Telco IDaaS

Telcos' Untapped Opportunity for Digital Identity Services in a Passwordless, Wallet-Driven Era

---

Executive Summary

In 2026, digital identity forms the backbone of the global digital economy. Secure, seamless verification underpins banking, government services, e-commerce, and more. The global digital identity solutions market is projected to grow from about $44 billion in 2025 to $132 billion by 2031. For telcos this creates a major opportunity.

Telcos already control the world's most trusted identity anchors: mobile numbers, SIM/eSIM cards, and network-based authentication.

As regulators advance digital wallets, enterprises seek passwordless solutions, and fraud evolves with deepfakes, telcos can evolve from connectivity providers into trusted digital identity leaders—generating new revenue in Identity-as-a-Service (IDaaS), verifiable credentials, and privacy-focused services.

The Digital Identity Goldmine: Telcos' Untapped Opportunity in a Passwordless, Wallet-Driven Era

In 2026, digital identity is no longer a niche IT function—it is the foundational infrastructure of the global digital economy. From opening bank accounts to accessing government services or logging into e-commerce platforms, every interaction hinges on proving "you are you" securely, privately, and seamlessly.

The market reflects this urgency: the global digital identity solutions market is projected to grow from approximately $44–64 billion in 2025 to $130–170 billion by 2031.

For telecommunications operators (telcos), this explosion represents a once-in-a-generation market opportunity. Telcos already own the most ubiquitous, trusted, and hardware-secured identity anchors on the planet: mobile numbers, SIM/eSIM cards, and network-level authentication.

As regulators push digital wallets, enterprises demand passwordless experiences, and fraudsters weaponize deepfakes, telcos are uniquely positioned to evolve from connectivity providers into trusted digital identity leaders—unlocking new revenue streams in Identity-as-a-Service (IDaaS), verifiable credentials, and privacy-preserving data services.

The Evolution of Digital Identity: From Passwords to Verifiable Wallets

Digital identity has undergone three waves of transformation:

1. **Password Fatigue and the Passwordless Shift:** Traditional credentials are being replaced by passkeys (FIDO2), biometrics (facial, fingerprint, behavioral), and device-bound authenticators. Awareness of passkeys surged in 2025, with users citing superior security and convenience.
2. **Biometrics and Anti-Spoofing at Scale:** Multimodal biometrics combined with liveness detection and edge processing are becoming table stakes. On-device

verification minimizes data exposure while defending against AI-generated deepfakes.

3. **Decentralized and Self-Sovereign Identity (SSI):** Users control their own verifiable credentials in digital wallets. Standards like W3C Verifiable Credentials and DID (Decentralized Identifiers) enable selective disclosure—share only what's needed, when needed.

The regulatory tailwind is unmistakable. Europe's eIDAS 2.0 regulation mandates that every EU Member State offer at least one EU Digital Identity Wallet (EUDI) by the end of 2026. These wallets will support high-assurance identity for banking, travel, healthcare, and more, with mandatory acceptance by large private-sector players in regulated industries (finance, telecom, energy, etc.).

Similar frameworks are advancing in Asia, Latin America, and the U.S. (via NIST and state-level digital ID pilots). The result: a massive addressable market for secure, interoperable identity infrastructure.

Why Telcos Hold the Winning Hand

Unlike pure-play tech giants or fintech startups, telcos possess three structural advantages:

- **Hardware-Rooted Trust:** The SIM/eSIM acts as a secure element certified to the highest assurance levels. Network authentication (via 3GPP standards in 5G/6G) provides out-of-band verification that is extremely difficult to spoof.
- **Pre-Existing KYC at Scale:** Every subscriber has already undergone rigorous identity verification during onboarding—often with physical presence in retail stores. This "golden source" data can be leveraged (with consent) for reusable digital credentials.
- **Ubiquitous Reach and Network Intelligence:** With billions of mobile connections globally, telcos can deliver identity services across borders, devices, and networks. GSMA's Mobile Connect framework, adopted by dozens of operators, already demonstrates federated mobile-number-based authentication at scale.

Telcos are also actively shaping the ecosystem. Major European operators—Deutsche Telekom, Orange, Telefónica, and Vodafone—participated in the POTENTIAL consortium's large-scale EUDI pilots, testing SIM-based credential issuance,

e-registration, and cross-border use cases.

Concrete Market Opportunities for Telcos

The opportunity spans B2C, B2B, and B2G models:

- **IDaaS and Authentication Platforms:** Offer passwordless login, strong customer authentication (SCA), and continuous behavioral monitoring as a service to banks, retailers, and enterprises. Revenue via per-transaction or subscription models.
- **Verifiable Credentials and Digital Wallets:** Act as issuers or intermediaries in national/EU wallets. Telcos can embed credentials (e.g., mobile number attestation, age verification) into EUDI wallets using the SIM as the secure root of trust.
- **eKYC and Onboarding Acceleration:** Partner with fintechs and governments to deliver instant, reusable KYC—reducing drop-off rates in digital customer journeys by up to 50%.
- **Fraud Prevention and Trust Services:** Leverage network signals to detect SIM-swap attacks, synthetic identities, and account takeovers in real time. Monetize via premium security layers or shared threat intelligence.
- **Privacy-Enhancing Data Services:** With consent frameworks like EUDI's selective disclosure, telcos can enable anonymized identity resolution for advertising and analytics—competing directly with Big Tech while respecting GDPR. Early joint ventures among European telcos already target this space.
- **IoT and Enterprise Identity:** Extend digital ID to connected devices, vehicles, and industrial assets using 5G network APIs and edge computing.

Early movers in South Korea (SK Telecom, KT, LG Uplus via the unified PASS platform) and Belgium (Proximus integrating itsme) have already demonstrated improved customer retention and cross-brand experiences.

Challenges on the Path to Leadership

Success is not guaranteed. Telcos must navigate:

- Competition from Big Tech: Apple, Google, and Microsoft dominate consumer passkeys and device wallets. Telcos must differentiate through network-level assurance and regulatory alignment.

- Regulatory Complexity and Privacy: High-assurance certification is demanding; data minimization and user consent are non-negotiable.
- Legacy Systems and Silos: Internal identity fragmentation must be resolved before external monetization.
- Investment and Partnerships: Success requires ecosystem collaboration—standards bodies (GSMA, ETSI), wallet providers, and governments.

Operators that treat digital identity as a core platform capability—investing in zero-trust architecture, API exposure via GSMA Open Gateway, and sovereign AI for fraud detection—will lead.

The Road Ahead: From Connectivity to Digital Trust Provider

By 2030, identity services could represent a meaningful new revenue pillar for forward-thinking telcos—potentially adding billions in high-margin, recurring income while reinforcing customer loyalty and regulatory relevance.

The window is open now. With EUDI wallets launching at scale in 2026, national digital ID programs accelerating worldwide, and enterprises desperate for fraud-resistant, privacy-first solutions, telcos that move decisively can transition from “pipe” providers to indispensable trust anchors in the digital economy.

The technology, the regulatory momentum, and the customer relationships are already in their hands. The only question is whether they will seize the digital identity goldmine—or watch others do it.

Unlocking New Revenue Streams for Telcos with the Verifiable Voice Protocol

Telcos: Traditional caller ID is dying in the age of AI deepfakes & fraud. Enter the Verifiable Voice Protocol – unlocking premium verified caller services, enterprise contracts & new revenue streams.In a world where AI-generated deepfakes and evolving cyber threats render traditional caller ID obsolete, secure, real-time authentication has never been more critical.

In this webinar join Randy Warshaw, CEO of Provenant, as he delves into how cryptographically secured verifiable Legal Entity Identifiers (vLEIs) are revolutionizing telecom security.

Verifiable Voice Protocol (VVP)

The Verifiable Voice Protocol (VVP), as outlined in the draft specification, presents a transformative commercial opportunity for telecommunications companies (telcos) by addressing the pervasive issue of trust in telephone communications.

Unlike existing solutions such as SHAKEN, RCD, and BCID, which rely on service provider signatures and face challenges like high costs, jurisdictional limitations, and limited independent verifiability, VVP introduces a decentralized, cryptographic approach to authenticate and authorize callers.

By binding robust, verifiable evidence to SIP INVITEs, VVP enables telcos to offer enhanced services that restore consumer confidence, reduce fraud, and create new revenue streams through premium identity verification and authentication offerings.

VVP leverages Authentic Chained Data Containers (ACDCs) based on the Key Event Receipt Infrastructure (KERI) protocol, integrating seamlessly with verifiable Legal Entity Identifiers (vLEIs) and other credentials. This allows telcos to provide services that prove a caller's legal identity, delegated authority, brand attributes, and rights to a phone number, all with non-repudiable audit trails.

Verified Caller Service

For example, a telco could offer a premium “verified caller” service, where businesses pay for enhanced call authentication, ensuring their calls are prioritized and trusted by recipients. This is particularly valuable for industries like finance, healthcare, or e-commerce, where verified identity can reduce fraud and improve customer experience.

Additionally, VVP’s compatibility with existing standards like SHAKEN and RCD allows telcos to enhance current systems without overhauling infrastructure, lowering implementation costs and enabling hybrid ecosystems.

The protocol’s decentralized and privacy-preserving design further amplifies its commercial potential. By avoiding reliance on centralized vetting regimes and supporting cross-jurisdictional verification, VVP enables telcos to cater to global enterprises seeking consistent, interoperable solutions.

For instance, a telco could offer VVP-based services to multinational corporations, ensuring their calls are trusted worldwide, creating a new market for cross-border authentication. The protocol also supports two-way evidence sharing for calls, texts, and non-telco contexts, opening opportunities for telcos to expand into adjacent markets like secure messaging or digital identity verification.

Developed with contributions from Provenant and GLEIF, VVP positions telcos as trusted intermediaries in a digital economy increasingly focused on verifiable identity. By offering scalable, cost-effective, and interoperable authentication services, telcos can tap into new subscription models, enterprise contracts, and consumer trust solutions, driving revenue while combating fraud.