Verified Voice

Restoring Trust in Voice Communications

A Solution Blueprint for Identity Security in Telecomnunications

TelcoFutures.net

Verified Voice

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

Executive Summary

In an era where voice calls remain a cornerstone of personal and business communication, trust in the identity behind every ring is eroding. Caller ID spoofing, robocalls, SIM swap fraud, and sophisticated social engineering attacks have turned the public switched telephone network (PSTN) and mobile voice channels into vectors for financial crime, reputational damage, and consumer distrust.

Global losses from telephone-based fraud now run into tens of billions of dollars annually, while legitimate enterprises—from banks and healthcare providers to government services—struggle to reach customers securely over voice.

Traditional defenses such as STIR/SHAKEN frameworks, basic CNAM databases, and carrier-level filtering have delivered incremental progress but fall short against determined adversaries. This market report examines the evolving threat landscape, quantifies the economic and operational impact of identity insecurity in telecom services, and maps the technology, policy, and business models required for meaningful remediation.

Beyond the "Hello": A Comparative Guide to Voice Security

1. The Modern Trust Crisis in Voice Communication

Voice communication is currently in a state of systemic collapse. For decades, the sound of a ringing phone was a signal for connection; today, it is a liability. This erosion of trust is driven by **industrialized harm**—a massive scale of organized fraud that exploits the structural weaknesses of aging telephone networks.

The scale of this crisis is unprecedented. The Global Anti-Scam Alliance estimates global losses to scams exceeded **$1 trillion in 2024**, with a recovery rate of a mere 4%. These are not isolated "hacker" incidents; they are the output of industrialized call centers—often linked to organized crime and human trafficking—leveraging Generative AI to create synthetic identities and iterate on social engineering scripts at a pace traditional defenses cannot match.

Over half of adults worldwide report being a victim of a scam in the last year. Beyond the financial wreckage, the emotional impact is severe, leading to widespread anxiety, depression, and insomnia. Traditional "trust in the ringtone" has become a vector for trauma, as scammers successfully impersonate trusted financial and governmental institutions.

To restore the voice channel, we must bridge the gap between legacy vulnerabilities and hardware-anchored trust.

---

2. The Vulnerability Gap: Why Traditional Security is Failing

Traditional voice security relies on methods that were designed for a closed network environment. In today's interconnected, AI-augmented landscape, these legacy

methods are no longer fit for purpose.

Legacy Method	How it Works	The Security Flaw
CLI Spoofing	Relies on Caller Line Identity (the number on screen) as proof of identity.	Modern VoIP and interconnected networks make it trivial for scammers to "spoof" any number, facilitating high-stakes impersonation.
Knowledge-Based Authentication (KBA)	Agents verify identity by asking "security questions" (e.g., Mother's maiden name).	Requires users to disclose sensitive data, creating "honeypots" for hackers and enabling **insider/data leakage** scenarios.
SMS One-Time Passwords (OTP)	Sends a temporary numeric code via text message for out-of-band verification.	Structurally weak against **SIM swapping**, phishing, and interception. Scammers easily trick users into revealing these codes.

These methods rely on "something you know" or "something you have" (in a non-secure way), both of which are easily compromised by industrialized call centers.

---

3. The Solution: Decentralized Identity and the SIM Root of Trust

The paradigm shift required to secure voice is the move from centralized databases to **Decentralized Identity**. In this model, identity data is held under the control of the user on their device, rather than in a vulnerable central database. Mobile operators (Telcos) are the critical link here, as they control the **SIM-based root of trust**.

The Three Pillars of Trust

1. **The SIM (Subscriber Identity Module):** The hardware-based anchor that authenticates devices to the network hundreds of times per day.
2. **Network Signals (Carrier APIs):** Real-time signals—specifically the **Number Verify API** (confirming device possession) and the **SIM Swap API** (detecting recent unauthorized card changes)—provide dynamic risk assessments.
3. **Decentralized Wallets:** Secure containers at the "edge" (the device) that hold **Verifiable Credentials**. This facilitates a three-way trust model:
    - **Issuer:** The Telco issues a credential proving number ownership and network standing.
    - **Holder:** The user stores this proof in their digital wallet.
    - **Verifier:** The business (e.g., a bank) validates the credential cryptographically during a call without needing to contact the issuer in real-time.

---

4. Inside the Verifiable Voice Protocol (VVP)

The **Verifiable Voice Protocol (VVP)** is the cryptographically secure upgrade to Caller ID. It is designed as a **STIR-compatible JWT (JSON Web Token)**, allowing it to piggyback on existing STIR/SHAKEN standards while providing much richer evidence.

Dossier vs. Passport

- **The Dossier:** A stable, long-term collection of evidence (legal identity, right to use a number, brand attributes) curated in advance.
- **The Passport:** An ephemeral, "one-time-use" token created for a specific call. It cites the dossier but expires within 15–60 seconds to prevent replay attacks.

Restoring Accountability

VVP restores accountability by distinguishing between two critical roles:

- **Accountable Party (AP):** The organization or individual who has the legal right to the phone number and is accountable to regulators.
- **Originating Party (OP):** The technical entity (often a call center or UCaaS provider) actually placing the call.

The Technical Claims of a VVP Passport

A VVP Passport answers four essential questions for a receiver:

1. **Who is signing? (`kid` header):** Identifies the OP's cryptographic key state and its Out-of-Band Introduction (OOBI).
2. **What is the evidence? (`evd` claim):** A citation (OOBI) to the AP's Dossier, providing a verifiable data graph of authorizations.
3. **What is the brand? (`card` claim):** Contains operator-certified brand attributes (logos, name) justified by the dossier.
4. **What is the intent? (`goal` claim):** A machine-readable code (e.g., "fraud-alert") that the OP is authorized by the AP to use.

---

5. Comparative Analysis: Legacy Security vs. Verifiable Voice

The shift to VVP transforms caller authentication from a high-friction interrogation into a seamless, cryptographic background process.

Dimension	Traditional Method (KBA/OTP)	Verifiable Voice Solution (VVP)
Time to Authenticate	**4–5 Minutes:** Spent answering security questions or waiting for SMS codes.	**Seconds:** Authentication occurs cryptographically during the call setup.
Data Privacy	**Low:** Users must reveal PII to agents; creates data liability for the enterprise.	**High:** Uses **Selective Disclosure** (proof of attribute without disclosure of value).
Fraud Resistance	**Vulnerable:** Susceptible to CLI spoofing, phishing, and SIM swap fraud.	**Robust:** Anchored in SIM hardware and real-time network risk signals.

---

6. The "So What?" for the Everyday User

This technology delivers immediate, measurable impact for both the enterprise and the individual.

- **Financial ROI:** Call centers currently spend roughly **0.75–1.50 per minute** on call handling. By reducing authentication from minutes to seconds, VVP offers a massive reduction in operational overhead.
- **Proof of Attribute Without Disclosure of Value:** Instead of telling an agent your birthdate to prove you are "over 18," the wallet provides a "Yes/No" cryptographic confirmation. The agent never sees the sensitive data.

A major security risk involves "insider leaks"—where a bribed call center employee accesses customer data to facilitate social engineering (famously seen in the Coinbase-style scenarios). Because VVP uses wallet-based verification, the agent on the line **never sees** your security answers or sensitive identifiers. The "math" handles the trust, meaning there is no data for a dishonest employee to steal.

---

7. Conclusion: Restoring Trust in the Ringtone

The adoption of the Verifiable Voice Protocol and **CAMARA "Verified Caller" APIs** (within the GSMA Open Gateway framework) represents a significant upgrade to global communication. We are moving toward a future where "Who is calling?" is a question answered by mathematics and hardware-anchored proof, not guesswork or a scammer's script.

For industries such as **Government, Finance, Healthcare, and Education**, this technology is transformative. A hospital following up with a patient can see connection rates skyrocket simply because the recipient sees a certified logo and a verified "Reason for Call" on their screen.

Future Outlook

As these standards scale globally through the GSMA Open Gateway, expect:

- **Multimedia Business Cards:** Your phone will display operator-certified branding and video clips for incoming calls.
- **Two-Way Trust (vCon/RCS):** Verifiable evidence will flow in both directions, extending beyond voice to include **RCS (Rich Communication Services)** and **vCon** (verifiable conversations).
- **Cross-Border Interoperability:** Because VVP is decentralized and based on IETF/IARC standards, it can verify callers across international boundaries, finally closing the loophole exploited by cross-border fraud syndicates.

Technical Interoperability Assessment: Layering VVP, STIR/SHAKEN, and Camara APIs for Global Trust

1. Strategic Context of the Caller Authentication Crisis

The global telecommunications landscape is currently facing a systemic erosion of trust that threatens the viability of the voice channel. For decades, caller authentication has relied on easily spoofed Caller Line Identity (CLI) and fragile Knowledge-Based Authentication (KBA). However, the industrialization of fraud—now a $1 trillion annual crisis—and the rise of AI-driven synthetic identities have rendered these legacy methods obsolete. Transitioning to cryptographic frameworks is no longer an optional upgrade; it is a strategic necessity to secure the voice channel against attackers who leverage modern interconnected networks to bypass traditional defenses.

Based on industry analysis and the GSMA/Telefónica pilot findings, several structural "Trust Gaps" must be addressed:

- **Reliance on Spoofable Identifiers:** Legacy networks allow bad actors to impersonate legitimate entities via CLI spoofing with minimal effort.
- **Authentication Operational Costs:** Manual questioning and KBA are universal pain points, typically requiring 4–5 minutes per call and costing enterprises between $0.75 and $1.50 per minute in handling time.
- **Data Liability and Exposure:** Forcing customers to disclose sensitive personal information to agents creates significant security risks and compliance burdens under the "Data = Liability" paradigm.
- **Jurisdictional Trust Silos:** Existing standards like STIR/SHAKEN are often constrained by national boundaries, making the sharing of cross-border trust evidence logistically fraught.

To restore the integrity of global communications, we must move toward a multi-layered trust architecture defined by the Verifiable Voice Protocol (VVP).

2. The Verifiable Voice Protocol (VVP) as a Connectivity Bridge

The Verifiable Voice Protocol (VVP) is a Standards Track protocol for the Network Working Group designed to provide cross-jurisdictional trust. Its strategic role is to enable the sharing of rich, independently verifiable evidence between callers and callees, regardless of the underlying network provider or national jurisdiction.

VVP functions as technical "glue" that enhances existing STIR/SHAKEN frameworks. It utilizes the STIR framework to bind cryptographic evidence to SIP INVITEs via a specialized VVP PASSporT. Crucially, VVP can provide the necessary out-of-band evidence to justify a SHAKEN "A" attestation when a call originates outside a national ecosystem, bridging the gaps between disparate national service provider environments.

Category	Traditional STIR/SHAKEN Model	VVP Integrated Model
Evidence Scope	Provider-level signatures; limited identity proof.	Rich dossiers (ACDCs); proves legal identity and delegation.
Governance Assumptions	Centralized by jurisdiction; set of known signers.	Decentralized; uses AIDs and cross-border evidence.
Deployment Cost	High maintenance and infrastructure overhead.	Lower; simpler deployment via decentralized caching.

This architectural approach ensures that identity evidence is not merely ephemeral but is anchored in a stable, persistent structure known as the "Dossier."

3. The Dossier Framework: Decentralized Identity Rooted in KERI

The VVP transition from ephemeral signatures to stable, curated evidence is managed through the "Dossier" framework. This move is essential for establishing non-repudiable trust for both callers and callees, as it provides a persistent record of identity evidence that can be cited in real-time.

The VVP model defines three critical roles for the Verified Party (VP):

- **Accountable Party (AP):** The entity (organization or individual) that owns the phone number and is legally accountable for the call.
- **Originating Party (OP):** The technical entity (call center, UCaaS provider, or SBC) that initiates the SIP INVITE.
- **Verified Party (VP):** The party using VVP to prove assertions about itself (either the AP or the Callee).

The dossier provides the cryptographic proof of the delegation relationship between the AP and the OP, ensuring that a specific call center is authorized to represent a brand. Technically, the VVP PASSporT utilizes two core components:

- **`kid` (Key Identification):** This header uses the Out-of-Band Introduction (OOBI) of an Autonomous Identifier (AID). These identifiers facilitate "viral discoverability" and are managed via **Key Event Receipt Infrastructure (KERI)**, providing an immutable audit log of key state evolution.
- **`evd` (Evidence):** This required claim points to an **Authentic Chained Data Container (ACDC)**—the dossier itself. ACDCs utilize Self-Addressing Identifiers (SAIDs) to create a "tamper-evident relationship" across the data graph, allowing for efficient caching and verification of the entire delegation chain.

Linking these decentralized identifiers to real-time network signals provides a definitive root of trust.

4. Integrating Camara Project APIs and GSMA Root of Trust

Mobile operators possess a unique strategic advantage as a "Root of Trust" because they authenticate subscribers via the SIM (Subscriber Identity Module). By integrating Camara Project APIs, telcos can secure the entire lifecycle of a verifiable credential, from issuance to real-time revocation.

The impact of Camara and GSMA Open Gateway APIs is transformative:

- **Number Verify & SIM Swap APIs:** These APIs secure the issuance of credentials by confirming device possession and checking for recent account takeover indicators. Strategically, they also enable **real-time revocation**; if a SIM swap is detected, the associated identity credentials can be automatically invalidated.
- **Verified Caller API:** This API enhances the "Verified Business Card" experience by allowing operator-certified information, including **multimedia (video**

clips/SMS) and logos, to be displayed on the called party's screen.

The technical workflow demonstrated in the GSMA/Telefónica pilot is as follows:

1. **Issuance:** The mobile operator uses Number Verify and SIM Swap APIs to secure the issuance of a verifiable credential.
2. **Storage:** The user (Holder) receives the credential in a secure digital wallet.
3. **Initiation:** Upon making a call, the credential generates a VVP PASSporT.
4. **Verification:** The verifier (e.g., an Amazon Connect call center) validates the PASSporT and checks network risk signals before the agent answers, significantly reducing call handling time.

These protocols collectively enable a seamless, real-time verification experience for both parties.

5. Multi-Layered Verification Mechanics and Performance Optimization

Rigorous verification is necessary to mitigate the computational burden of deep evidence chains, which VVP achieves through strategic caching of SAIDs and localized data reuse.

The verification algorithm for a VVP PASSporT MUST follow these steps:

1. **Temporal Analysis:** Check `iat` (issued at) and `exp` claims. PASSporTs SHOULD have aggressive timeouts (e.g., 15–30 seconds) to prevent replay attacks.
2. **Cryptographic extraction:** Extract the `kid` header and fetch the Key Event Log (KEL). The `alg` claim **MUST** be **EdDSA** or **FN-DSA**; RSA, HMAC, and ES256 **MUST NOT** be used.
3. **Signature & Witness Validation:** Verify the signature using the OP's public key from the KEL. Key state MUST be checked against independent **Witnesses** to detect duplicity.
4. **Dossier Validation:** Use the **SAID** as a lookup key for cached validation. If not cached, traverse the ACDC data graph, checking each signature against the issuer's key state at the time of issuance.

Two-Way Assurance (Callee Verification): VVP supports two-way trust where the Callee is also a VP. The Callee proves identity by adding an `a=callee-passport:X` attribute to the SDP body of the SIP response (200 OK). This response PASSporT

MUST include the `call-id` and `cseq` from the original INVITE to bind the proof to the specific dialog.

Furthermore, VVP enables **Historical Analysis**. Unlike standard JWTs, the KERI-based KEL allows verifiers to determine if a PASSporT was valid at a specific moment in the past, facilitating non-repudiable auditing and dispute resolution.

6. Security Outcomes and Ecosystem Scaling

The integration of VVP and Camara APIs drives the "Less Data = Less Liability" paradigm, where callers are authenticated via cryptographic attestations rather than the exchange of PII.

Implementers must prioritize several security outcomes:

- **Compromise Recovery:** VVP utilizes **Prerotation**, a KERI mechanism that allows for recovery from key compromise by pre-committing to future keys, ensuring long-term dossier stability.
- **Multi-Signature Schemes:** Credential issuers SHOULD employ threshold-based multi-sig schemes for their AIDs to prevent single-point-of-failure compromises.
- **Replay Prevention:** Rigorous adherence to `iat`/`exp` windows and JTI tracking ensures that captured PASSporTs cannot be reused.

Scaling this architecture is driven by the **GSMA Foundry** and the **Open Gateway** initiative, which provide the global distribution path for standardized Telco APIs. By layering VVP's decentralized dossiers over the telco's SIM-based root of trust, the industry can finally restore transparency, efficiency, and security to the global voice channel.

The Trust Triangle: How Your Phone Proves You're You Without Saying a Word

1. The Crisis of Trust in Our Pockets

In the modern digital landscape, proving your identity over a phone call has devolved into a full-scale "Trust Crisis." Traditional methods are no longer merely inefficient; they have become engines for "industrialized harm." This systemic failure is exploited by global fraud syndicates—often linked to human trafficking operations in Southeast Asia—resulting in staggering financial losses and severe emotional trauma, including anxiety, depression, and insomnia for victims.

Analyze the structural collapse of traditional methods below:

Traditional Authentication	Core Vulnerabilities	Resulting Impact
Knowledge-Based Auth (KBA)	Relies on "shared secrets" (SSN, mother's maiden name); creates massive **data honeypots**.	**Systemic Risk:** Centralized databases are prime targets. If the call center is breached, your identity is stolen.
SMS One-Time Passwords (OTP)	Vulnerable to SIM swapping, phishing, and interception.	**Security Friction:** High-stress waiting periods for codes that can be diverted to attackers.
Caller Line Identity (CLI)	Trivial to spoof on modern interconnected networks.	**Spoofing:** Scammers easily impersonate trusted brands, eroding the integrity of the voice channel.

Key Insight: Traditional methods actually increase risk by requiring users to reveal the very data they are trying to protect. Once a "shared secret" is shared, it is no longer a

secret; it becomes a liability for the enterprise and a target for criminals.

To solve this, we must transition from a model of sharing secrets to an architectural model anchored in cryptographic proof: The Trust Triangle.

---

2. Meet the Trust Triangle: The Three Pillars of Identity

The Trust Triangle is a decentralized framework that redistributes the power of identity. Instead of relying on a vulnerable central database, trust is established through three distinct roles:

- **The Issuer**
  - *Role:* The authority that verifies a fact and secures it with a digital seal.
  - *Real-World Identity:* The **Mobile Operator** (Telco). They issue credentials confirming you own a specific number and device.
- **The Holder**
  - *Role:* The individual who receives the credential and maintains it in a secure "digital wallet" on their device.
  - *Real-World Identity:* **You (the User)**. You control exactly when and with whom you share proof.
- **The Verifier**
  - *Role:* The entity—such as a bank or health provider—that must confirm your identity.
  - *Real-World Identity:* The **Call Center or Brand**.

Key Insight: The brilliance of this triangle lies in **cryptographically signed proofs**. This allows the Verifier to validate a credential instantly and privately without ever needing to contact the Issuer to ask for permission.

While this triangle provides the functional shape of the system, the Mobile Operator provides the physical foundation of truth through the SIM card in your hand.

---

3. The Mobile Operator: The "Root of Trust" and the SIM

Telecommunications companies possess a unique advantage in the identity ecosystem:

the SIM (Subscriber Identity Module). This isn't just a chip for cellular service; it is a physical "Root of Trust." Your device authenticates itself to the network hundreds of times per day, creating a continuous, high-assurance heartbeat of identity that no password can match.

By exposing "Network Risk Signals" via real-time APIs, Telcos can now share critical security context without revealing personal data:

Signal Type	Why it Matters for Trust
SIM Swap Check	Instantly detects if a SIM card was recently changed, flagging a hijacked account.
Number Recycling	Ensures a credential is not linked to an old owner after a number reassignment.
Real-time Lifecycle Events	Tracks port-outs, disconnects, and reconnects to maintain a continuous chain of trust.
Number Verify	Confirms in real-time that the person on the call is in physical possession of the device.

Key Insight: Because the network verifies the device "hundreds of times per day," the mobile phone is the ultimate anchor for proving identity. We are moving from "what you know" (which is easily stolen) to "what you have"—a cryptographically secured device backed by real-time network intelligence.

This "root of trust" moves from the network into the user's hand via a Digital Identity Wallet.

---

4. The Digital Identity Wallet: Your Privacy Shield

A Digital Identity Wallet uses **Decentralized Identity** and **Verifiable Credentials** to flip the script on privacy. Using a process called **Selective Disclosure**, your identity is

reduced from a file of sensitive documents to a simple, unhackable confirmation.

The Selective Disclosure Process:

1. **The Request:** The Verifier (Call Center) sends a digital request for proof to your wallet.
2. **The Check:** The Wallet validates credentials issued by your Telco and your own biometric.
3. **The Proof:** The Wallet generates a "simple yes/no confirmation" or a specific, signed proof.
4. **The Shield:** The Verifier receives the proof without ever seeing the underlying personal data.

Key Insight: "Less Data = Less Liability." This model eliminates the "Insider Threat." In traditional call centers, bribed agents (a common factor in major data breaches) can steal customer data because they can see it. With a wallet, the agent never sees your data—only the proof that you are verified. This significantly reduces the enterprise's compliance burden under regulations like GDPR.

This shift from data-sharing to proof-sharing transforms the call center from a point of friction to a point of efficiency.

---

5. From Minutes to Seconds: The Impact of Verified Calls

Replacing Knowledge-Based Authentication with wallet-based verification is a quantum leap in operational efficiency. Recent Proof of Concept (PoC) simulations—utilizing environments like **Amazon Connect**—demonstrate that this isn't just a security upgrade; it’s a massive ROI driver.

The Efficiency Transformation

Traditional Call Center KPIs	PoC Security & User Outcomes
4–5 Minute Auth Time: Callers waste minutes being interrogated by	**Seconds-Long Auth:** Verification occurs almost instantly via the wallet interaction.

strangers.	
High Operational Cost: Each minute of a call costs an enterprise **0.75–1.50**.	**Drastic ROI:** Reducing auth time by minutes saves millions in monthly operational expenses.
Vulnerable to Spoofing: Relies on easily faked Caller ID (CLI).	**Eliminated Fraud Paths:** Cryptographic proof eliminates CLI spoofing, phishing, and social engineering.

Key Insight: For you, the "Holder," the benefit is total control. You gain the power to prove your identity in seconds without sacrificing your privacy or your time.

This system is rapidly evolving from a localized pilot into a global architectural blueprint.

---

6. The Global Blueprint: Scaling Trust with Open Standards

To achieve global scale, trust must act as "glue"—bridging different jurisdictions and carriers. This vision is being realized through three essential pillars of coordination:

- **Open Gateway APIs:** Standardized technical "doors" that allow any enterprise to access Telco security signals globally.
- **GSMA Coordination:** The global industry body driving cross-operator collaboration to ensure your identity works wherever you travel.
- **Verifiable Voice Protocol (VVP):** A groundbreaking standard that enables **Two-way evidence sharing**.

Key Insight: The Verifiable Voice Protocol (VVP) represents the pinnacle of this movement: **Mutual Trust**. It allows the bank to prove itself to the customer just as much as the customer proves themselves to the bank. This two-way verification ensures that when you pick up the phone, you are as protected as the institution you are calling.

Trust is restored to our communications when identity is anchored in technology, not shared secrets. This new global standard, recently showcased at **MWC Barcelona**, marks the end of the era of industrialized fraud and the beginning of the era of verified

truth.

Strategic Implementation Roadmap: Transitioning to Decentralized, Cryptographically Secure Caller Verification

1. The Strategic Imperative for Identity Transformation

The global voice channel is facing a crisis of confidence that has transcended "fraud" and evolved into a regime of **industrialized harm**. With global scam losses estimated at over $1 trillion in 2024 and a staggering recovery rate of only ~4%, these operations represent a systemic threat to enterprise viability.

More critically, these scams are increasingly orchestrated by organized crime syndicates linked to human trafficking and forced labor operations in Southeast Asia. For the modern enterprise, maintaining legacy authentication is no longer just an operational inefficiency; it is a profound regulatory and ESG risk. The transition from vulnerable, centralized databases to decentralized, hardware-anchored models is a strategic necessity to restore fundamental consumer trust.

The structural weaknesses of Knowledge-Based Authentication (KBA) and SMS-based One-Time Passwords (OTPs) have been laid bare. KBA relies on static PII widely available on the dark web, while SMS OTPs are trivial to intercept via SIM swapping or Caller Line Identity (CLI) spoofing. These legacy methods force organizations to act as honeypots for sensitive data, increasing the "blast radius" of any inevitable breach.

Legacy vs. Decentralized Authentication: A Strategic Comparison

Method	Root of Trust	Primary Weakness	Enterprise Liability
Knowledge-Based (KBA)	Static PII (SSN, DOB, etc.)	Data is leaked/dark web; easily social-engineered.	High: Must store and protect massive PII databases.

SMS One-Time Password	Network-sent code	Vulnerable to SIM swapping, CLI spoofing, and interception.	Moderate: Regulatory risk and friction-heavy UX.
Decentralized (SIM-Based)	SIM Cryptography & Network Signals	Requires ecosystem coordination and wallet adoption.	**Low**: "Selective Disclosure" allows verification without PII storage.

Operationally, the status quo is unsustainable. GSMA benchmarks indicate that manual KBA-based authentication consumes **4 to 5 minutes** per call, with operational costs ranging from **$0.75 to $1.50 per minute**. By shifting the root of trust, organizations can reclaim this lost productivity while neutralizing the industrialized threat landscape.

2. The Architectural Foundation: SIM-Based Root of Trust and Decentralized Identity

To mitigate the risks of centralized data silos, enterprises must adopt a **"User-in-the-Loop" model**. This architecture shifts the storage of identity credentials to the "edge"—specifically to a digital wallet on the user's mobile device—anchored by telecommunications infrastructure. This moves the organization away from being an identity provider to becoming a verifier of high-assurance network signals.

The Three Roles of the Decentralized Model

- **Issuer:** The Mobile Network Operator (MNO) issues a verifiable credential proving the subscriber's control of a phone number and device.
- **Holder:** The user secures these credentials in a digital identity wallet on their mobile device.
- **Verifier:** The enterprise validates the credential in real-time during a call interaction.

The strategic advantage of this model is the **Subscriber Identity Module (SIM)**. Unlike third-party apps, the SIM is a hardware root of trust. Telecommunications networks are uniquely positioned for this role because they authenticate devices and subscribers

hundreds of times per day as part of standard network operations.

Mitigating Fraud with Camara Project APIs

This architecture is fortified by real-time network signals via **Camara Project APIs**, which provide a dynamic layer of intelligence that static databases cannot match:

- **Number Verify API:** Seamlessly confirms that the user initiating the session is in physical possession of the device and phone number associated with the credential.
- **SIM Swap API:** Detects recent hardware changes. If a SIM swap occurred within a high-risk window (e.g., the last 24 hours), the system can automatically trigger re-authentication or revoke the credential.
- **Number Recycling Signal:** A critical lifecycle management tool that automatically revokes or invalidates credentials if a phone number is decommissioned or reassigned, preventing "zombie" identities from being exploited by new owners.

Selective Disclosure: Less Data = Less Risk

By utilizing **Selective Disclosure**, the verifier only receives the specific proof required for the transaction (e.g., a "yes/no" cryptographic confirmation) rather than the underlying PII. This principle ensures that the enterprise minimizes its data footprint, directly reducing its liability under global privacy regulations.

3. Technical Framework: The Verifiable Voice Protocol (VVP)

The Verifiable Voice Protocol (VVP) bridges the gap between existing STIR/SHAKEN standards and the decentralized identity ecosystem. It introduces richer evidence that remains verifiable across jurisdictional boundaries, solving the logistical hurdles of cross-border telecom governance.

The VVP Lifecycle

The protocol operates through a distinct three-step chronological flow:

1. **Curation:** The party curates a **"Dossier"** (stable evidence). This is a long-lived collection of credentials proving legal identity, right to use a phone number, and organizational affiliations.
2. **Citation:** For each call, the system generates a **"Passport"** (ephemeral

evidence). This is a lightweight, short-lived JWT that "cites" the dossier to prove identity for that specific interaction.
3. **Verification:** The verifier checks the passport signature and the cited dossier, including real-time revocation status, to make an authentication decision.

Two-Way Verification and the Camara "Verified Caller" API

VVP enables **Two-Way Verification**, allowing the callee to verify the enterprise's identity. This is supported technically by the **Camara Verified Caller API**, which allows operator-certified "business card" information—including **certified logos, SMS notifications, and video clips**—to be displayed on the customer's phone screen before they answer. This dramatically improves connection rates and protects brand integrity against spoofing.

Security Requirements and Cryptographic Rigor

To ensure long-term resilience, VVP mandates the use of modern cryptographic schemes:

- **Required Algorithms:** Implementations MUST use **EdDSA** or post-quantum algorithms, specifically **FN-DSA-512**.
- **Prohibited Legacy Schemes:** To prevent degradation of the trust ecosystem, the use of **RSA, HMAC, or ES256** is explicitly prohibited.

4. Operational Excellence: Optimizing Call Center KPIs

Cryptographic authentication transforms the call center from a friction-heavy cost center into a high-trust customer experience hub. Replacing "security interrogations" with automated proofs yields immediate, measurable improvements in operational health.

Measurable KPI Improvements

- **Reduced Average Handle Time (AHT):** Authentication moves from 4-5 minutes of KBA questioning to seconds of automated, **biometric-bound credential** checks.
- **First Call Resolution (FCR):** Starting calls with established trust allows agents to bypass friction and move directly to issue resolution.
- **Customer Satisfaction (CSAT):** Eliminating intrusive security questions reduces the "psychological burden" on the customer, improving brand sentiment.

Neutralizing the "Insider Threat"

The VVP model addresses the "Insider Threat" scenario, exemplified by **"Coinbase-style" breaches** where call center agents were bribed or social-engineered to extract customer PII. By using wallet-based verification, agents never see sensitive customer data; they only see a system confirmation of successful verification. When combined with **biometric-bound credentials** (ensuring the presenter is the authorized holder), the risk of agent-facilitated social engineering is effectively eliminated.

5. Implementation Roadmap and Ecosystem Integration

Scalability requires industry coordination through the **GSMA Open Gateway** and **GSMA Foundry**, ensuring that these protocols work across carrier boundaries and prevent new "identity silos."

Three-Phase Implementation Guide

- **Phase 1: Pilot and Integration:** Integrate **Decentralized Identity Stacks** (e.g., Truvera or Dock Labs) with existing platforms like Amazon Connect. Leverage Camara APIs (Number Verify, SIM Swap) to add immediate risk signals to legacy flows.
- **Phase 2: Credential Issuance:** Transition the enterprise to a "Verifier" role. Establish the organization as an "Issuer" for employee credentials to prove delegated authority.
- **Phase 3: Global Scaling:** Adopt VVP for cross-border interoperability, utilizing branded calling and two-way verification to ensure consistent trust in international voice traffic.

KERI and Historical Analysis for Compliance

VVP utilizes **Key Event Receipt Infrastructure (KERI)** to provide a non-repudiable audit log. By maintaining **Key Event Logs (KELs)** and utilizing **Witnesses**, enterprises can perform "Historical Analysis." This allows an auditor to verify whether a specific call was valid at an arbitrary point in the past, even if keys have since been rotated. This witness-based infrastructure provides the ultimate architectural guarantee for regulatory compliance and fraud investigations.

By following this roadmap, enterprises can move beyond the "industrialized harm" of the legacy voice channel and restore cryptographic certainty to every interaction.

Why Your Phone is Finally Learning to Tell the Truth: 5 Takeaways from the Future of Caller Identity

The voice channel has become a digital wasteland—a high-friction, low-trust attack surface where the "Unknown Caller" label is less a mystery and more a threat. According to the Global Anti-Scam Alliance, the scale of this trust deficit is staggering: global scam losses breached $1 trillion in 2024, with a abysmal 4% recovery rate. For over half the world's adult population, the simple act of answering the phone has become an exercise in anxiety.

We have all endured the "security theater" of the modern call center: sitting through a gauntlet of "What was the name of your first pet?" questions or waiting for a spotty SMS code to arrive. But a new alliance between the GSMA, Telefónica, and the architects of decentralized identity protocols is about to change the math. By shifting authentication from knowledge-based hurdles to cryptographically secure proof, the industry is moving toward a world where your phone doesn't just display a number—it presents a verifiable identity.

---

1. The Death of the "Security Question" (and the 5-Minute Wait)

The "mother's maiden name" interrogation is a relic of a pre-data-breach era—a security theater that has become a liability for everyone involved. Traditional Knowledge-Based Authentication (KBA) and SMS-based One-Time Passwords (OTPs) are structurally weak; hackers can find your first pet's name in a data dump, and "SIM swap" attacks can intercept your codes in real-time.

Current verification flows are agonizingly slow, often burning four to five minutes of a customer's time before the actual problem is even addressed. In the enterprise world, this friction is expensive: industry benchmarks suggest call center costs range from $0.75 to $1.50 per minute.

Analysis: Moving to a "yes/no" confirmation via a digital wallet doesn't just save time; it

fundamentally re-engineers risk. By eliminating the need to store sensitive personal data, enterprises remove the "honeypot" that attracts hackers. This reduces the risk of "Coinbase-style" insider leakage—where bribed call center agents extract customer data for targeted social engineering. Less data held in a central database means less liability for the brand.

2. Your SIM Card is the New "Root of Trust"

The secret weapon in this new landscape is already in your pocket: the SIM card. While current systems like STIR/SHAKEN rely on the signatures of originating service providers, they often lack independently verifiable proof. The new model uses the SIM as a unique "Root of Trust," leveraging real-time network signals—like SIM swap detection and number recycling—to ensure a caller is who they claim to be.

This decentralized model utilizes three distinct roles:

- **The Issuer:** The mobile operator, who issues a credential proving ownership of the phone number.
- **The Holder:** The user, who secures that credential in a device-based digital wallet.
- **The Verifier:** The brand or call center that validates the credential instantly.

To ensure this trust isn't brittle, the protocol incorporates **Key Event Receipt Infrastructure (KERI)** and **Authentic Chained Data Containers (ACDC)**. These allow for non-repudiable, publicly accessible audit logs (Key Event Logs or KELs) of how a key state evolves. If a key is compromised, "prerotation" enables recovery without destroying the underlying identity.

"Telcos are reacting to a broader trust crisis... The strategic goal: restore trust in communications by bringing stronger proof into voice interactions."

3. Two-Way Trust: Why Knowing Who *You* Are Calling Matters

Trust is a two-way street, yet current protocols focus almost exclusively on identifying the caller. The upcoming **Verifiable Voice Protocol (VVP)** introduces mutual authentication, allowing evidence to flow from the callee back to the caller.

Under VVP, organizations curate a **"Verifiable Dossier"**—a stable data graph of evidence that includes **TNAlloc (Telephone Number Allocation)** credentials. This

proves not just who the company is, but their specific legal "right to use" that number.

The technical handshake is elegant: while the caller uses the Identity header in a **SIP INVITE**, the callee responds by placing an attribute line in the **SDP (Session Description Protocol) body** of their SIP response. This signed citation allows the caller to verify the organization they've reached before a single word is spoken.

Analysis: This is a game-changer for enterprise credibility. Consider the "hospital follow-up" use case: patients routinely ignore legitimate medical calls out of fear of insurance scams. By providing a verifiable identity to the callee, a hospital can prove its authority and brand before the patient even answers, transforming a "blocked" call into a life-saving connection.

4. The Rise of the "Multimedia Business Card"

We are entering the era of the "Verified Caller." Moving beyond the easily spoofed Caller ID (CLI), the **Camara Project** is developing APIs that allow businesses to display operator-certified multimedia business cards directly on the recipient's screen.

These cards are not just unverified graphics; they are backed by the mobile operator's root of trust and can include:

- Official brand logos and color schemes.
- Video clips or SMS previews explaining the purpose of the call (e.g., "Your delivery is 2 minutes away").
- A "Verified" badge that is only triggered once the cryptographic handshake is successful.

Analysis: This visual verification is the front line against the "industrialized harm" of CLI spoofing. By vividly displaying professional identity through a secure, operator-certified channel, legitimate services can dramatically improve connection rates. It replaces "answer anxiety" with "verified authority," ensuring that a bank's fraud alert is actually seen as a fraud alert, not just another telemarketing annoyance.

5. Fighting Industrialized Fraud in the Age of AI

It is a mistake to view phone fraud as the work of isolated hackers. Scams have become "industrialized," with investigations linking global call-center fraud operations to human trafficking and forced labor. Furthermore, Generative AI is now accelerating

"synthetic identity fraud," making it impossible for human agents to spot a fake caller through manual questioning alone. AI-driven voice clones can mimic a loved one or a CEO with terrifying accuracy.

Analysis: In this environment, cryptographic verification is no longer an optional luxury; it is a baseline necessity. Manual verification in an age of GenAI is essentially a form of negligence. When fraud is industrialized and AI-driven, only a high-tech infrastructure built on mathematical proof—using KELs to audit key transitions and ACDCs to chain evidence—can effectively combat global criminal networks.

Conclusion: A New Standard for Connection

The blueprints for this trusted network are moving from theory to production. With the **GSMA Open Gateway** initiative providing the distribution path, these aren't just theoretical protocols—they are APIs that developers can call today. As the industry prepares to showcase the results of these pilots at **MWC Barcelona**, we are seeing the emergence of a new standard for human connection.

In a world of deepfakes and industrialized spoofing, the "mother's maiden name" is dead. The question for every consumer and enterprise is simple: Can we afford to rely on anything less than cryptographic proof? As the SIM-based digital wallet moves to the center of our lives, the phone call might finally become what it was always meant to be: a trusted bridge between two people. Would you feel safer answering your phone if every ring was backed by a mathematical guarantee?

The Future of Verifiable Caller Identity and Authentication

Executive Summary

The voice communication channel is currently facing a profound trust crisis, driven by the industrialization of fraud and the obsolescence of traditional authentication methods. Current security measures, such as Knowledge-Based Authentication (KBA) and SMS One-Time Passwords (OTPs), are increasingly ineffective and create significant operational friction and data liability. In response, a new paradigm is emerging—led by organizations like GSMA, Telefónica, and the proponents of the Verifiable Voice Protocol (VVP)—that leverages decentralized identity and telecommunications network signals as a new "root of trust."

This briefing document outlines the transition toward cryptographically secure caller authentication. Key takeaways include:

- **The Inefficacy of Current Systems:** Traditional methods like Caller Line Identity (CLI) are easily spoofed, while KBA forces the storage of sensitive data that attracts attackers.
- **Decentralized Identity (DeID):** The shift moves data control from centralized databases to the user's device (wallet) using Verifiable Credentials (VCs).
- **The Telco Root of Trust:** Mobile operators are uniquely positioned to provide authentication by anchoring digital identities in the SIM card and real-time network signals (e.g., SIM swap and number recycling checks).
- **Protocol Innovation:** The Verifiable Voice Protocol (VVP) provides a standards-based framework for two-way assurance between callers and callees, integrating seamlessly with existing SIP and STIR/SHAKEN infrastructure.
- **Business Impact:** Early pilots indicate that these technologies can reduce call center authentication from minutes to seconds, lower fraud-related losses, and significantly improve customer connection rates.

The Crisis of Trust in Voice Communication

The Scale of Industrialized Harm

Voice and messaging channels have become primary attack surfaces for "industrialized harm." The global impact of scams is estimated at over **$1 trillion in losses for 2024**, with a recovery rate of only approximately 4%.

- **Victimization:** Over half of the world's adult population reports being targeted by a scam in the last year.
- **Psychological Impact:** Beyond financial loss, victims suffer from severe emotional distress, including anxiety and depression.
- **Criminal Infrastructure:** Fraud operations are increasingly sophisticated, often linked to human trafficking and utilizing Generative AI to create synthetic identities and iterate on social engineering tactics.

Failure of Legacy Authentication

The industry identifies several structural weaknesses in current call center and telephony authentication:

- **Knowledge-Based Authentication (KBA):** Requires customers to disclose sensitive personal information to agents, creating a massive data liability and an "insider threat" risk where agents can be bribed to leak data.
- **CLI Spoofing:** Modern interconnected networks make it trivial for attackers to spoof Caller Line Identity, rendering it useless as a security signal.
- **Operational Friction:** Consumers typically spend 4–5 minutes merely proving their identity before addressing their actual issue, costing call centers an estimated **0.75–1.50 per minute**.

Technical Foundations: Decentralized Identity and VVP

The Decentralized Model

Unlike centralized systems where personal data is stored in third-party databases, the

decentralized model places identity data under the control of the user in a digital wallet. The ecosystem relies on three primary roles:

1. **Issuer:** The mobile operator issues a credential proving ownership of a phone number or legal identity.
2. **Holder:** The user stores the credential in a secure wallet on their device.
3. **Verifier:** The call center or brand validates the credential without needing to contact the issuer directly.

The Verifiable Voice Protocol (VVP)

VVP is an emerging standard (Internet-Draft, March 2026) designed to authenticate both individuals and organizations. It builds upon STIR/SHAKEN but introduces richer evidence through **Verifiable Dossiers**.

Key Roles in VVP

- **Accountable Party (AP):** The organization or individual with the legal right to a phone number. They are "the caller" from a regulatory perspective.
- **Originating Party (OP):** The entity controlling the technical infrastructure (e.g., a Session Border Controller) that initiates the call. This might be a call center acting on behalf of an AP.
- **Verified Party (VP):** The party using VVP to prove assertions about itself.

VVP Passport Structure (Citing Dossiers)

The protocol uses a VVP PASSporT passed in the Identity header of a SIP INVITE. It includes several critical fields:

Field	Description
`alg`	Cryptographic algorithm (MUST be EdDSA or post-quantum FN-DSA-512).
`kid`	Key identifier; an OOBI (Out-of-Band Introduction) of an AID (Autonomic Identifier).

`evd`	The OOBI of a "Dossier"—a verifiable data graph justifying identity and authorization.
`card`	Optional brand attributes (vCard format) justified by the dossier.
`goal`	A machine-readable code describing the intent of the call.
`iat`/`exp`	Issued-at and expiration timestamps to prevent replay attacks (recommended 15–30 seconds).

The Role of Telecommunications Operators

SIM-Based Root of Trust

Mobile operators (telcos) possess a unique advantage in the identity ecosystem due to the **SIM (Subscriber Identity Module)**. The SIM is the foundation for network authentication, occurring hundreds of times daily. Telcos can now expose real-time network signals through standardized APIs to bolster caller trust:

- **Number Verify API:** Confirms the user currently possesses the device and phone number.
- **SIM Swap API:** Detects recent SIM card changes, a primary signal for potential account takeover fraud.
- **Number Recycling API:** Tracks if a number has been disconnected or reassigned, ensuring old credentials are revoked.

The GSMA Open Gateway and Camara Project

The **Camara Project** is a collaborative effort to standardize these telco APIs. A key component is the **Verified Caller API**, which enables:

- **Multimedia Business Cards:** Enterprises can display operator-certified branding, including logos, text, and video clips, on the recipient's screen before the call is answered.

- **Enhanced Connection Rates:** Use cases in healthcare (e.g., hospital follow-ups) show that patients are significantly more likely to answer when they see a verified identity, improving service satisfaction and reducing the cost of repeated call attempts.

Implementation and Security Outcomes

Success Metrics from Pilots

Joint proof-of-concept (PoC) initiatives by **Telefónica Tech, GSMA, and TMT ID** (utilizing the Dock Labs/Truvera stack) have demonstrated the following:

- **Reduced Friction:** Cryptographic checks replace time-consuming security questions, allowing for near-instant authentication.
- **Data Minimization:** "Less data = less liability." By using selective disclosure and Zero-Knowledge Proofs, callers can prove their identity with a simple "yes/no" confirmation without revealing underlying PII (Personally Identifiable Information).
- **Interoperability:** The use of open standards (DIDComm, ACDCs, and KERI) ensures that the solution can scale across different mobile operators and jurisdictions.

Security Guarantees

The security of this new framework rests on several advanced cryptographic principles:

- **Autonomic Identifiers (AIDs):** These provide a non-repudiable, publicly accessible audit log of key state changes (KERI), enabling recovery from key compromises through pre-rotation.
- **Authentic Chained Data Containers (ACDC):** These make evidence revocable and stable even across key rotations.
- **Two-Way Assurance:** Unlike traditional systems that only verify the caller, VVP allows callees (e.g., a bank's call center) to present their own credentials in the SIP response, reassuring the caller that they have reached the intended party.

Verification Algorithm Highlights

Verifiers perform a rigorous check that includes:

1. Validating the signature against the OP’s current key state.
2. Fetching the **Verifiable Dossier** referenced in the passport.
3. Traversing the dossier's data graph to the root of trust for each credential.
4. Checking real-time revocation status.
5. Applying business logic (e.g., "Is this call center authorized to call on behalf of this brand during these hours?").