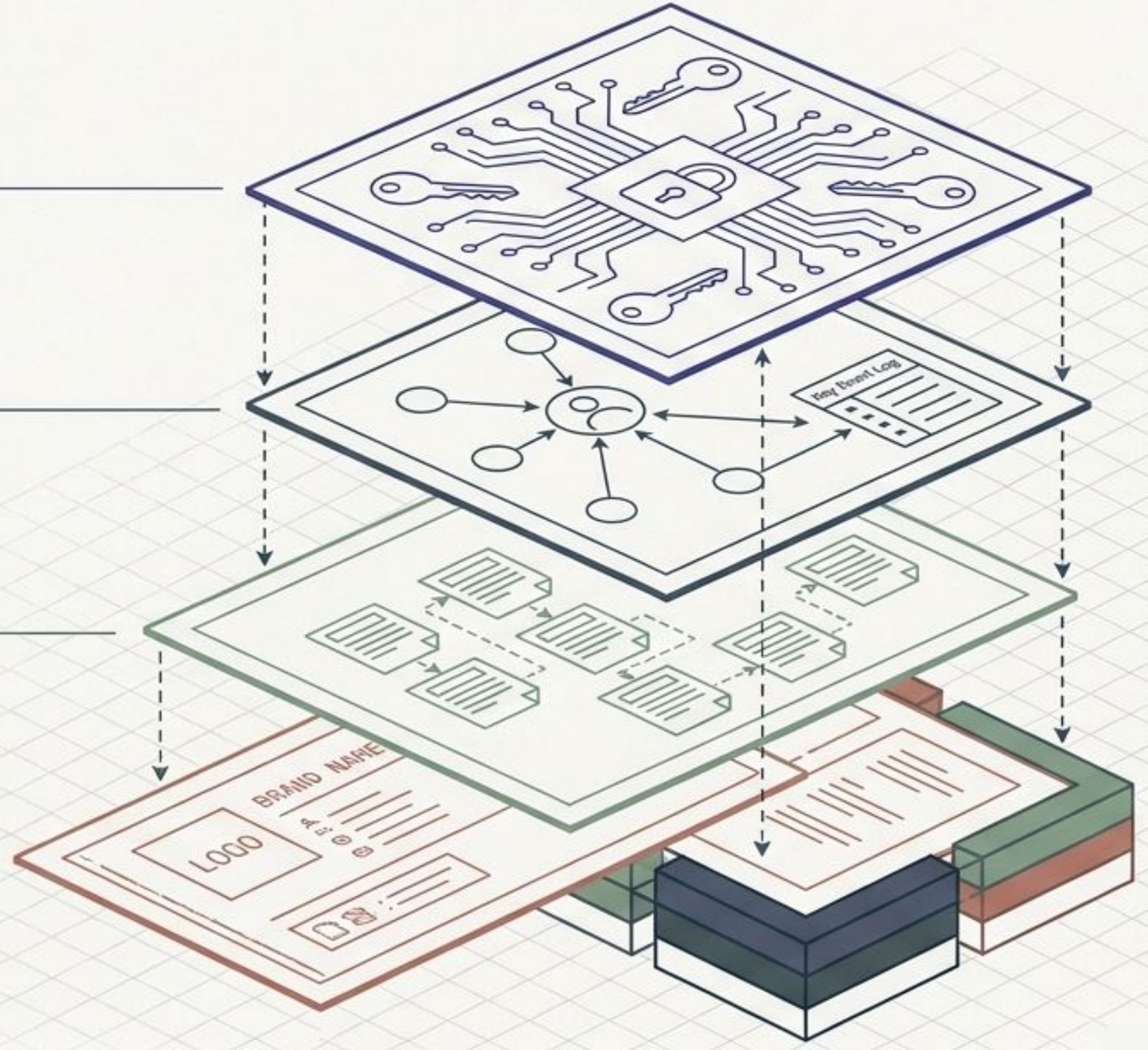
The Out-of-Band Introduction (OOBI) linking to the caller's Autonomous Identifier and Key Event Log (KEL).

Plate 3: evd Header

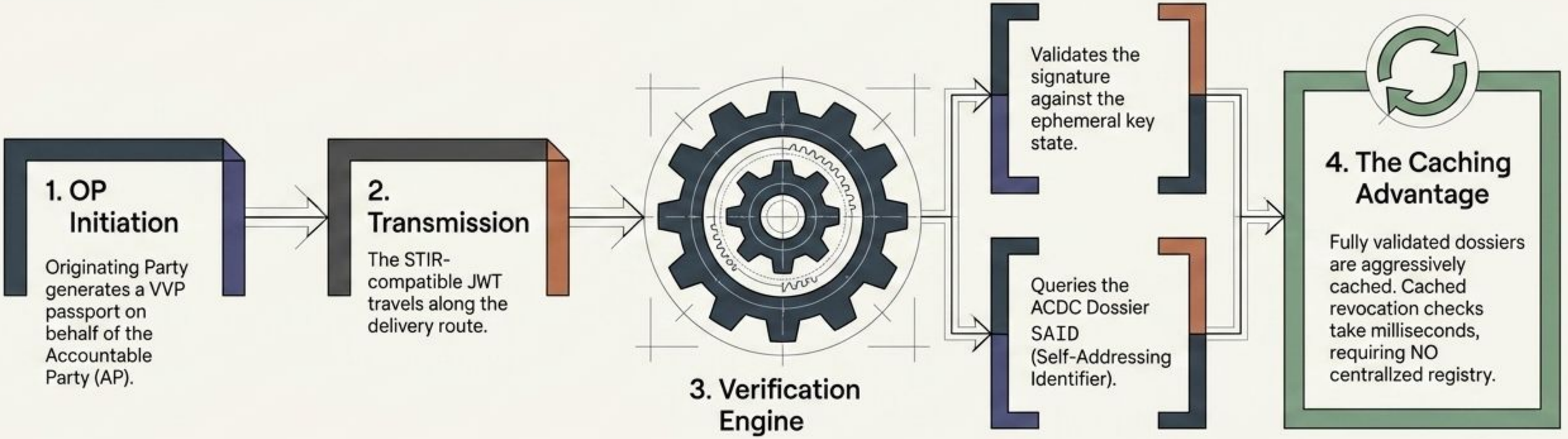
The OOBI linking directly to the Authentic Chained Data Container (ACDC) — the verifiable evidence dossier.

Plate 4: card & goal Claims

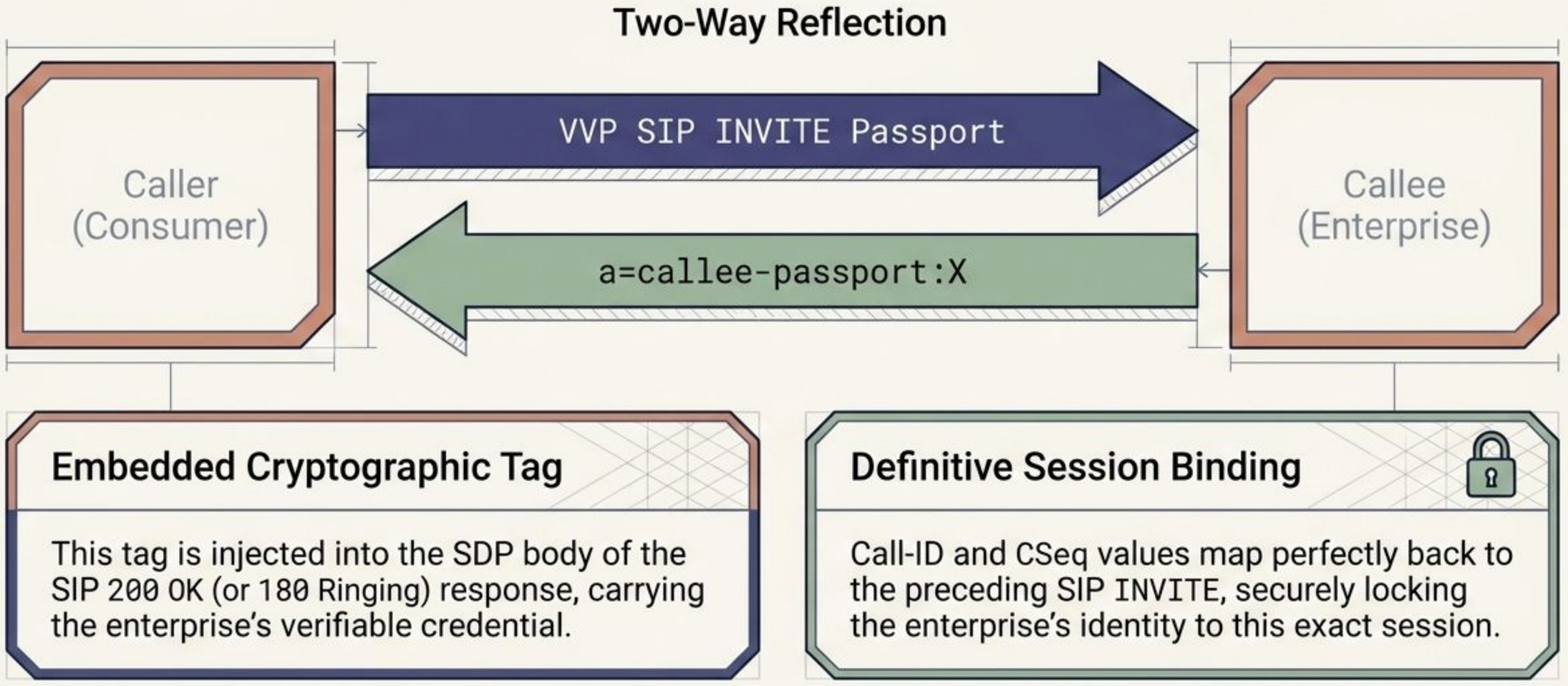
VCard-compliant brand attributes and machine-readable business intent.



The VVP engine separates ephemeral call data from long-term identity dossiers, enabling massive scalability through localized caching.



Cryptographic trust is bidirectional. VVP allows enterprises to cryptographically prove their identity to consumers, eliminating “Is this really my bank?” anxiety.



The CAMARA Verified Caller API translates protocol-level security into rich, operator-certified business cards on the consumer's screen.

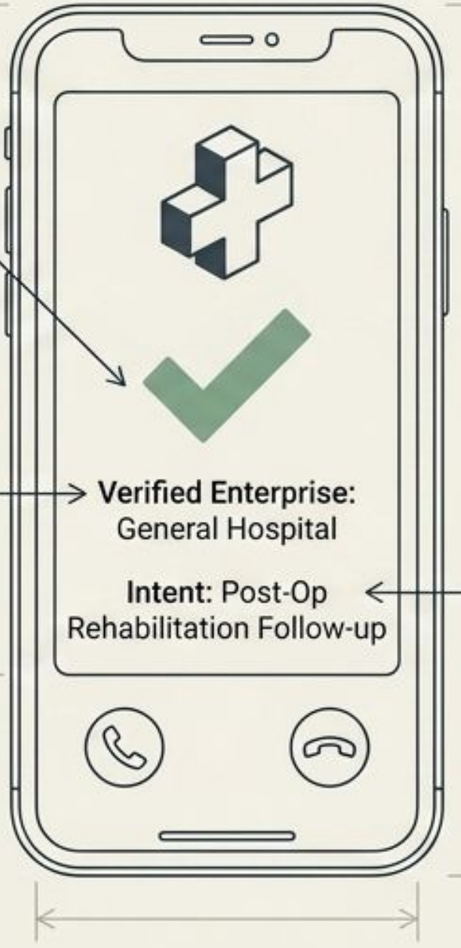
By replacing anonymity with verified intent, enterprises drastically increase their effective connection rates.

Operator-Certified Information

Displays cryptographically backed identity rather than easily spoofed caller ID.

Multimedia Integration

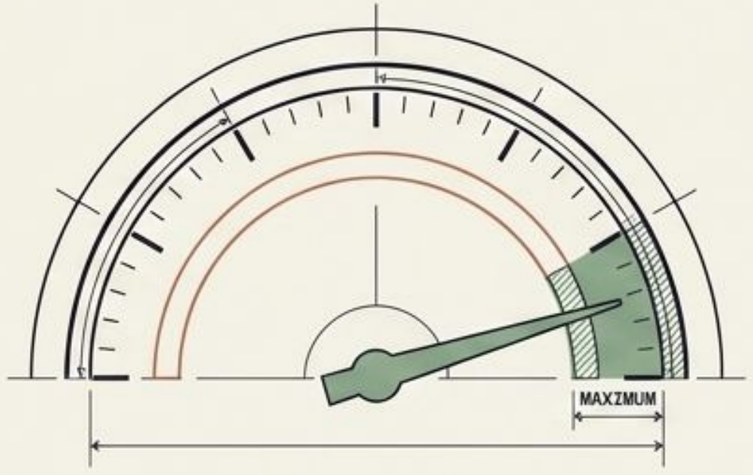
Capable of displaying logos, verification badges, and secure video snippets.



Flexible Activation (Per-Call)

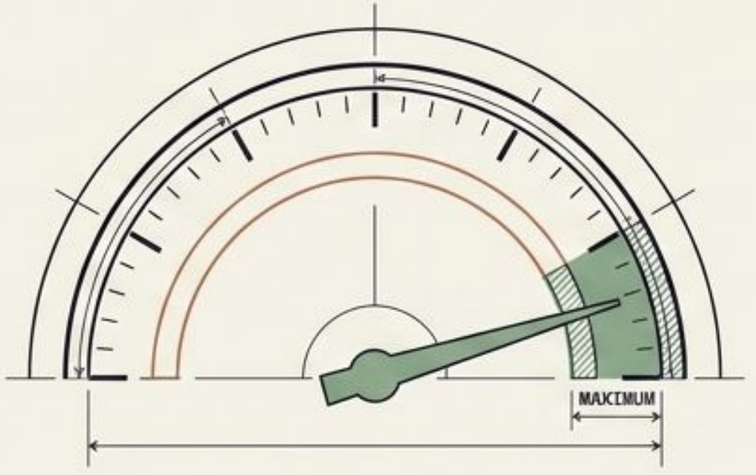
Enterprises activate features on a per-call basis, embedding specific, localized reasons for calling.

The live GSMA and Telefónica Tech pilot proved that decentralized identity can integrate seamlessly with legacy call center infrastructure.



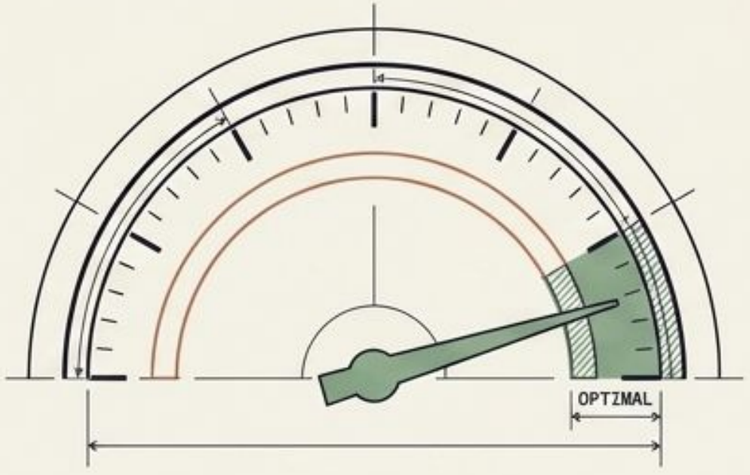
1. Seamless Integration

Successfully unified Dock Labs' decentralized ID stack, Telco Open Gateway APIs, and legacy call centers (Amazon Connect).



2. UX Acceptance

Achieved near-zero friction. Provided total privacy and control for consumers while delivering an exact operational fit for operators.

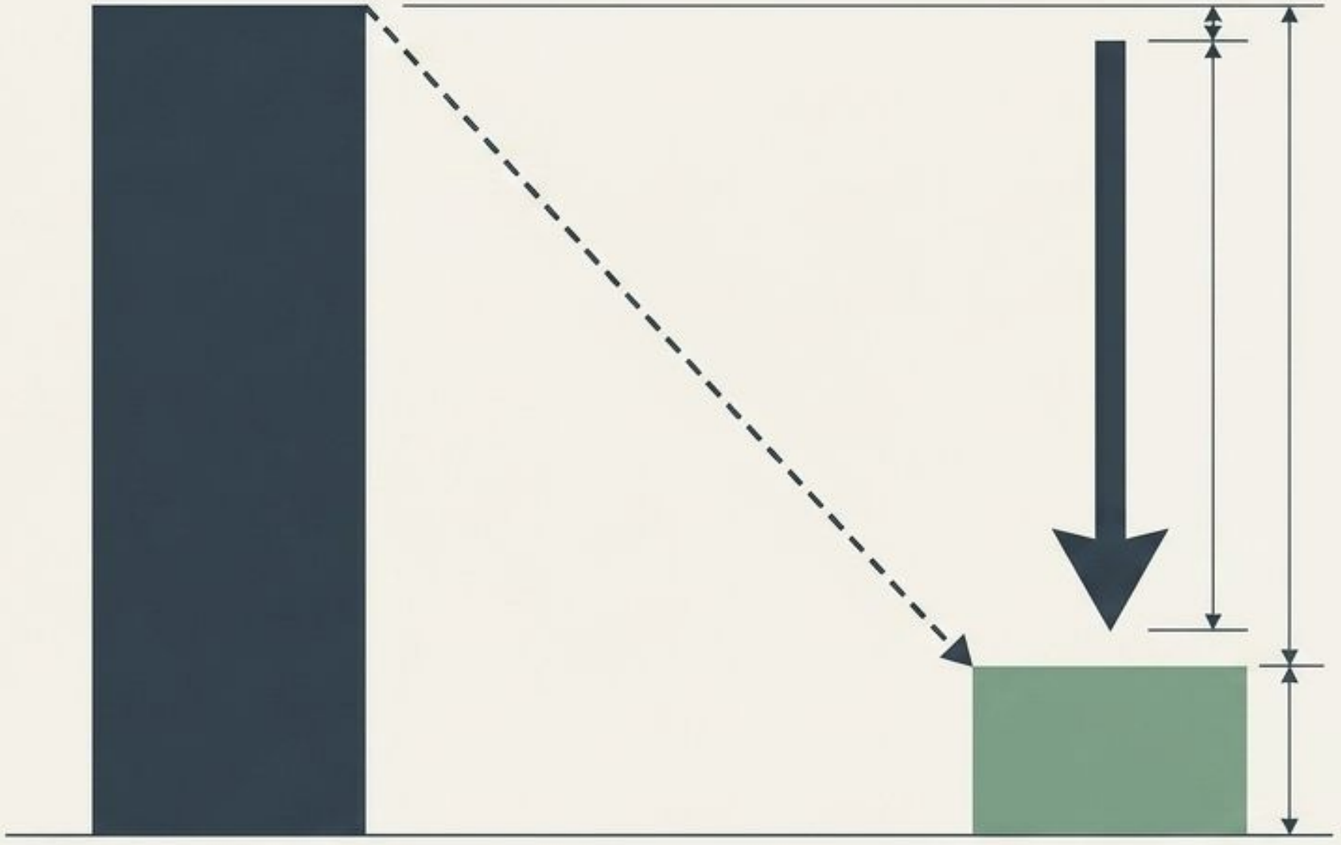


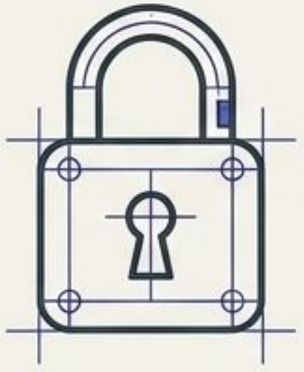
3. Connection Acceleration

Drastically slashed friction, reducing caller authentication time from minutes to seconds.

Cryptographic authentication slashes call handling times and effectively neutralizes the liability of insider data leakage.

ROI Waterfall Chart





Insider Threat Mitigation

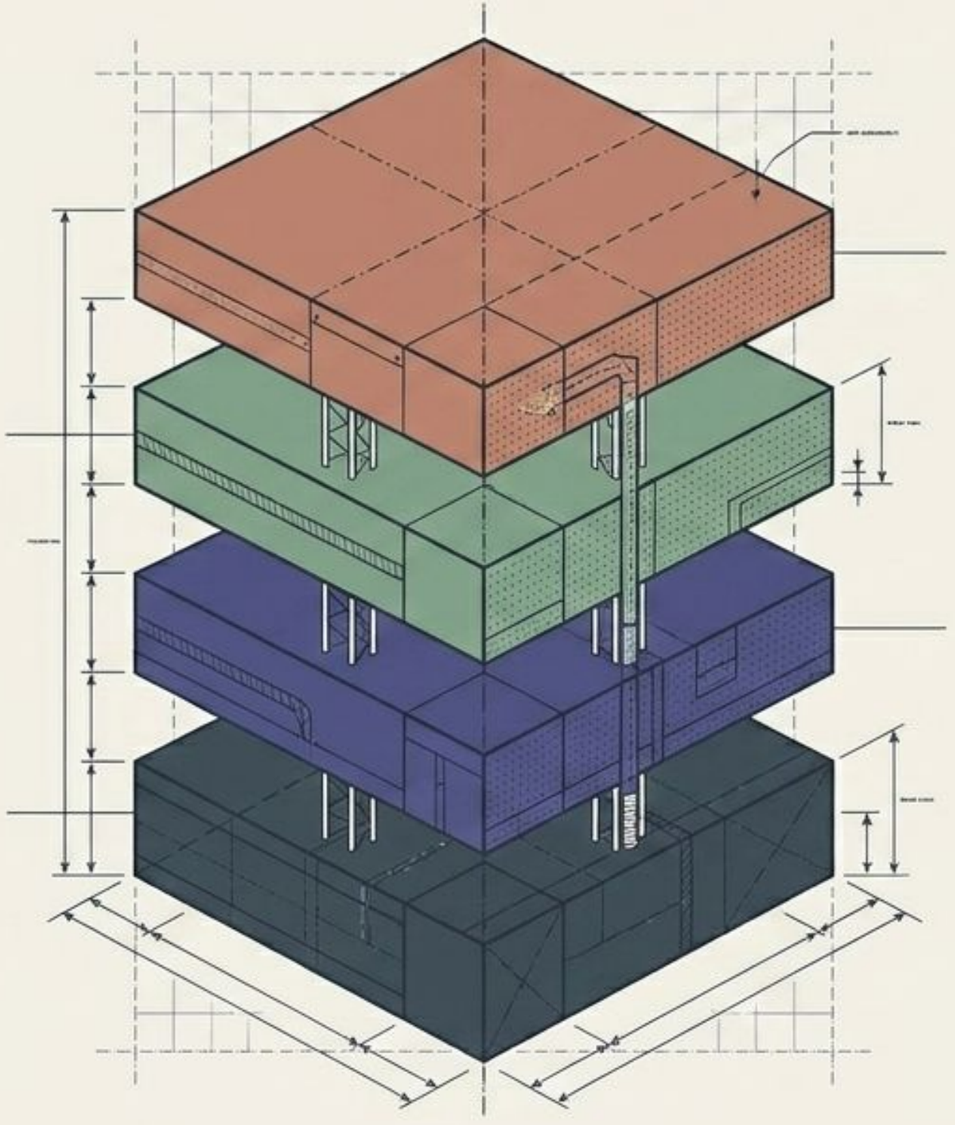
Less Data = Less Liability

Selective disclosure (wallet-based yes/no confirmation) completely removes sensitive data from the call center agent's view. This eliminates the risk of bribed agents extracting customer data, neutralizing Coinbase-style social engineering attacks.

The Unified Trust Ecosystem: A coordinated stack of open standards, global telco networks, and decentralized infrastructure.

Layer 4: The Surface (Infrastructure)
Truvera & Dock Labs decentralized edge wallets managing the user's verifiable credentials.

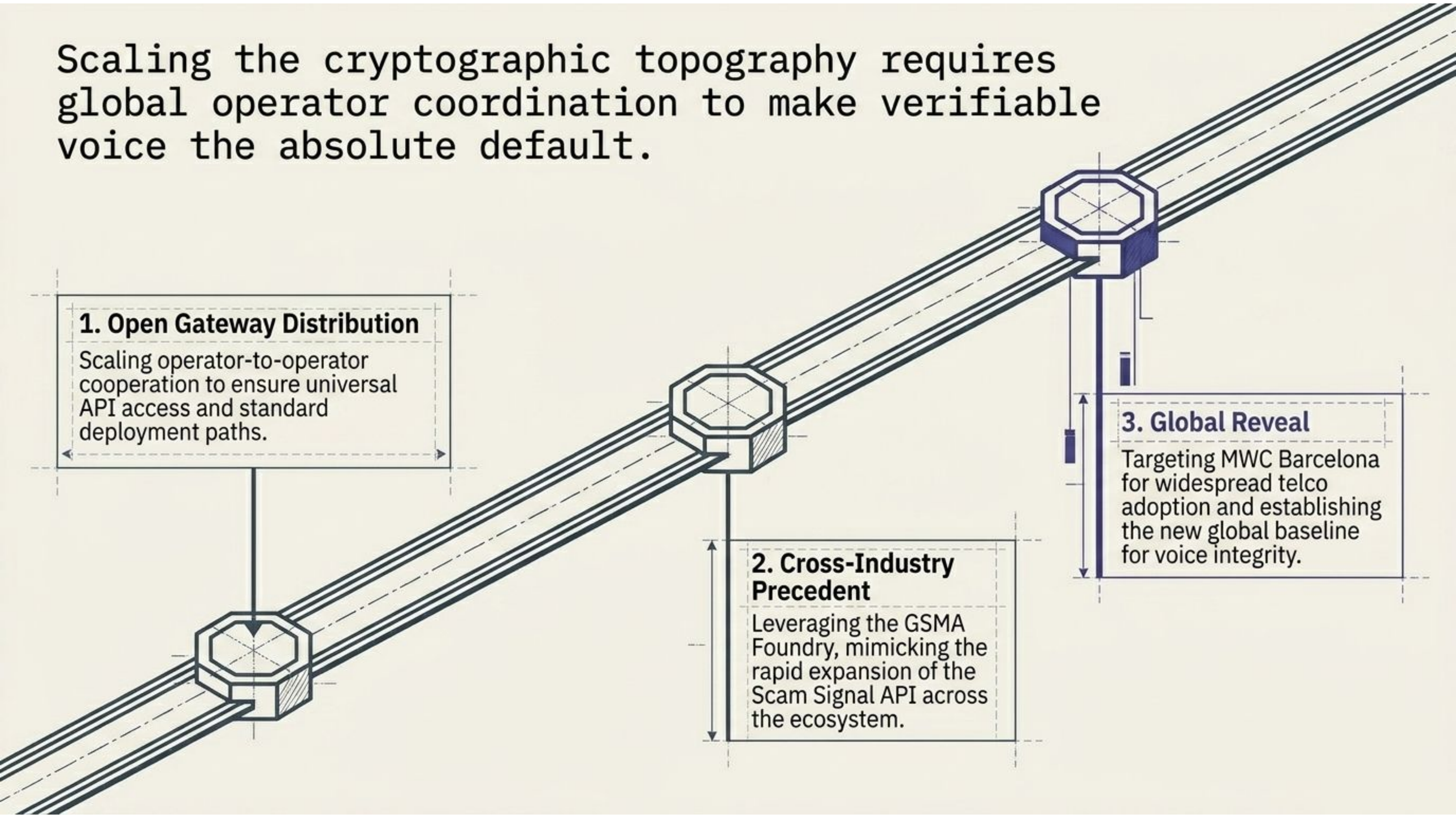
Layer 3: The Interconnect
CAMARA Open Gateway APIs ensuring standardized, cross-border enterprise access.



Layer 2: The Anchor (Root of Trust)
Telco SIMs and real-time GSMA network signaling APIs.

Layer 1: The Standard
IETF Verifiable Voice Protocol (VVP) providing the cryptographic engine.

Scaling the cryptographic topography requires global operator coordination to make verifiable voice the absolute default.



1. Open Gateway Distribution

Scaling operator-to-operator cooperation to ensure universal API access and standard deployment paths.

2. Cross-Industry Precedent

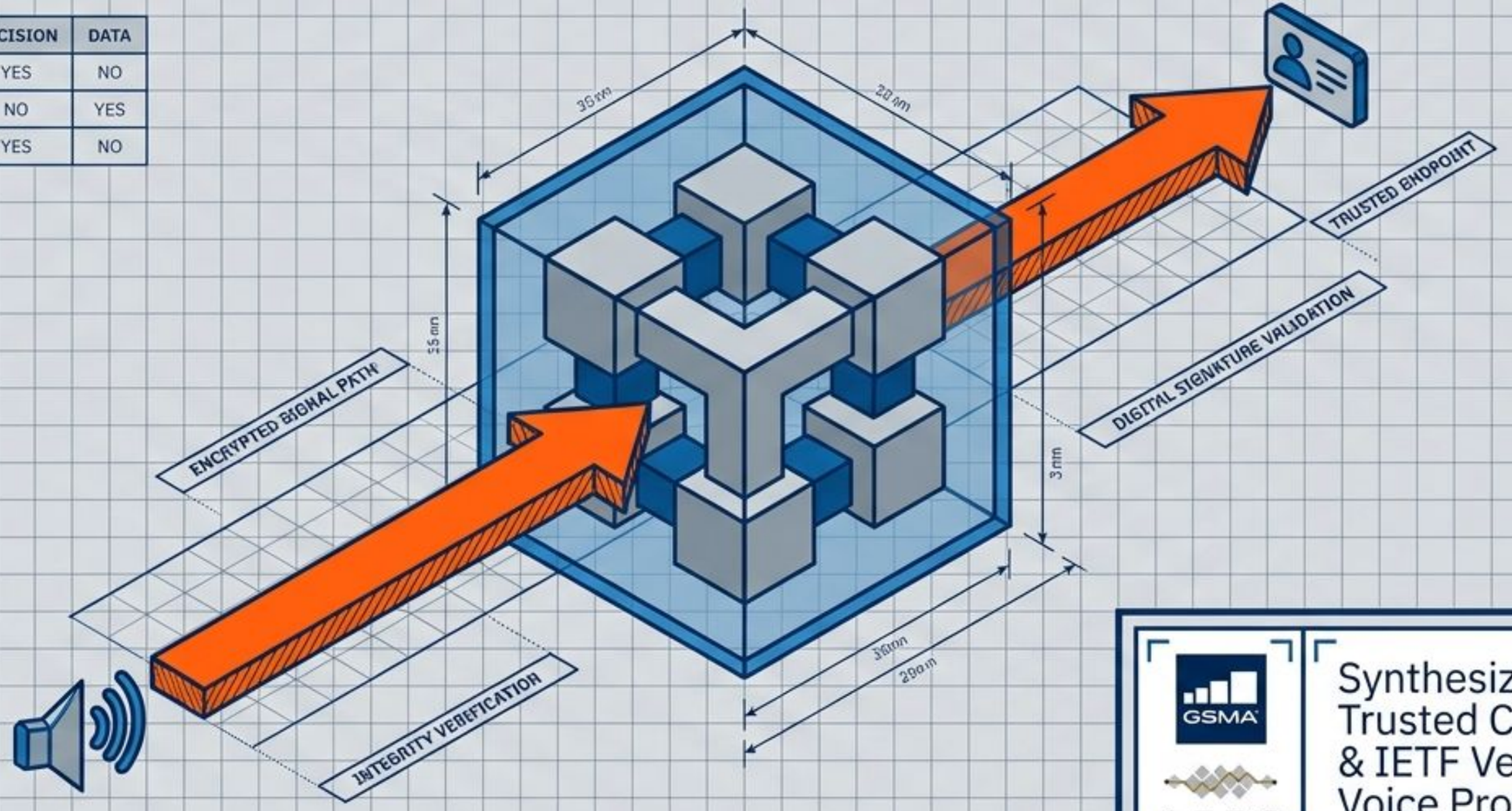
Leveraging the GSMA Foundry, mimicking the rapid expansion of the Scam Signal API across the ecosystem.

3. Global Reveal

Targeting MWC Barcelona for widespread telco adoption and establishing the new global baseline for voice integrity.

CRYPTOGRAPHIC PROOF REPLACES KNOWLEDGE-BASED AUTHENTICATION IN THE VOICE CHANNEL

DECISION	DECISION	DATA
VOICE SUCNNAL	YES	NO
DIGITAL APR	NO	YES
CRYPTIOGRAPHIC APMIF	YES	NO



GSMA

IETF

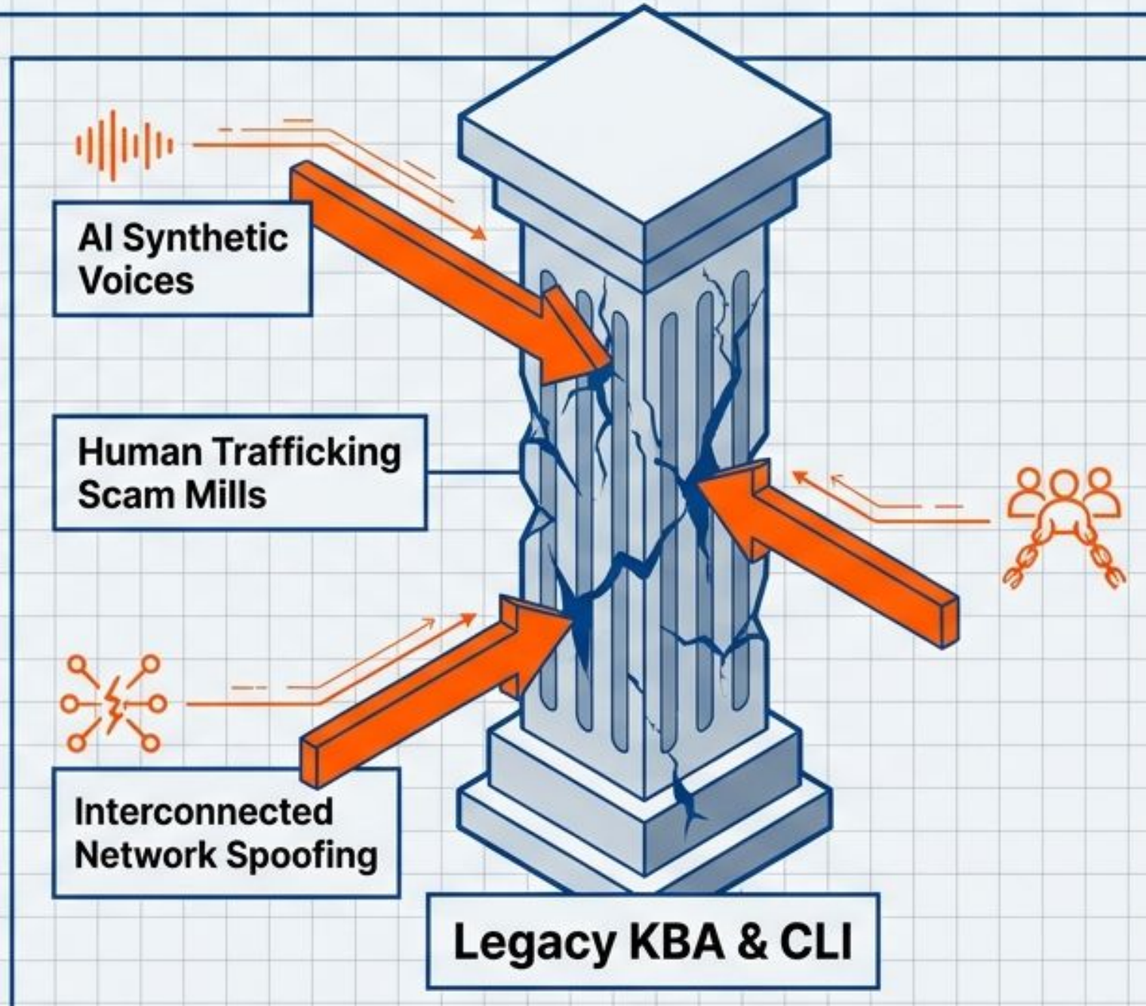
Synthesizing GSMA Trusted Caller Identity & IETF Verifiable Voice Protocol

Interconnected networks and Generative AI have rendered Caller Line Identity structurally defenseless.

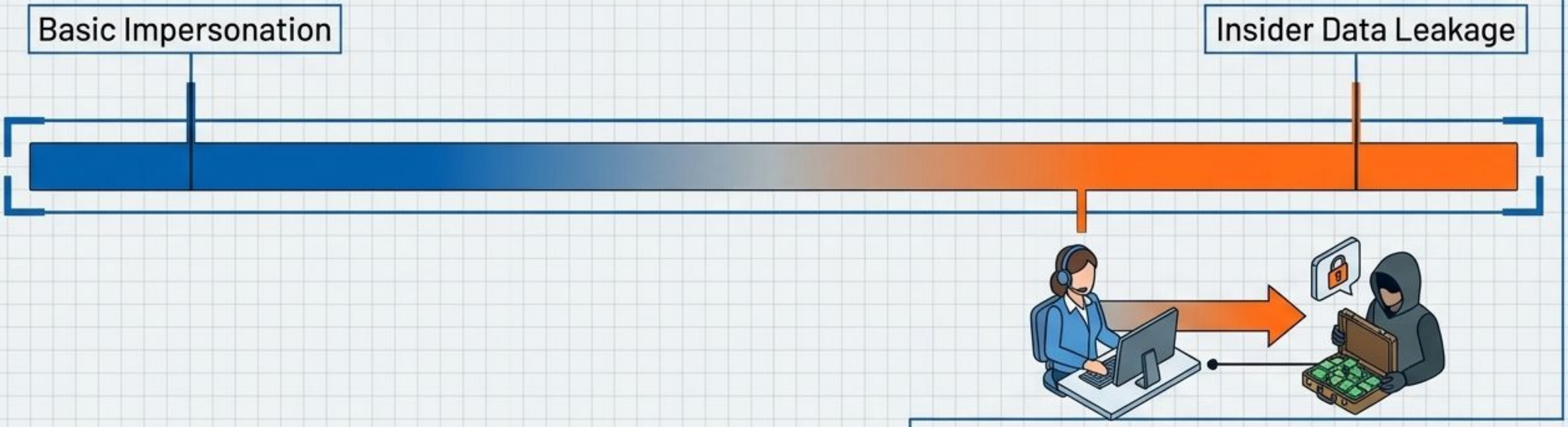
$1T+

Losses (2024)

Only ~4% Recovered



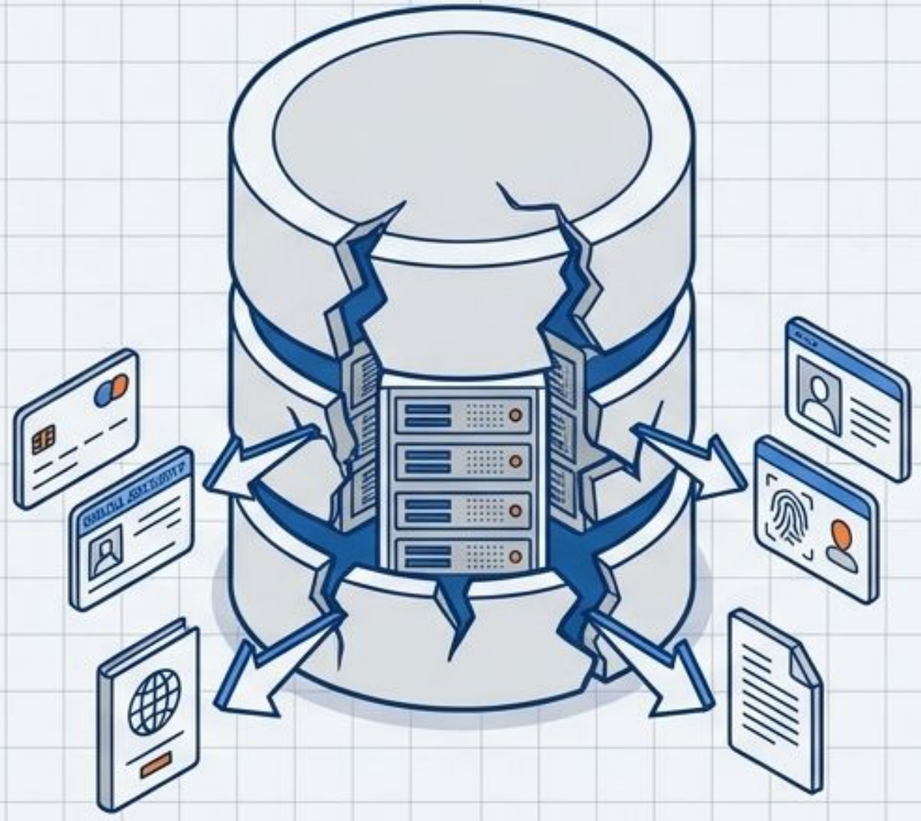
Centralizing personal data for verification transforms call centers into high-risk targets.



Traditional KBA demands sensitive data disclosure, turning customer service infrastructure into lucrative honeypots.

Decentralized wallets shift identity control to the edge, enabling verification without exposing raw data

Data Storage Liability (Legacy)



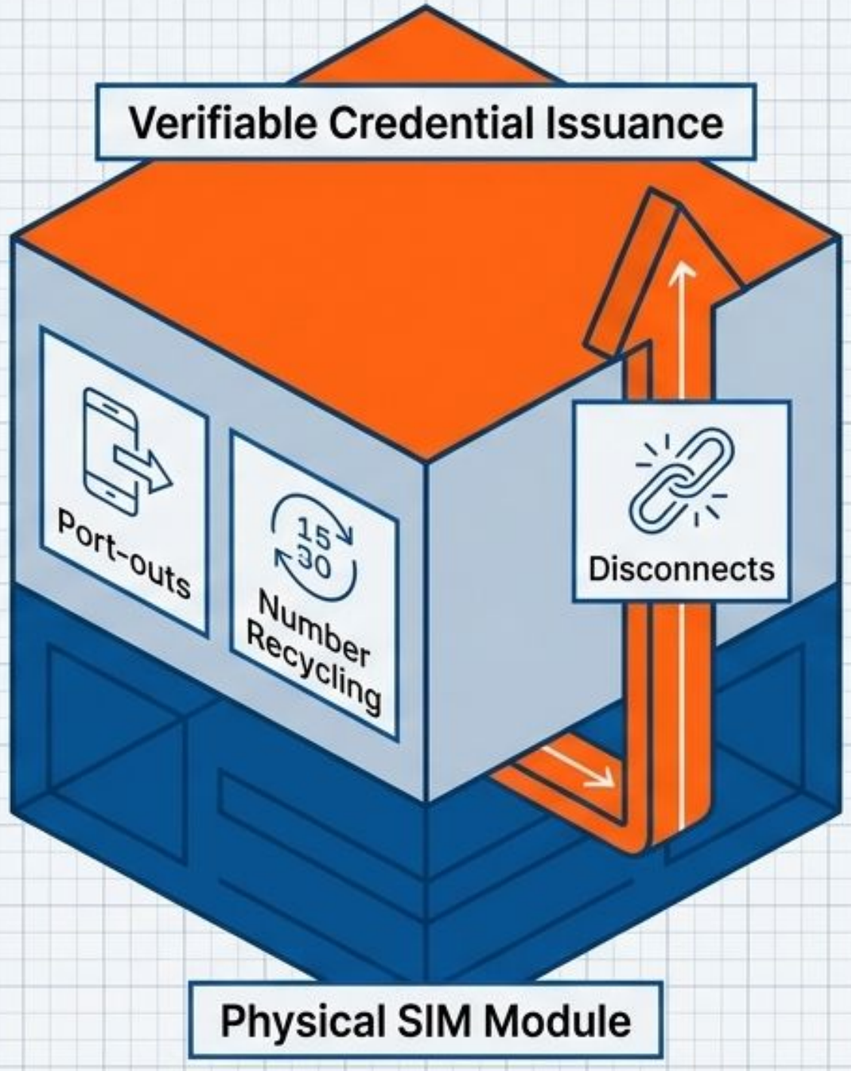
Edge-Held Proof (Future)

Selective Disclosure: Only necessary proofs are shared.

Edge-Held Data: Verifiers validate credentials locally without storing raw PII.

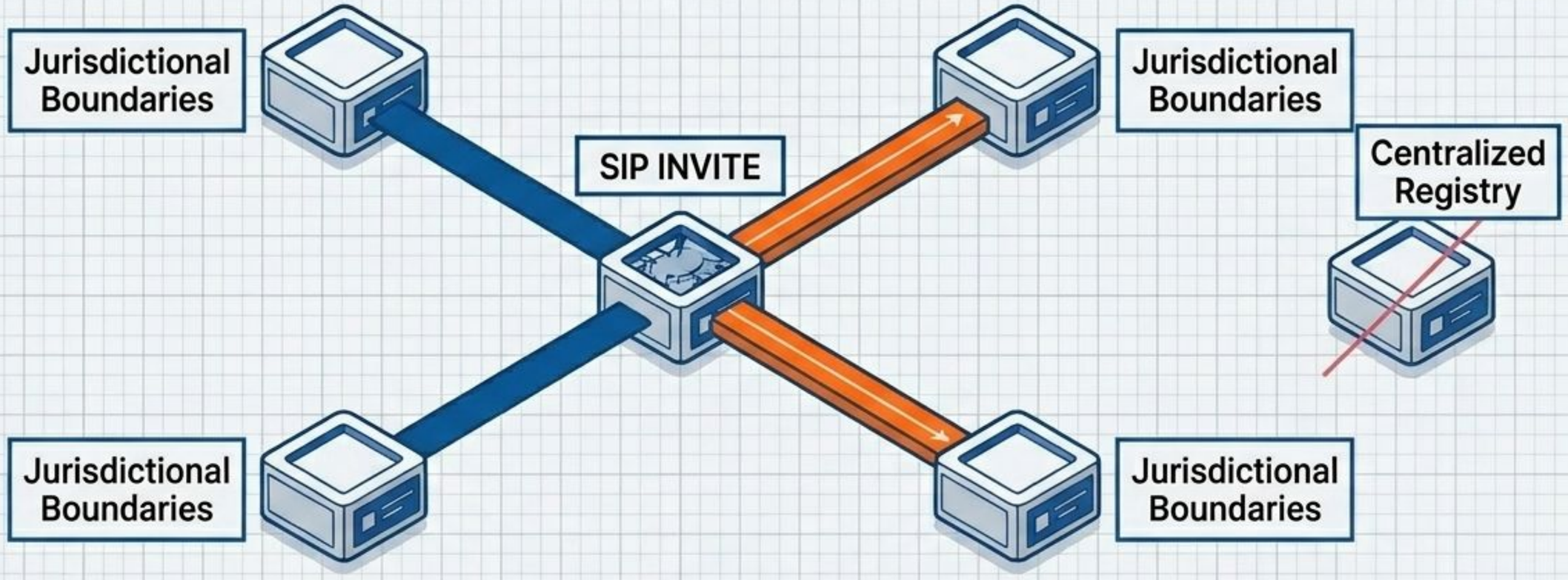
Telecom operators provide the foundational cryptographic anchor through continuous network lifecycle authentication.

The Telecom Root of Trust



Operators authenticate devices hundreds of times daily, uniquely equipping them to automatically revoke credentials when network trust conditions change.

VVP binds cryptographic evidence directly to network signaling to eliminate trust gaps.



STIR-Compatible: Operates natively within standard SIP signaling architectures.

Independent Proof: Standardizes evidence transmission without requiring global centralized governance.

Narrowly defined cryptographic identities isolate risk and clarify legal accountability.

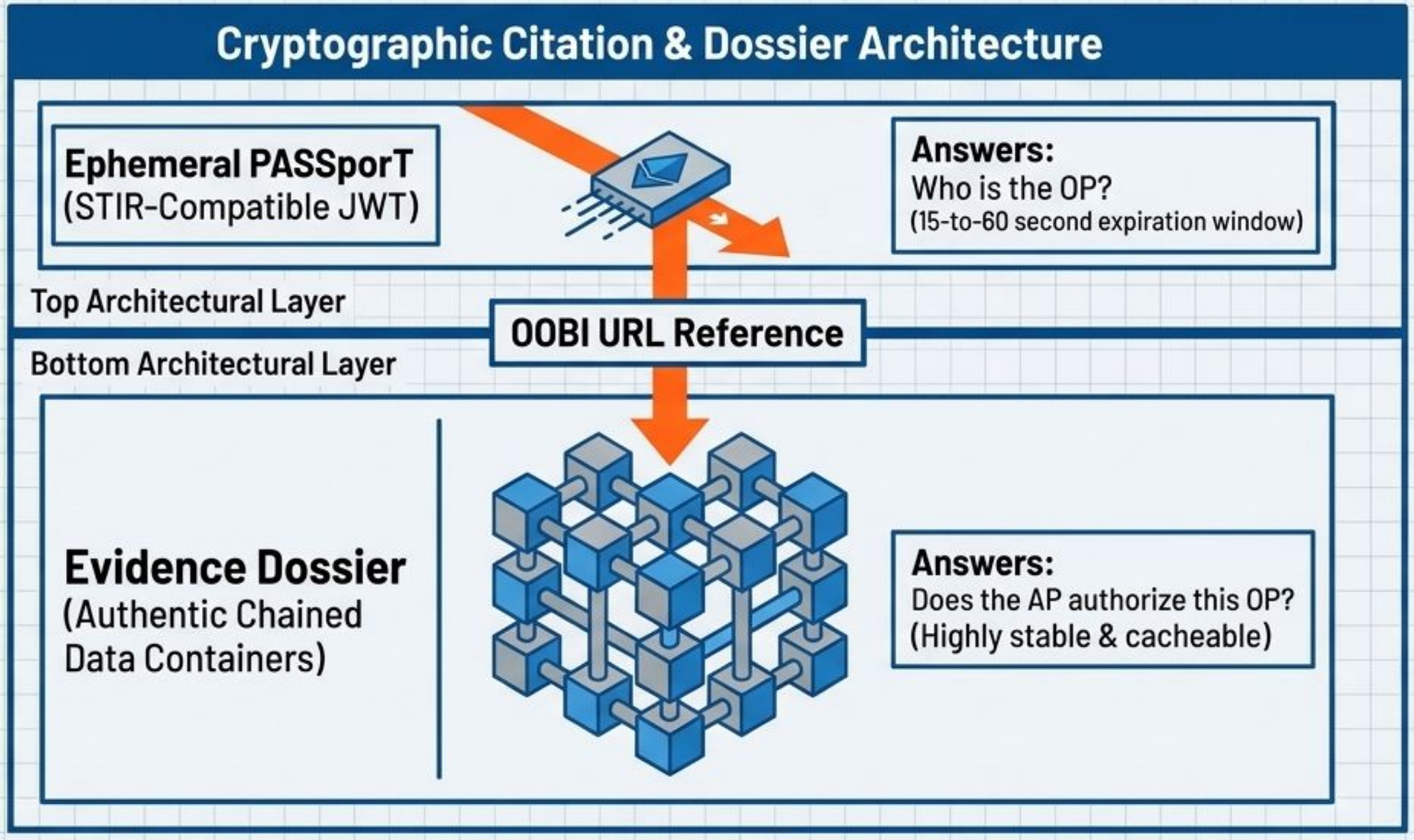
Role Definition Matrix

Accountable Party (AP)	Originating Party (OP)	Verifier
Legally owns the phone number and sets delegation authority.	Cryptographically signs the SIP INVITE on behalf of the AP.	Examines cryptographic evidence against local business rules.

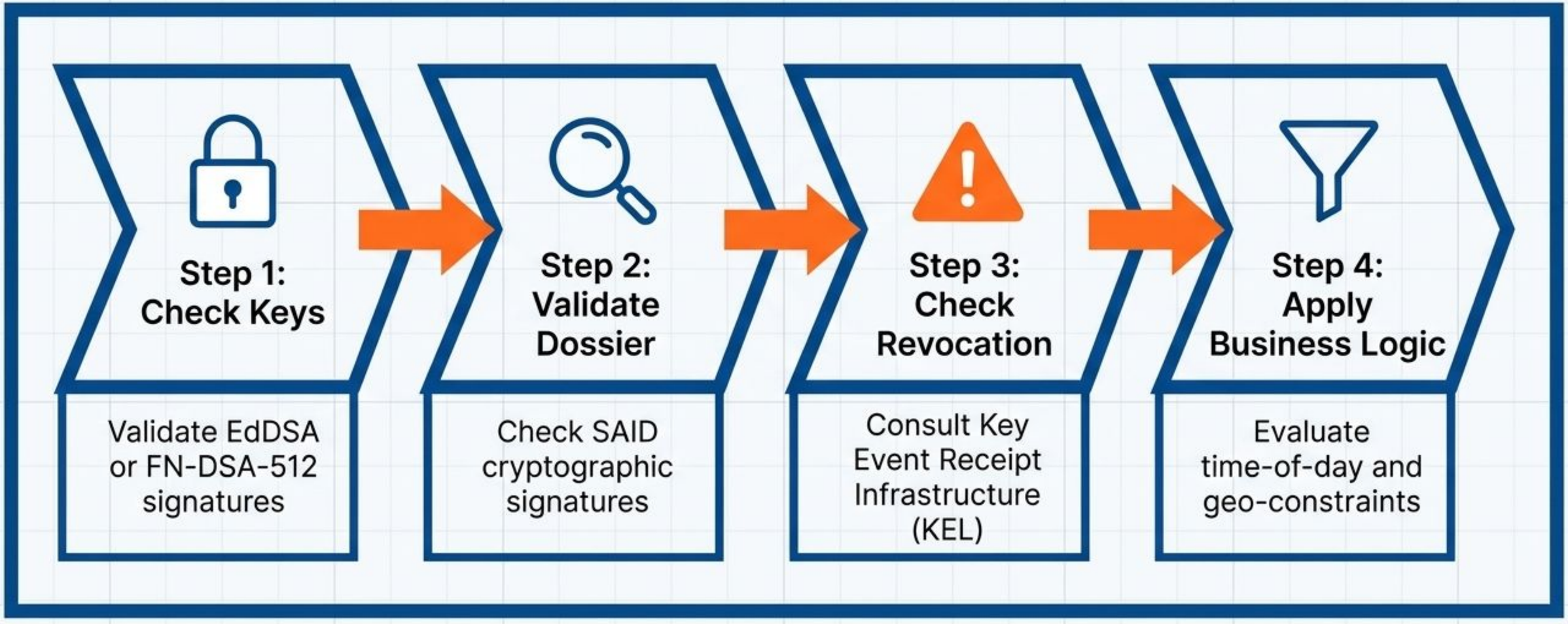
Delegation of Signing Authority

SIP INVITE with PASSporT

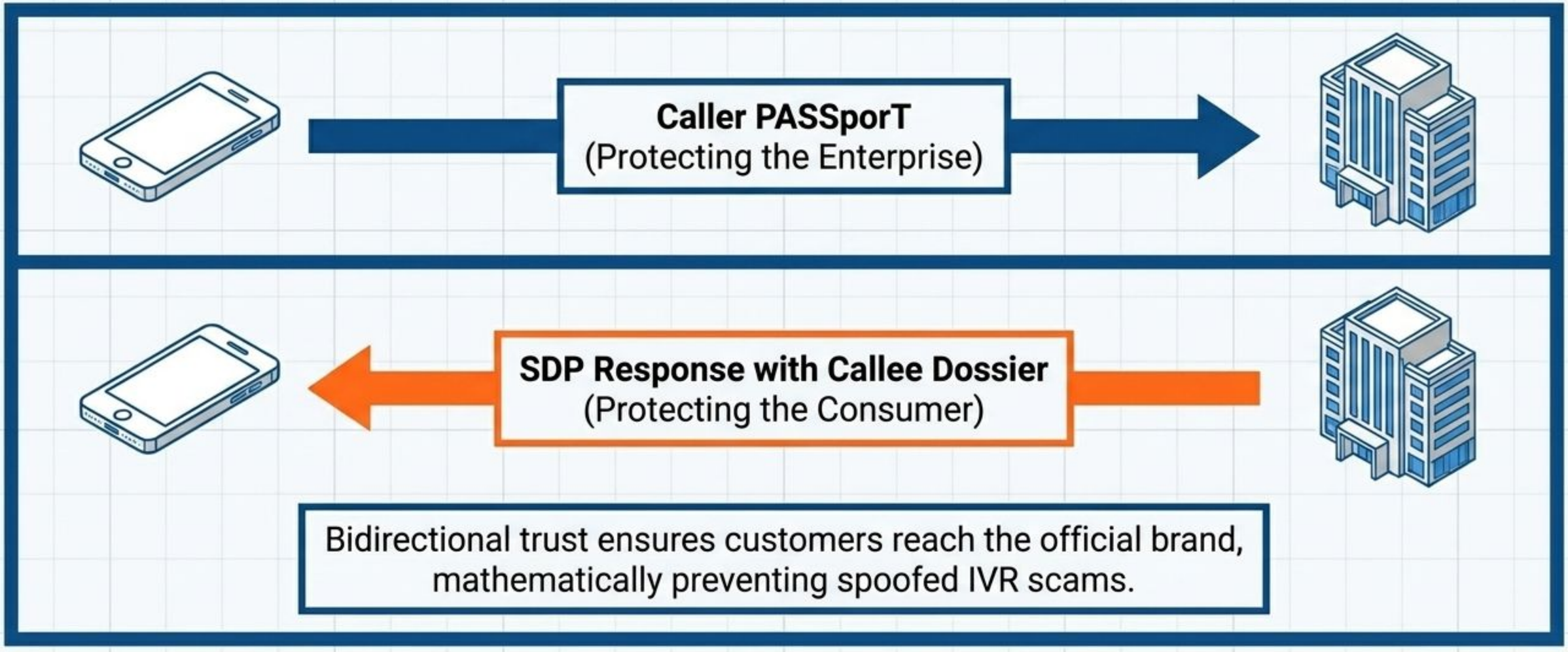
Lightweight SIP headers safely cite comprehensive, cacheable cryptographic dossiers.



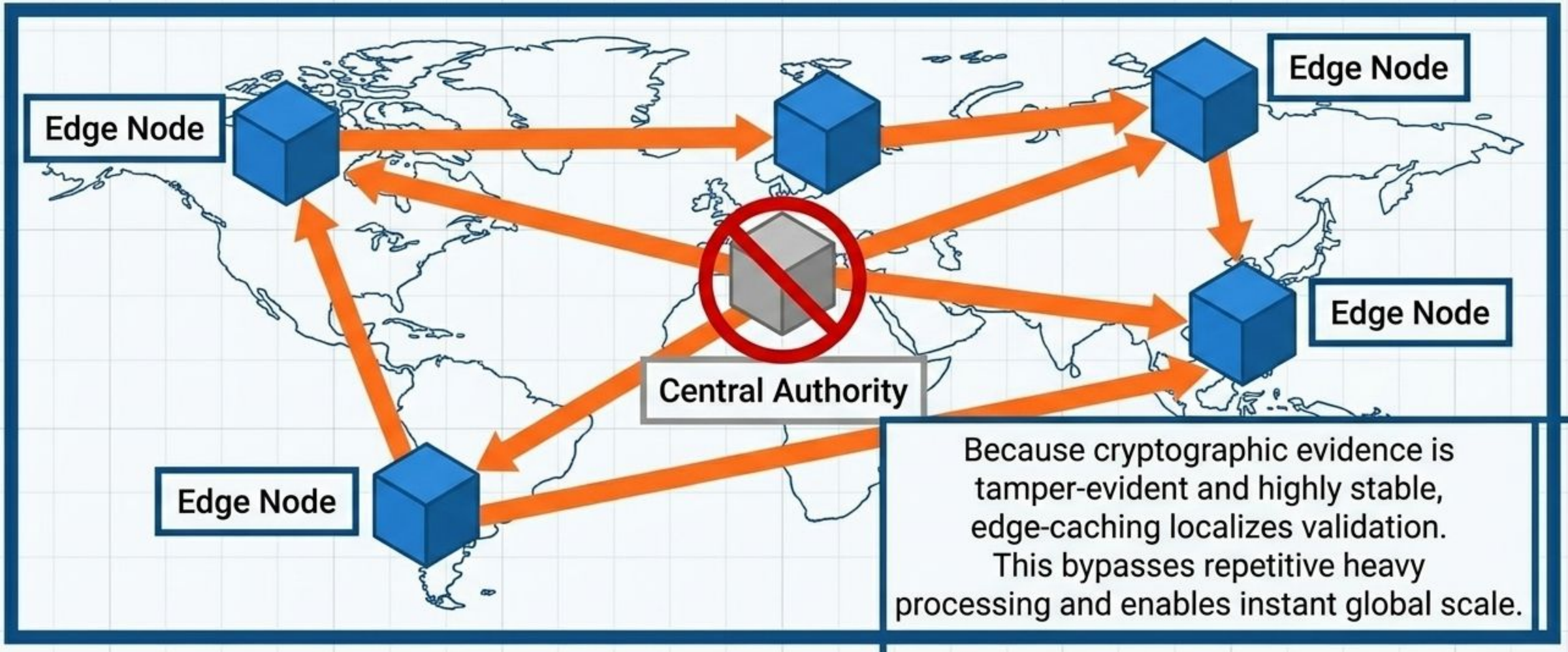
Verifiers authenticate identity, delegation, and intent locally before a call connects.



VVP enables bidirectional cryptographic proof, protecting enterprise call centers and end-users equally.

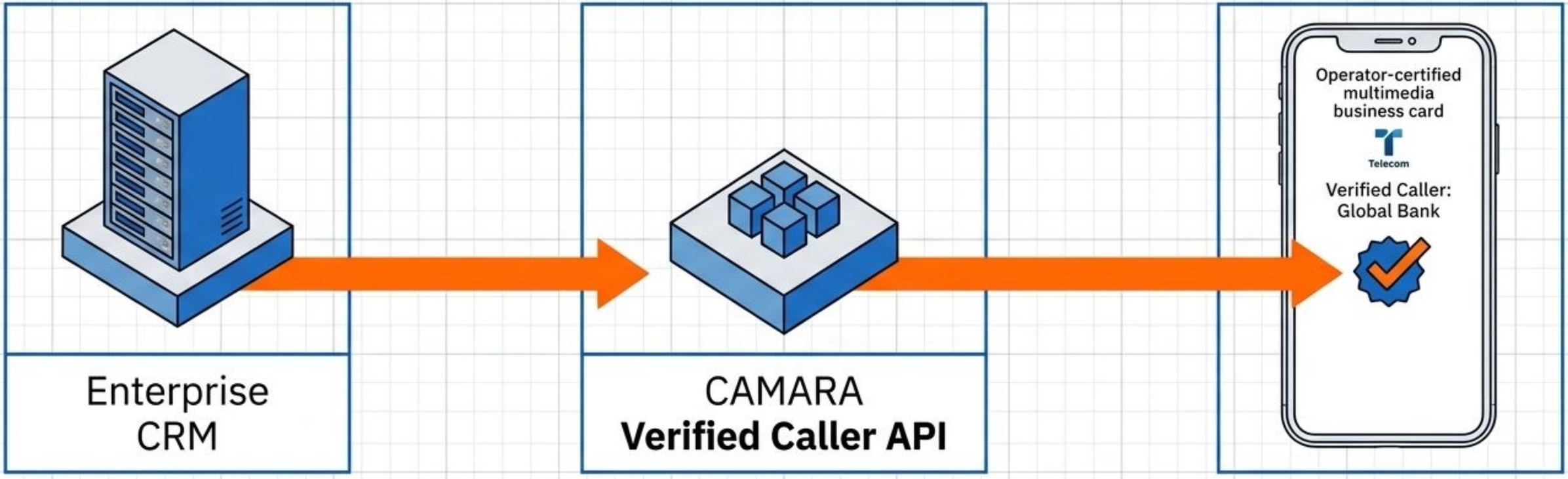


Edge-cached validations scale globally without requiring coordinated central registries.



Because cryptographic evidence is tamper-evident and highly stable, edge-caching localizes validation. This bypasses repetitive heavy processing and enables instant global scale.

Standardized telecom APIs translate cryptographic proof into vivid, customer-facing verification



Healthcare Use Case:
Patient trust drives connection rates.

Finance Use Case:
Instant visual verification prevents fraud.

Cryptographic verification reclaims minutes of call time while mathematically eliminating spoofing paths.

The Current Cost

4-5 Minutes for Authentication

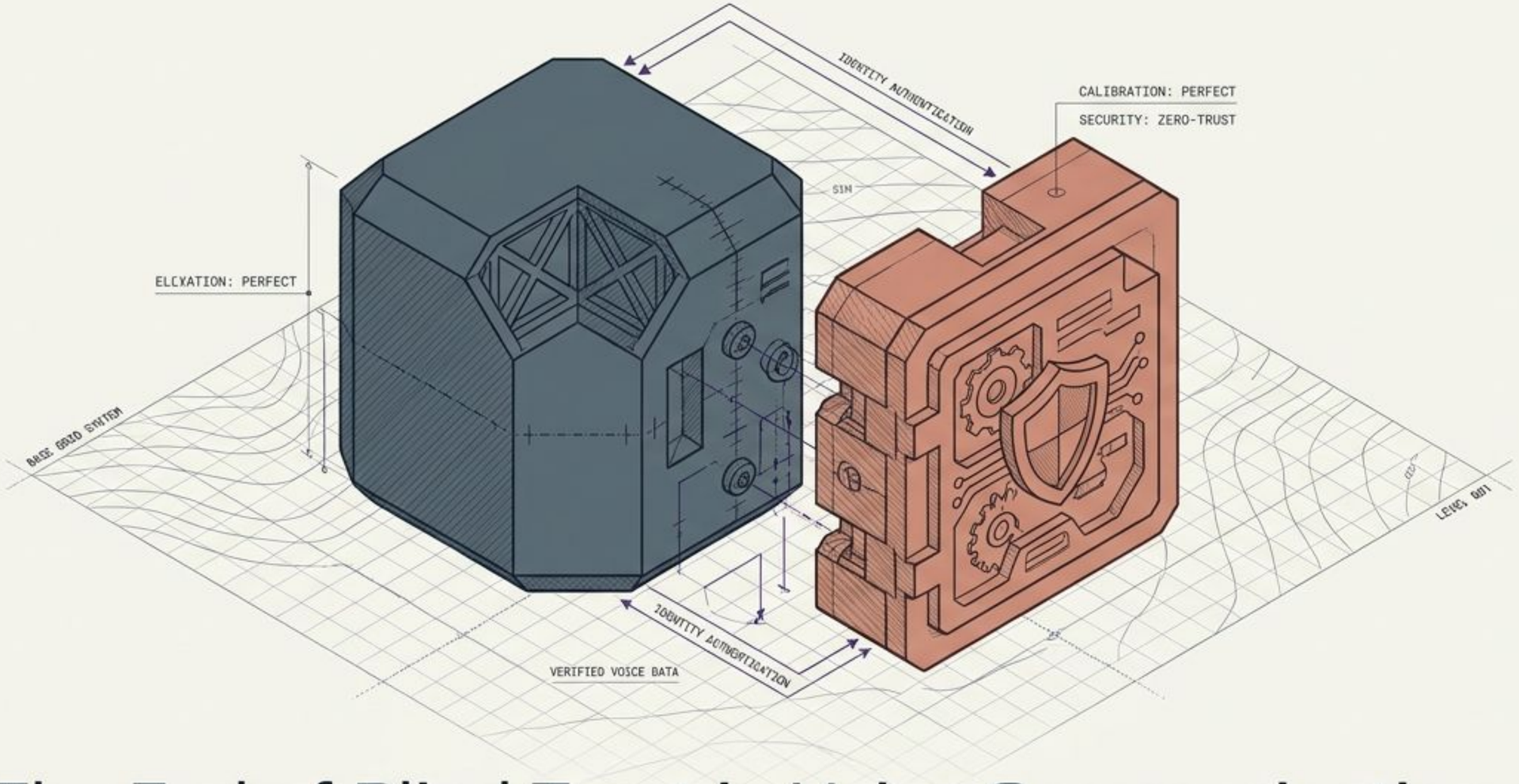
$0.75 - $1.50 Cost Per Minute

The Cryptographic ROI

Instant Edge-Verification

Eliminates CLI Spoofing & SIM Swap Vulnerabilities

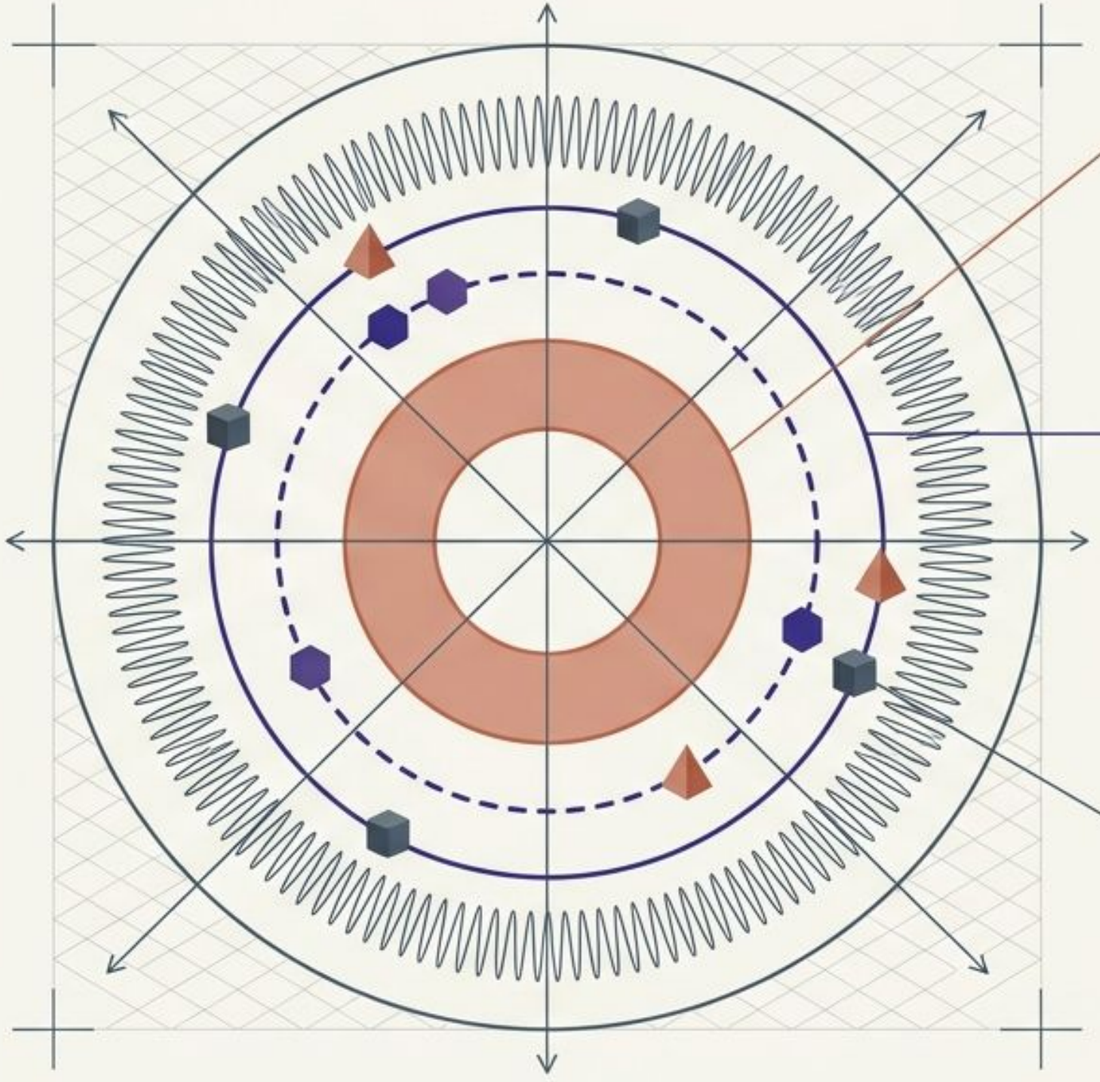
Moving identity to the cryptographic edge turns security from a multi-minute cost center into an instant, friction-free asset.



The End of Blind Trust in Voice Communications

A strategic blueprint for restoring the integrity of the voice channel through Telco-rooted identity, decentralized wallets, and the Verifiable Voice Protocol.

Industrialized fraud and Generative AI have transformed voice channels into the most exploited attack surface in the world.



1. Financial Impact

> $1 Trillion global losses in 2024 (GASA estimate)

Only **~4%** of financial losses are successfully recovered.

2. Industrialized Operations

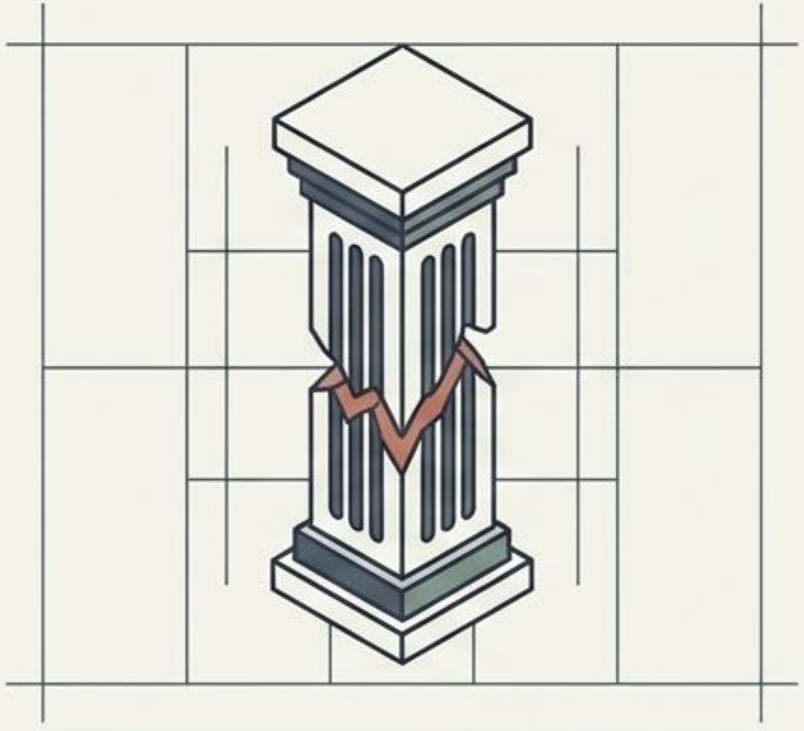
Call center fraud operations are highly organized, frequently tied to human trafficking in Southeast Asia.

Severe psychological harm impacts **>50%** of targeted adults globally.

3. AI Acceleration

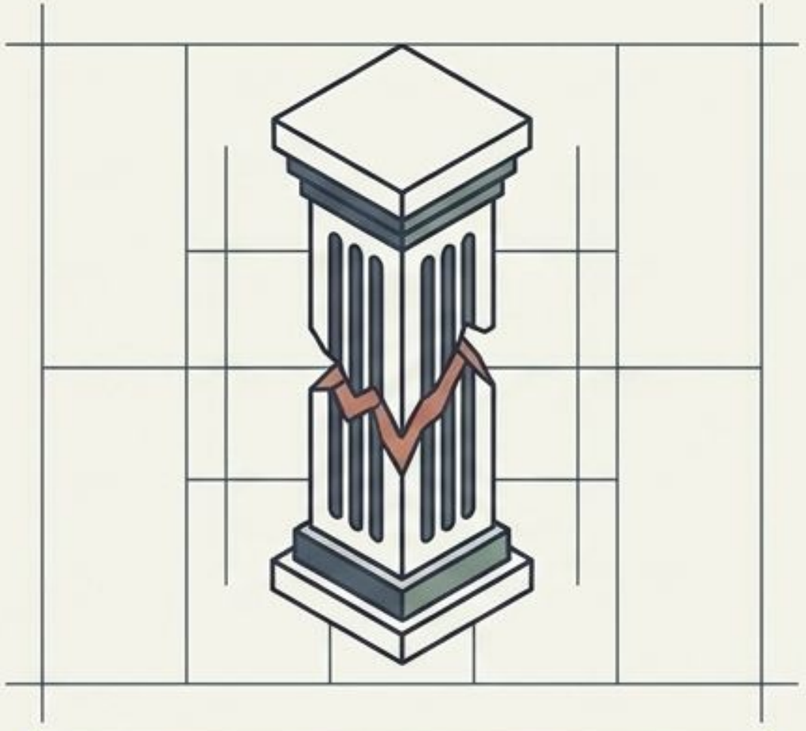
Synthetic Identity Proliferation via Generative AI allows malicious actors to iterate rapidly on real-looking synthesized voices and identities.

Legacy authentication relies on easily spoofed signals and forces mass data exposure, turning security into a profound corporate liability.



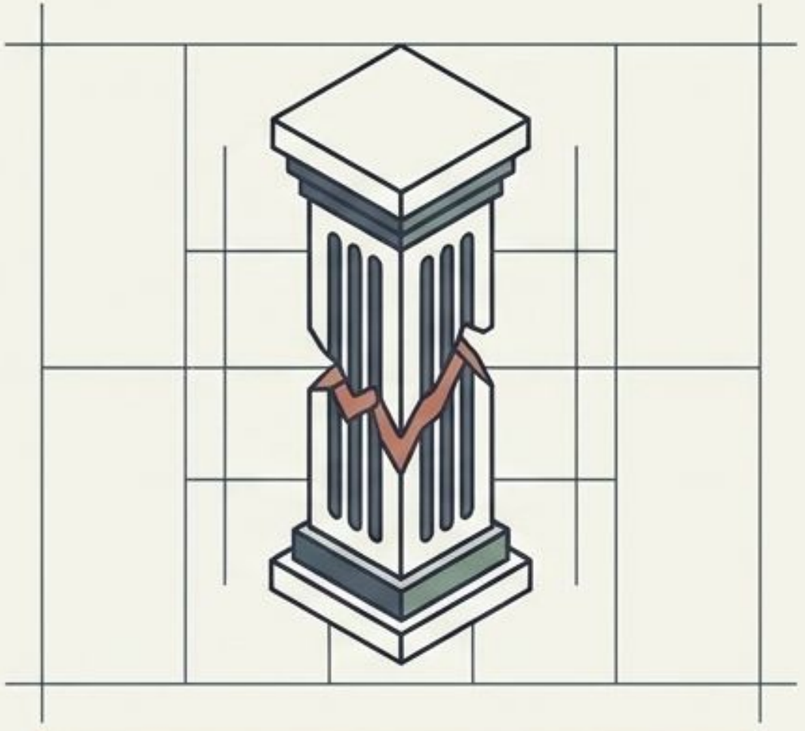
Caller Line Identity (CLI)

The Fault: CLI was designed for a closed system. On modern interconnected networks, it is easily spoofed, enabling mass impersonation without friction.



Knowledge-Based Authentication (KBA)

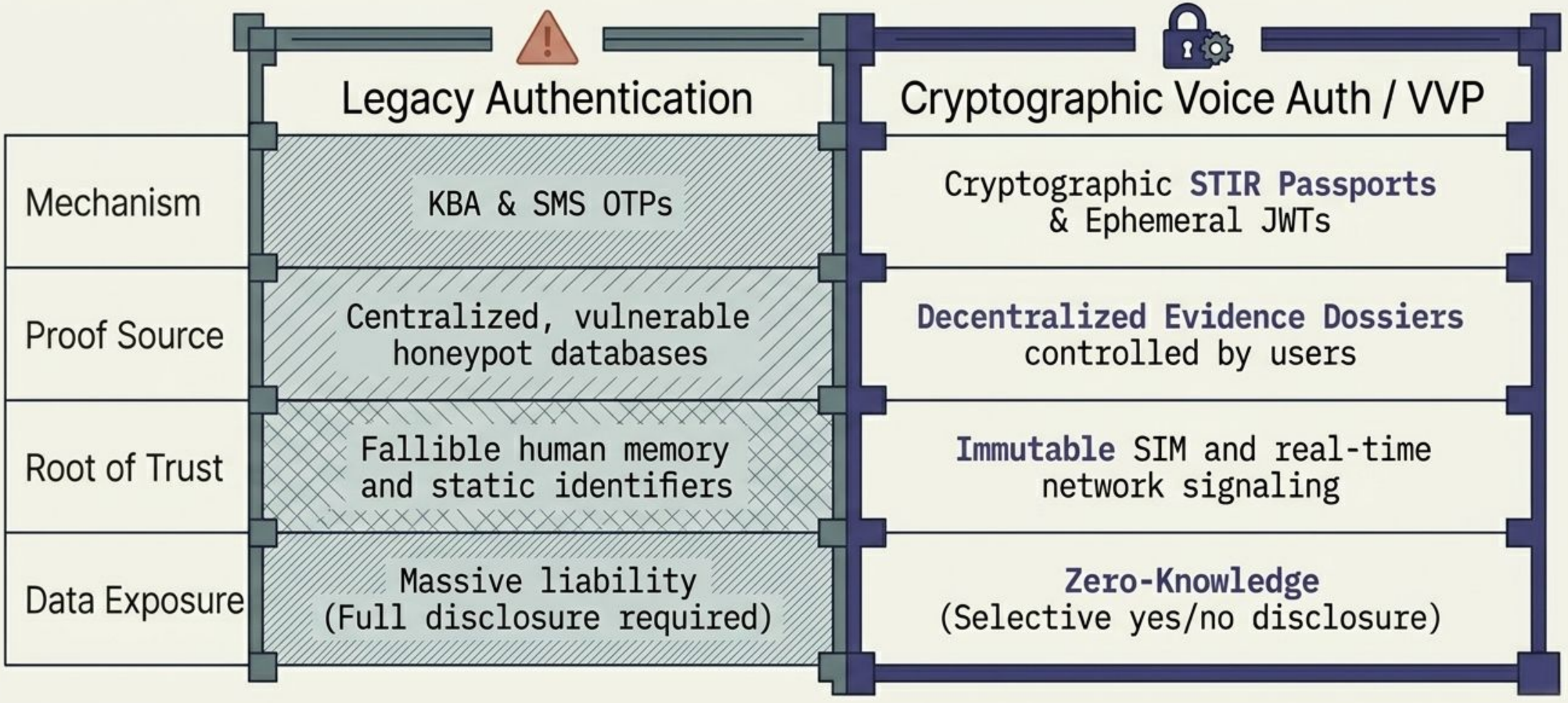
The Fault: Forces consumers to disclose sensitive data (e.g., Mother's maiden name), turning call center databases into massive honeypots and creating immense enterprise liability.



SMS One-Time Passwords (OTPs)

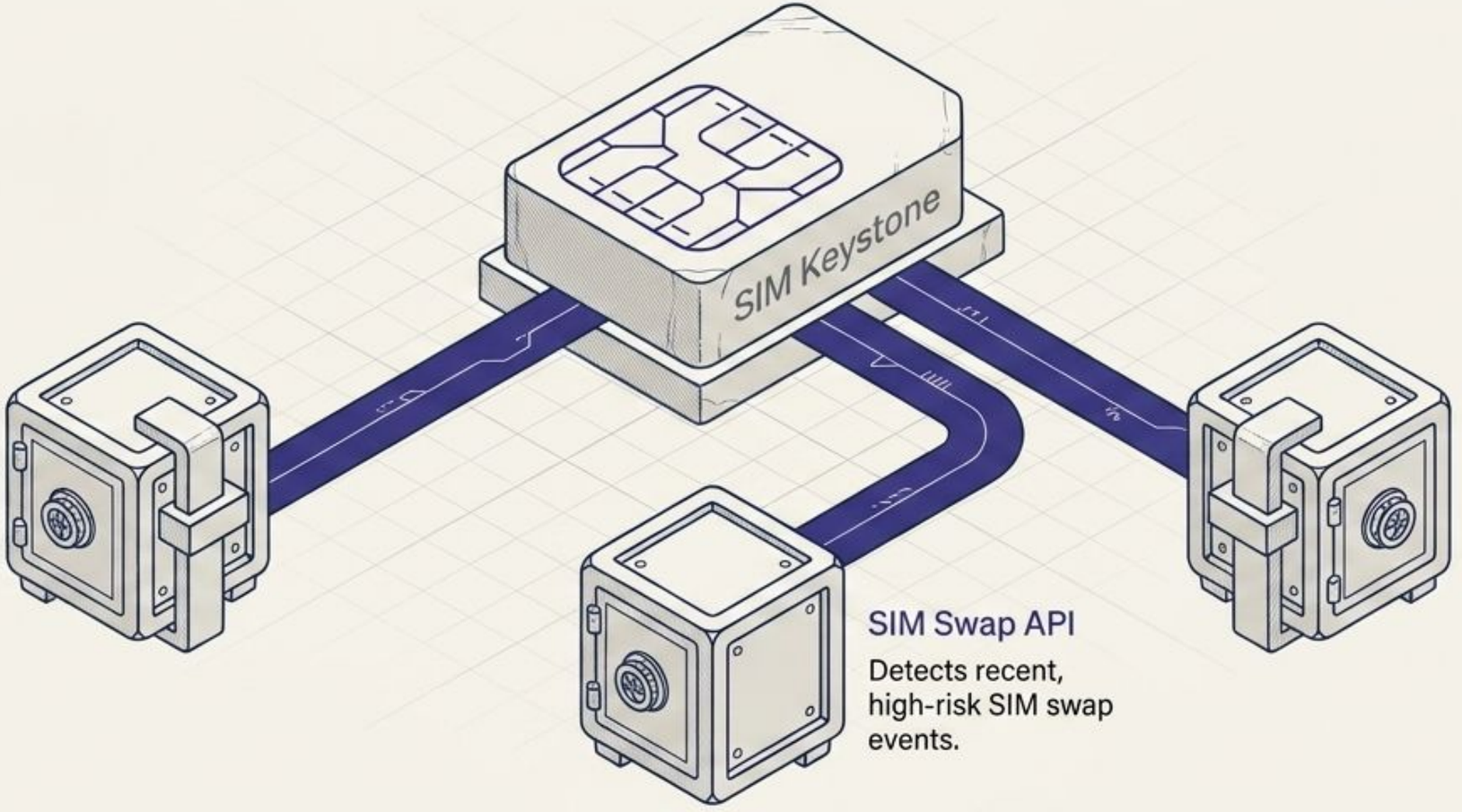
The Fault: Introduces high friction to the user experience and is increasingly vulnerable to network interception and targeted social engineering.

To secure the voice channel, the industry must transition from centralized data silos to decentralized cryptographic trust.



Mobile operators authenticate devices hundreds of times a day, making the SIM the definitive anchor for real-time digital identity.

Unlike static databases, Telcos process dynamic lifecycle events. If a number is recycled or ported, APIs instantly revoke the associated digital credentials, updating trust conditions in real-time.



Number Verification API

Confirms the user currently possesses the device and number.

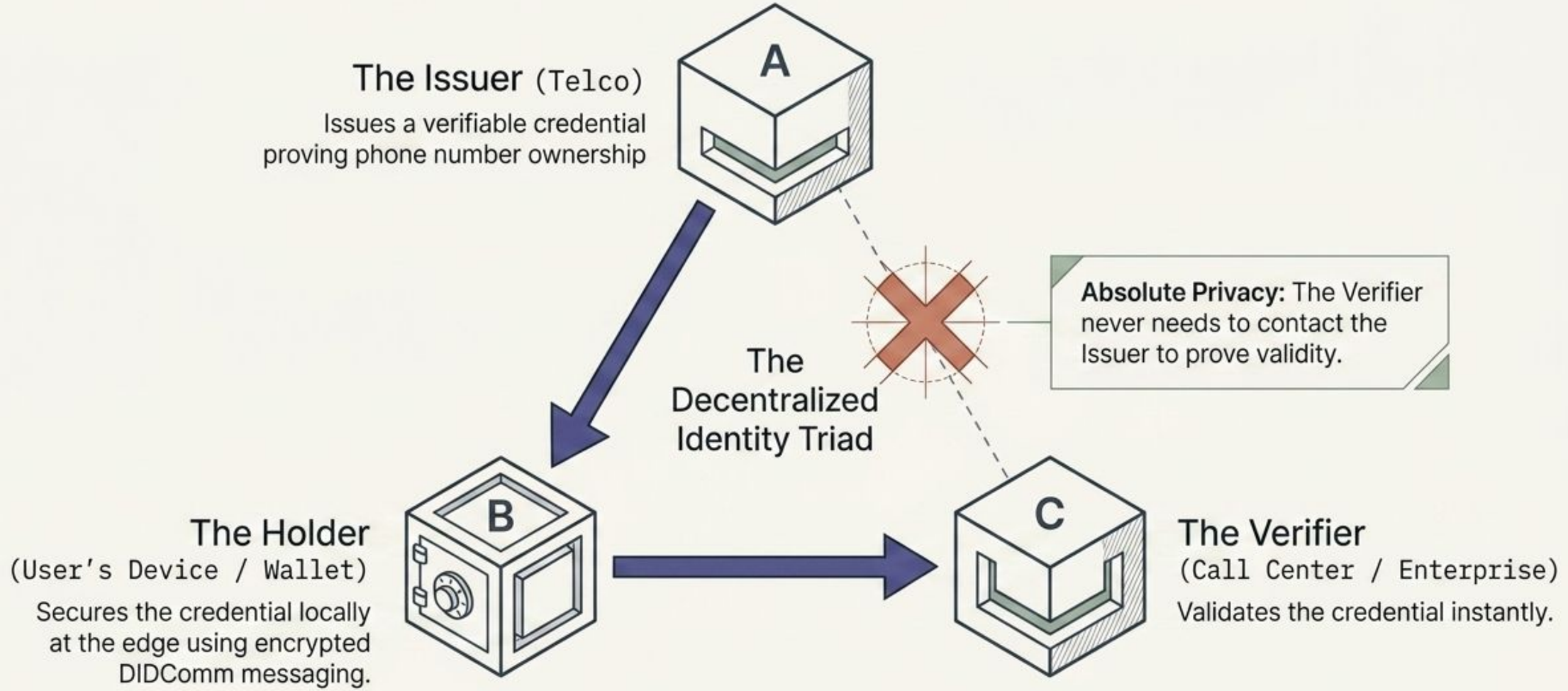
SIM Swap API

Detects recent, high-risk SIM swap events.

Network Lifecycle Events

Monitors real-time port-outs, disconnects, and number recycling.

Decentralized identity empowers users to hold their credentials locally, allowing instant verification without pinging central servers.



Under the hood, the Verifiable Voice Protocol (VVP) binds stable, cryptographic evidence directly to an ephemeral SIP INVITE.

Anatomy of a Passport

Plate 1: Cryptography

Mandates EdDSA or quantum-proof FN-DSA-512. Replay attack window clamped to an aggressive exp expiration of 15-60 seconds.

Plate 2: kid Header

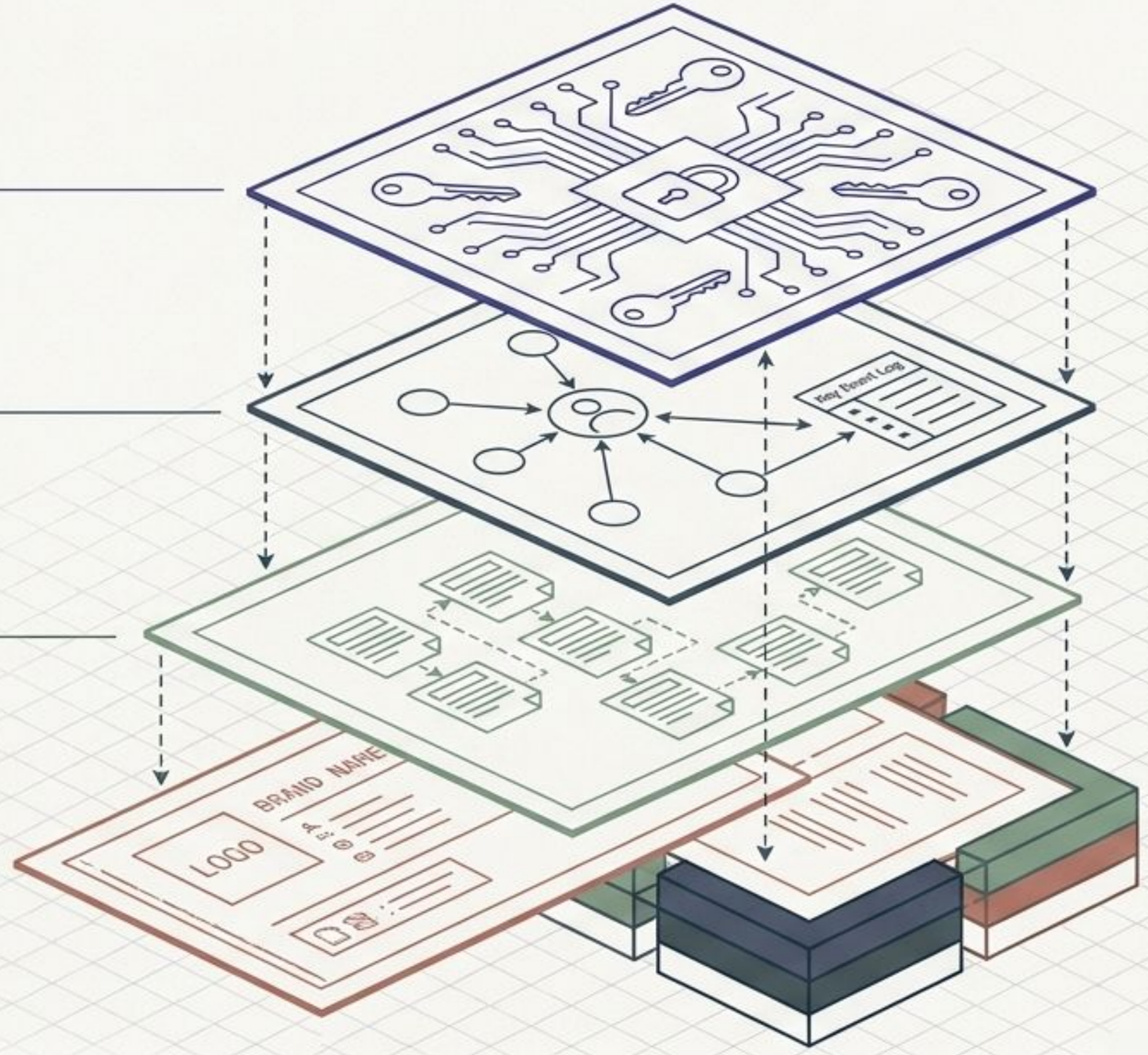
The Out-of-Band Introduction (OOBI) linking to the caller's Autonomous Identifier and Key Event Log (KEL).

Plate 3: evd Header

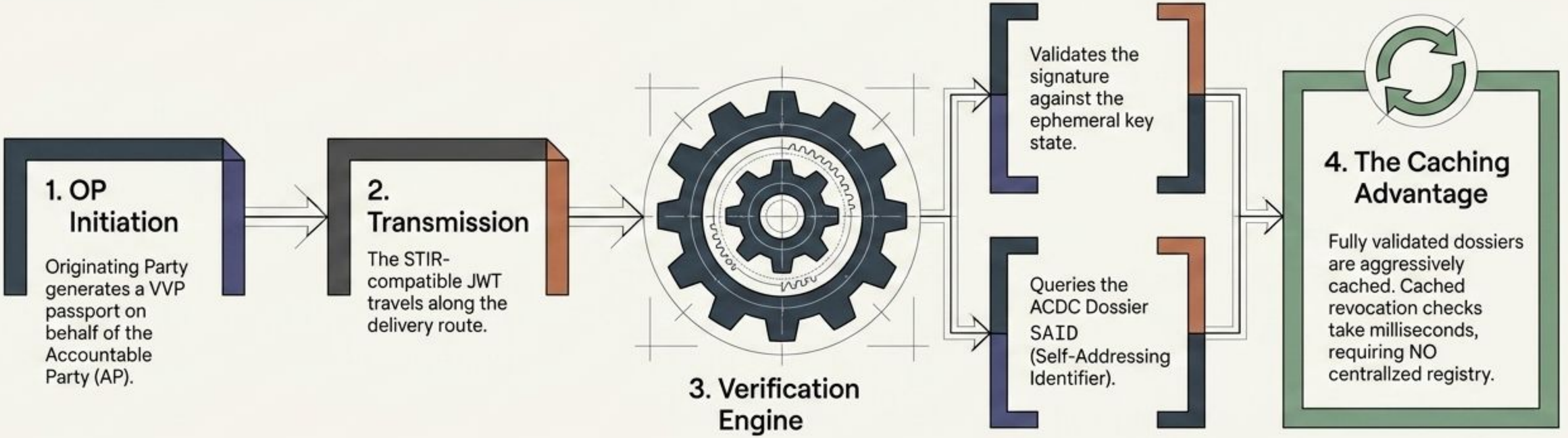
The OOBI linking directly to the Authentic Chained Data Container (ACDC) — the verifiable evidence dossier.

Plate 4: card & goal Claims

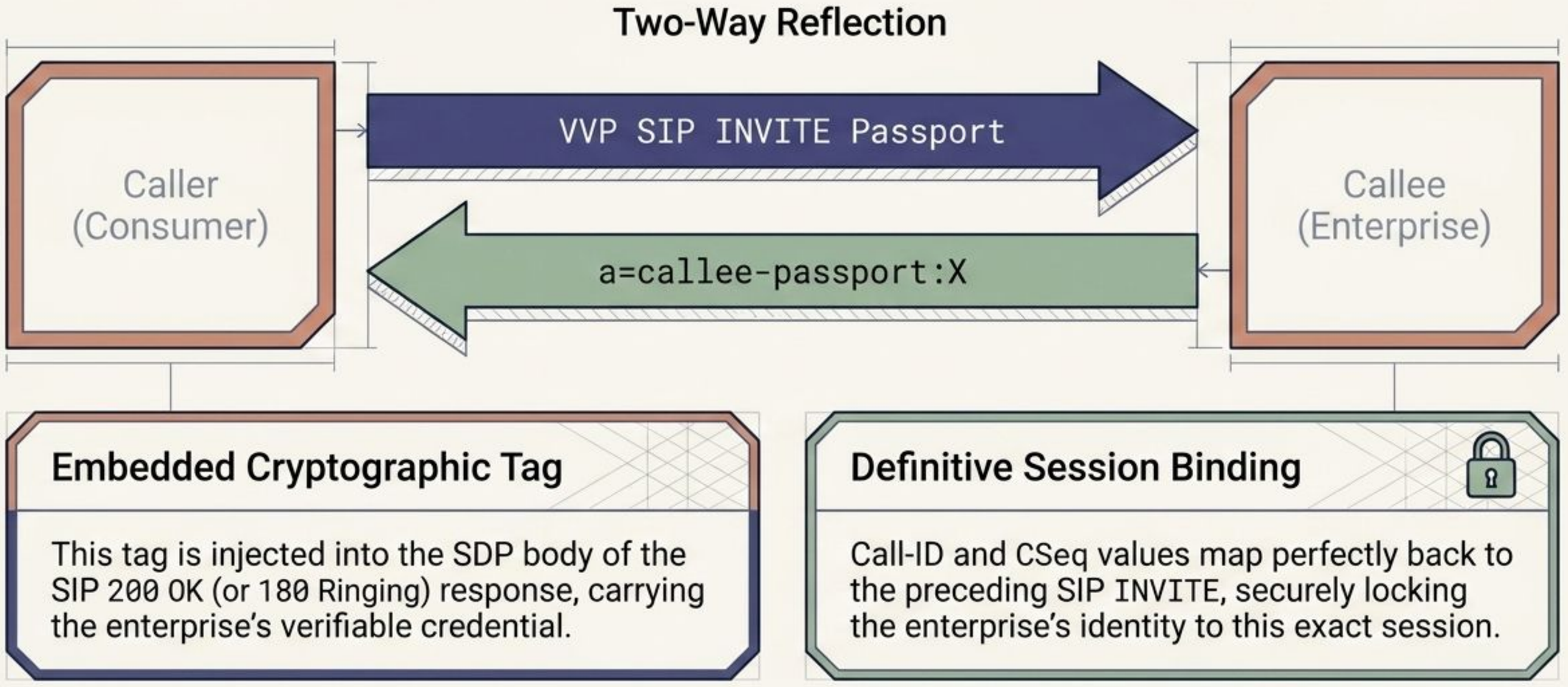
VCard-compliant brand attributes and machine-readable business intent.



The VVP engine separates ephemeral call data from long-term identity dossiers, enabling massive scalability through localized caching.



Cryptographic trust is bidirectional. VVP allows enterprises to cryptographically prove their identity to consumers, eliminating “Is this really my bank?” anxiety.



The CAMARA Verified Caller API translates protocol-level security into rich, operator-certified business cards on the consumer's screen.

By replacing anonymity with verified intent, enterprises drastically increase their effective connection rates.

Operator-Certified Information

Displays cryptographically backed identity rather than easily spoofed caller ID.

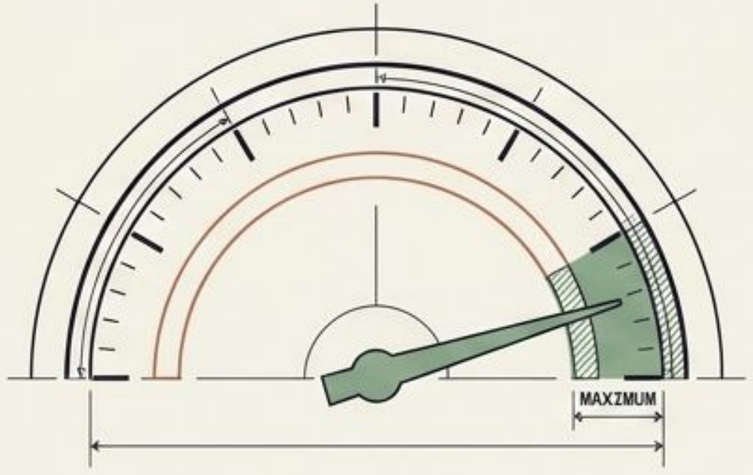
Multimedia Integration

Capable of displaying logos, verification badges, and secure video snippets.

Flexible Activation (Per-Call)

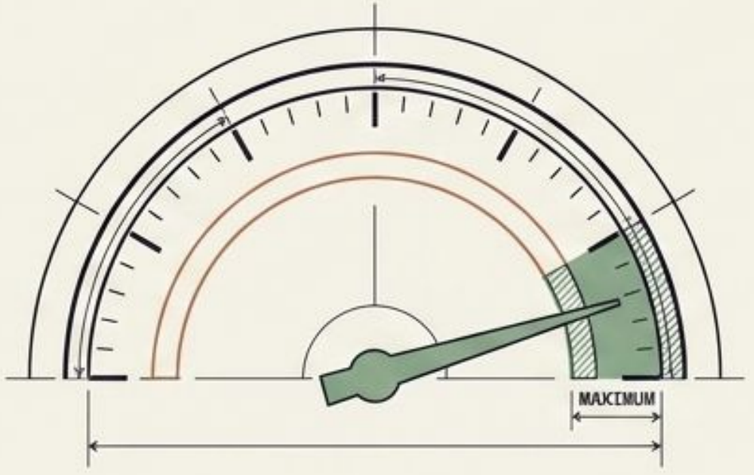
Enterprises activate features on a per-call basis, embedding specific, localized reasons for calling.

The live GSMA and Telefónica Tech pilot proved that decentralized identity can integrate seamlessly with legacy call center infrastructure.



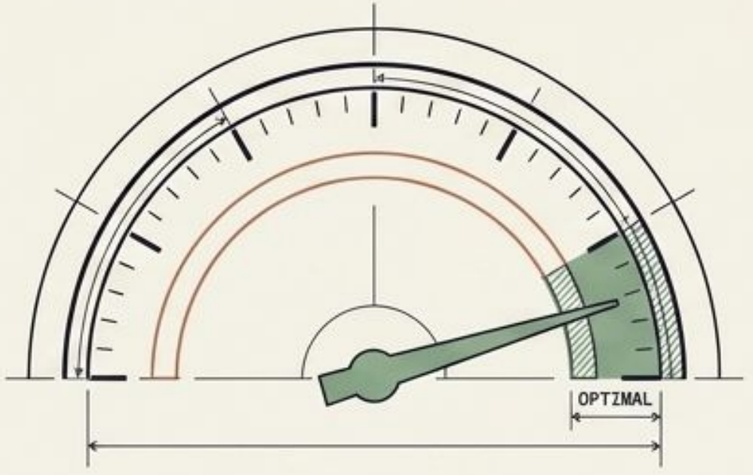
1. Seamless Integration

Successfully unified Dock Labs' decentralized ID stack, Telco Open Gateway APIs, and legacy call centers (Amazon Connect).



2. UX Acceptance

Achieved near-zero friction. Provided total privacy and control for consumers while delivering an exact operational fit for operators.

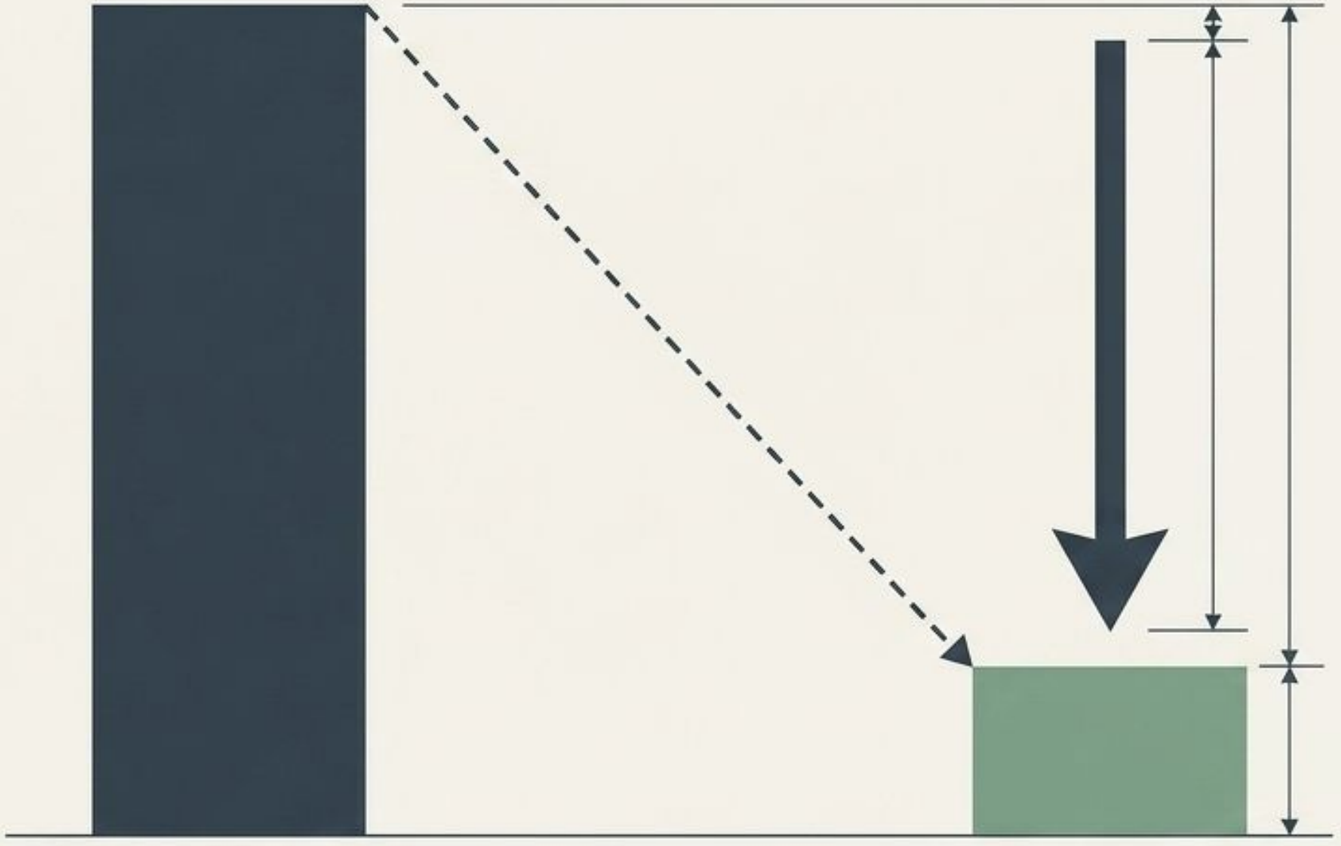


3. Connection Acceleration

Drastically slashed friction, reducing caller authentication time from minutes to seconds.

Cryptographic authentication slashes call handling times and effectively neutralizes the liability of insider data leakage.

ROI Waterfall Chart



Legacy KBA Auth:
$3.00 - $7.50 per call
(4-5 mins)

VVP Auth:
Pennies per call
(Seconds to Verify)

Insider Threat Mitigation

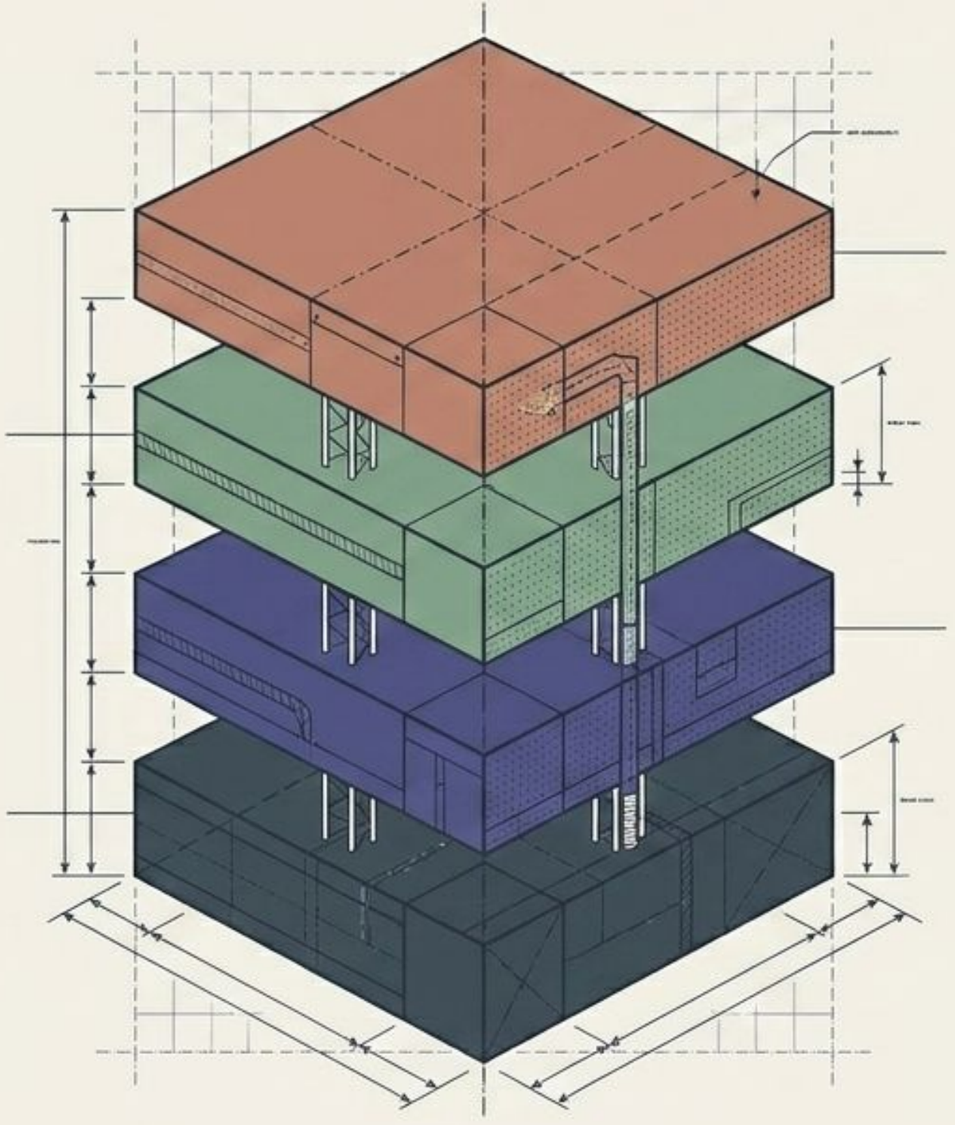
Less Data = Less Liability

Selective disclosure (wallet-based yes/no confirmation) completely removes sensitive data from the call center agent's view. This eliminates the risk of bribed agents extracting customer data, neutralizing Coinbase-style social engineering attacks.

The Unified Trust Ecosystem: A coordinated stack of open standards, global telco networks, and decentralized infrastructure.

Layer 4: The Surface (Infrastructure)
Truvera & Dock Labs decentralized edge wallets managing the user's verifiable credentials.

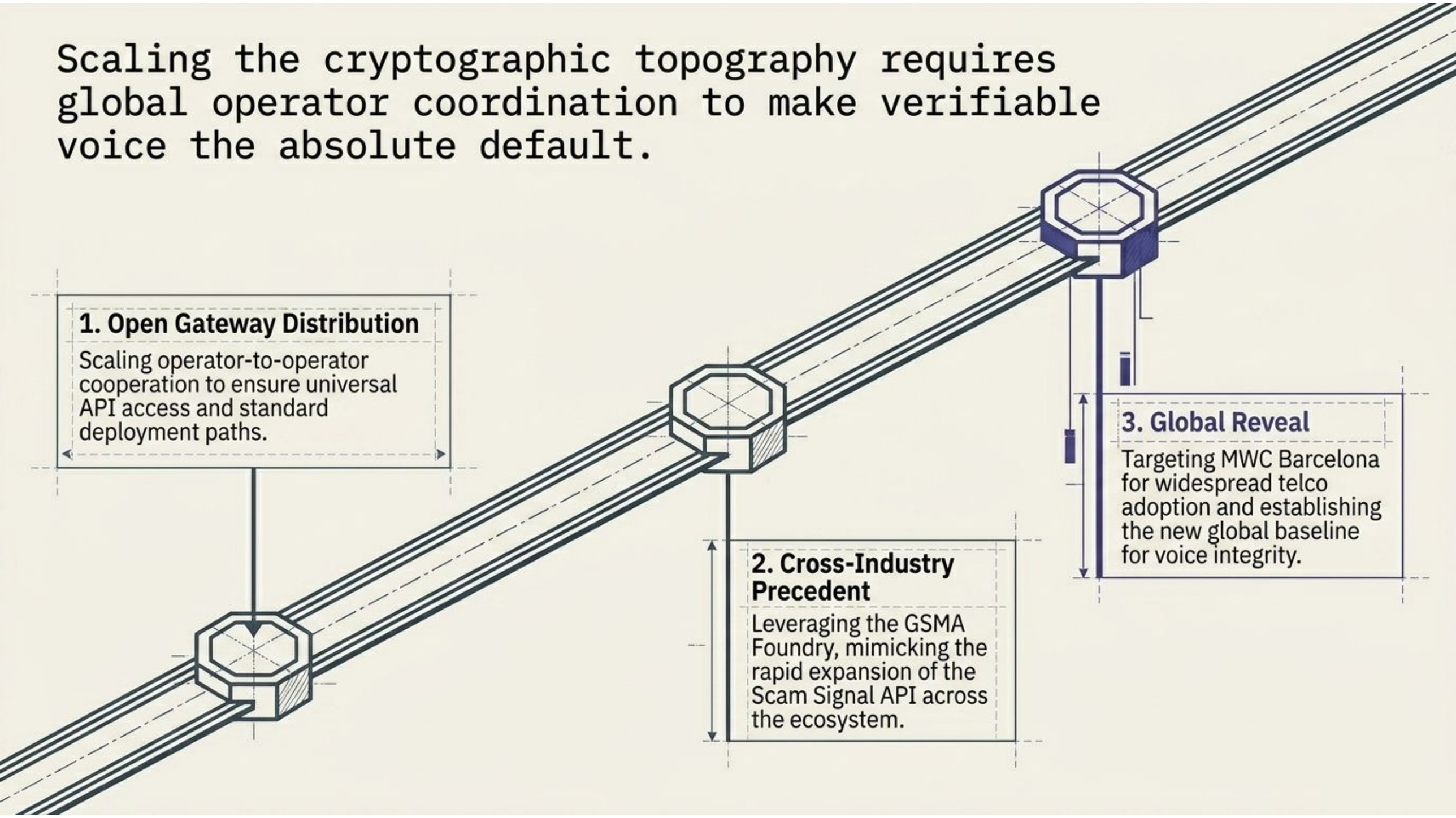
Layer 3: The Interconnect
CAMARA Open Gateway APIs ensuring standardized, cross-border enterprise access.



Layer 2: The Anchor (Root of Trust)
Telco SIMs and real-time GSMA network signaling APIs.

Layer 1: The Standard
IETF Verifiable Voice Protocol (VVP) providing the cryptographic engine.

Scaling the cryptographic topography requires global operator coordination to make verifiable voice the absolute default.



1. Open Gateway Distribution

Scaling operator-to-operator cooperation to ensure universal API access and standard deployment paths.

2. Cross-Industry Precedent

Leveraging the GSMA Foundry, mimicking the rapid expansion of the Scam Signal API across the ecosystem.

3. Global Reveal

Targeting MWC Barcelona for widespread telco adoption and establishing the new global baseline for voice integrity.