MOBILE IDENTITY

Meta

# White Paper
# The Promise of Phone Number Silent Authentication APIs

By Pushpendra Singh Erez Naveh Eliraz Levi Ilan Zak Jeff Louie Vladimir Wolstencroft

January 2026

## Executive Summary

As the digital landscape evolves, so too must our methods of securing online interactions. The traditional six-digit One-Time Password (OTP) via SMS reached global adoption because the mobile industry aligned on global standards, but it now faces growing challenges in terms of security, user experience, performance, and cost. This report, a collaborative effort by Meta and leading Telco partners, introduces the Silent Authentication API as the natural evolution of SMS OTP: a superior, more secure, and more seamless alternative designed for today's threat landscape and user expectations. We will delve into its mechanics, its benefits to the digital ecosystem, and the crucial steps required for its widespread adoption, anchored in GSMA Open Gateway, CAMARA's open APIs, and GSMA Service Entitlement Configuration (TS.43), as the best path to enable interoperability and scale beyond SMS OTP.

> *Industry-wide scale only happens through open global standards. SMS OTP reached global adoption because the Mobile industry aligned on global standards, Silent authentication is the natural evolution to SMS OTP addressing modern day security and performance issues highlighted in this white paper. We welcome Meta's direction to support GSMA's Open Gateway framework, CAMARA's open APIs and GSMA Service Entitlement Configuration (TS.43), creating a secure scale beyond SMS OTP.*
> ***— Henry Calvert, Head of Networks, Technology, GSMA***

## What is Silent Authentication and How it Works

Silent Authentication is a modern, frictionless method of user verification that leverages mobile network operator (MNO) data for identity confirmation, eliminating the need for users to wait for an OTP SMS to be received and actively input a code. In addition, it creates a trusted and more predictable chain, increasing security level unlike SMS OTP routing which is shared in plain text across the supply-chain.

### How it Works:

a. **User Login Attempt:** A user attempts to log in or perform a secure action on an Application on Consumption Device.

b. **Initiation:** API Consumer backend evaluates the request and provides instructions to the Application on Consumption Device to initiate an API Provider / Operator based authentication.

c. **Authentication:** Depending on the setup, the Application on Consumption Device will send a request directly to the API Provider / Operator, performing a handshake required to authenticate the SIM session. On successful authentication, the API Provider / Operator provides an authentication token.

d. **API Call:** The Application on Consumption Device propagates the auth token back to its API Consumer backend. Then the API Consumer backend uses this token to consume different APIs, like phone number verification by calling the API Provider / Operator servers.

e. **Verification Response:** The API Provider / Operator provides a secured confirmation signal, used to confirm or deny the user’s identity.

f. **Access Granted/Denied:** The API Consumer backend receives this confirmation and grants or denies access accordingly.

This entire process is virtually instantaneous and seamless to the user, providing a superior user experience compared to waiting for and entering an SMS OTP.

## Learnings and Benefits for the Ecosystem

Our initial deployments and engagements with Silent Authentication have yielded significant insights and demonstrate clear advantages for the entire digital ecosystem:

- **Improved User Experience:** The seamless, instantaneous nature of Silent Authentication eliminates friction for users, leading to a better user experience and delight. Additionally, the API provides real-time failure feedback, enabling the application backend to quickly offer other methods to verifying identity. Minimizing roundtrips and maintaining an efficient latency is important, as it translates into friction impacting the end user.
- **Enhanced Security:** Silent Authentication is inherently more secure than SMS OTPs, which are vulnerable to interception, phishing, and SIM swap attacks. More details in the *Security Enhancement* section below.
- **Reduced Operational Costs:** For businesses, Silent Authentication can significantly lower the costs associated with sending SMS OTPs, as unlike SMS, which incurs charges for every message sent regardless of outcome, Silent Authentication leverages API-driven feedback loop that enables a pay-per-success billing model.
- **Immunity to premium number abuse:** SMS OTP can be exploited by attackers who trigger OTP messages to premium-rate phone numbers, resulting in unexpected charges for users or companies. Silent Authentication does not interact with phone numbers or SMS infrastructure, eliminating the risk of fraud via premium number abuse.
- **Stronger Telco-Enterprise Partnerships:** This technology fosters a deeper, more collaborative relationship between telcos and enterprises, creating new revenue streams for MNOs and enhanced security for businesses.
- **Protecting Ecosystem Integrity:** Adopting a pay-per-success model can protect ecosystem integrity and trust, as it eliminates the economic incentives behind Artificially Inflated Traffic (AIT). With APIs, untrustworthy ecosystem participants cannot profit from incomplete verifications.
  This approach gives businesses predictable costs tied to real user identity verification and shifts carrier traffic from insecure bypass to official Network APIs.
- **Ecosystem Efficiency:** Standardizing the Silent Authentication API is key to unlocking efficiency for both demand-side (businesses/enterprises) and supply-side (MNOs/platforms). A unified standard reduces integration complexity and time-to-market for businesses, while enabling MNOs to offer a single, scalable service that is universally accepted, thereby accelerating widespread adoption and scaling the overall market.

## Security Enhancement

While SMS has been the ubiquitous delivery of OTP codes due to its reach and its standardization across the world, it has consistently suffered from security issues resulting in various attack scenarios seriously degrading the quality, deliverability and integrity of SMS messages. Some of these issues are solved via Silent Authentication adoption as follows:

- **Clear text transmission and poorly designed protocols:**
  SMS continues to use protocols such as SMPP which not only have inherent flaws, they generally run on clear text, non encrypted signals and protocols. SMPP itself is also poorly protected with fixed length authentication parameters and poor resiliency in protocol design
- **Multiple hop routes and Bypass Fraud:**
  SMSC ((Short Message Service Center) and intermediate equipment can often be unprotected, badly designed and aggregators who run clear text SMS incoming and outgoing systems have a mostly unknown security posture. Common aggregators running outdated equipment and storing OTP codes along the way frequently leak sensitive data. This includes SMS bypass fraud where GSM gateways or SIMBoxes are utilized, which has resulted in leaked OTP codes across many users and systems.
- **SMS OTPs are vulnerable to phishing attacks:**
  Attackers can trick users into entering OTPs on fake websites or apps, enabling account takeover. Silent Authentication eliminates this risk by automating authentication within trusted apps, removing user interaction with codes.
- **Silent Authentication is immune to SS7-based number hijacking attacks, while SMS OTP is not:**
  SS7 vulnerabilities allow attackers to intercept or redirect SMS messages (such as OTPs) by manipulating telecom signaling protocols (e.g., through location update attacks). This means SMS OTPs can be stolen remotely, even without physical access to the device. Silent Authentication does not rely on SMS or telecom signaling; it authenticates users based on device-bound credentials and secure app signals, making it unaffected by SS7 exploits.
- **Silent Authentication does not solely rely on SMS and phone number ownership for authentication:**
  Instead, it uses device-based signals (such as device tokens, app integrity checks, or secure hardware) that are bound to the physical device, making it much harder for attackers to impersonate the user by simply taking over a phone number.

Silent Authentication vs. SMS OTP

| Feature | Silent Authentication API | SMS OTP |
|---|---|---|
| **User Experience** | Seamless, instantaneous verification | Requires user to wait for SMS, retrieve code either automatically or manually |
| **Security** | High; leverages MNO data, resistant to common phishing/SIM swap attacks | Moderate; vulnerable to interception, phishing, and SIM swap attacks |
| **Reliability** | High; direct network verification, not dependent on SMS delivery ecosystem | Variable; dependent on SMS delivery, can be affected by network congestion/issues |
| **Cost to Business** | Predictable, stable pricing that’s less vulnerable to fraud spikes. | Can be high due to SMS inefficiency and ecosystem |
| **Fraud Prevention** | Strong; reduces attack vectors | Weak; susceptible to social engineering and AIT |
| **Network** | Requires active cellular data limiting coverage for Wi-Fi only connections. Moving to network agnostic solutions like TS43 would enable greater coverage. | Operates via the signaling layer. Works on Wi-Fi if the device is registered with the carrier's signaling network |
| **Failure feedback** | Provides real-time failure feedback, allowing for immediate fallback to secondary methods (e.g. SMS/Voice). | Lacks a reliable real-time feedback loop; fallbacks are typically triggered manually by the user or after a preset timeout. |
| **Global Coverage** | Growing, requires MNO integration | Ubiquitous, but performance varies by region |

## Meta's Insights on Achieving Higher Coverage and Success Rates

- **Limited coverage of users with active cellular data:** The current available API's reliance on active cellular data restricts coverage by about 50%, depending on the country. Efforts to automatically switch users to cellular data or prompt them to enable it manually haven't led to meaningful improvements. Adopting network agnostic solutions are expected to overcome this limitation, enabling silent authentication for off-net and WiFi-connected devices.
- **Precision Carrier Discovery:** Enhance carrier matching accuracy by utilizing Android's MCC/MNC APIs and supplementary network signals to ensure requests are routed to the correct operator.
- **Network Path Optimization:** Prioritize users on cellular data, as those accessing the app via Wi-Fi are less likely to succeed.
- **UX Transparency:** Provide real-time progress indicators to maintain user engagement during the API handshake; implement carrier-specific timeouts to trigger deterministic fallback paths proactively.
- **Latency Management:** Reduce client API handshake roundtrips to minimum for enhanced and more reliable UX.

## Meta's Next Steps and Future Explorations

Core initiatives designed to maximize the potential and impact of the Silent Authentication API:

- **Flexible Integration and Scalability:** We are evaluating multiple integration models, including different aggregators,evolving the CAMARA API standard, and custom MNO APIs, to ensure maximum flexibility and scale with our carrier partners.
- **TS43 Standard Expansion and Validation:** As the TS43 standard becomes available across more carriers, we are actively expanding our integrations and testing efforts to thoroughly validate performance, and the anticipated coverage improvement, especially for off-net and WiFi-connected devices.
- **Broadening Use Cases to Multi-Device Experiences:** While our initial efforts centered on single-device users, we are now expanding our focus to include cross-device and secondary device use cases.
- **Optimizing Experience, Conversion, and Fraud Mitigation:** A core objective is to explore further ways to leverage the API to enhance user experience, boost conversion rates, and strengthen anti-fraud/scam capabilities.

### What Needs to Be True for Solid Replacement

For Silent Authentication to become a solid replacement for SMS OTPs, several critical factors need to be addressed and realized:

- **Pricing Model:** A clear, predictable, and scalable pricing model is essential, optimized for outcome. The model should account for volume, regional variations, and the enhanced security value.
- **Scale and Coverage:** Widespread adoption hinges on achieving broad geographical coverage and the ability to handle massive transaction volumes. This necessitates accelerated integration efforts across more MNOs globally.
- **Standardization:** Industry-wide standards for the Silent Authentication API are crucial to ensure interoperability, ease of integration for developers, and a consistent user experience across different services. This is where GSMA's role is paramount.
- **Regulatory Alignment:** Collaboration with regulatory bodies to recognize and endorse Silent Authentication as a secure and compliant authentication method will be vital for its widespread acceptance, especially in sensitive sectors like finance and healthcare.
- **Developer Ecosystem:** Robust SDKs, comprehensive documentation, and developer support are necessary to lower the barrier to entry for businesses looking to integrate Silent Authentication into their platforms.
- **Public Awareness and Trust:** Educating both businesses and end-users about the benefits, security, and seamless nature of Silent Authentication will build trust and accelerate adoption.

> *Silent Authentication represents the natural evolution beyond SMS OTP—delivering a seamless, secure experience that users expect in today's digital world. By collaborating with telcos and GSMA on open standards like CAMARA, we're not just solving today's authentication challenges; we're laying the foundation for future innovation in identity verification. Pay-per-outcome models will drive this transformation, aligning incentives across the ecosystem and ensuring trust and efficiency at scale. This is how we build a more trustworthy, frictionless digital future.*
> ***— Marc Sommer, VP Telco Ecosystem Partnerships, Meta***

## Next Steps for the Industry: Timeline and Beyond

The following steps are critical for the industry to collectively undertake to solidify Silent Authentication's position as the leading Telco-based phone number authentication method:

**Phase 1: Foundation and Expansion (H1’2026)**

- **Establish a Taskforce within GSMA:** Meta, Telco partners, interested industry participants and GSMA should formalize a taskforce focused on accelerating Silent Authentication adoption, sharing best practices, and addressing challenges.
- **API Standardization (GSMA Leadership):** GSMA to support development and lead promotion of GSMA’s Open Gateway framework, CAMARA’s open APIs (including Number Verification) and GSMA Service Entitlement Configuration (TS.43).
- **Pilot Programs Expansion:** Expand current pilot programs with more enterprises and MNOs in diverse geographical regions to gather further data, refine the API, and demonstrate real-world benefits.
- **Economic Models for Telcos:** Develop and test new pricing models that drive the right transformation towards API, ensuring a sustainable ecosystem.
- **Public Awareness Campaign** (Meta & Telcos): Launch targeted awareness campaigns highlighting the benefits of Silent Authentication to businesses and the enhanced security and convenience for end-users.

**Phase 2: Broad Adoption and Innovation (by end of H1’2027)**

- **Accelerated MNO Integration:** Drive initiatives to bring a significant majority of global MNOs to deploy the CAMARA APIs that support Silent Authentication, aiming for comprehensive coverage in key markets.
- **Developer Hub and Resources:** Create a dedicated developer portal with comprehensive documentation, SDKs for various platforms, and community support to empower businesses to easily integrate the API.
- **Interoperability Certification:** Establish a certification program for Silent Authentication implementations to ensure compliance with standards and interoperability across providers.
- **Integration with Identity Providers:** Explore and implement integrations with major identity providers (IdPs) to offer Silent Authentication as a primary or secondary authentication factor.
- **Regulatory Advocacy:** Actively engage with government bodies and regulators to advocate for the recognition and eventual mandate of Silent Authentication in specific sectors where security is paramount.
- **Improved Coverage:** Work on identifying additional use cases like cross device authentication and provide solutions.

**Phase 3: Ubiquity and Evolution (H2’2027 and Beyond)**

- **Global Standard:** Establish CAMARA’s open APIs and GSMA Service Entitlement Configuration (TS.43) as the de-facto global standard for telco-based phone number verification, largely replacing SMS OTPs.
- **Advanced Use Cases:** Explore and develop advanced use cases beyond basic login, such as transaction verification, age verification, and seamless onboarding processes.
- **Continuous Security Enhancements:** Invest in ongoing research and development to further enhance the security and resilience of Silent Authentication against emerging threats.
- **Integration with Emerging Technologies:** Adapt Silent Authentication to integrate with future technologies such as Web3, decentralized identity, and post quantum-resistant cryptography.

## Conclusion

The transition from SMS OTP to Silent Authentication API is not merely an upgrade; it is a fundamental shift towards a more secure, efficient, and user-friendly digital authentication paradigm. By fostering strong collaboration between Meta, Telco, Industry partners and GSMA, and by committing to the strategic steps outlined above, we can collectively usher in a new era of digital trust and convenience for businesses and consumers worldwide. The future of phone number authentication is silent, secure, and seamless.