API-driven Silent Authentication: why telcos can’t afford to move slowly

Silent Authentication is emerging as a leading near-term opportunity for Network APIs, with early deployments showing faster authentication, higher conversion and growing transaction volumes. But concerns over SMS cannibalisation and pricing could limit adoption. This article explores the business case, emerging proof points and what telcos need to do to capture the opportunity.

Miriam Sabapathy, Senior Consultant, NaaS and Network APIs Practice Lead

August 2026

What is API-driven Silent Authentication, and why now?

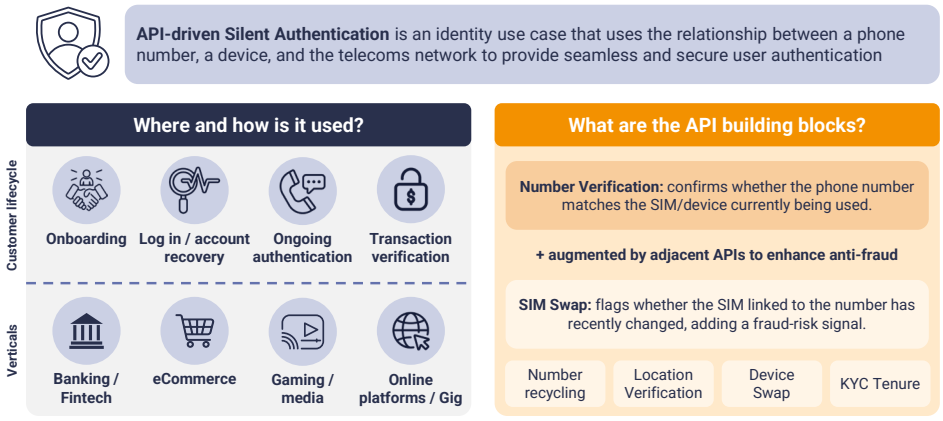
Authentication is becoming a growing pain point for digital businesses. Customers increasingly expect fast, seamless digital journeys, while organisations face pressure to strengthen fraud controls and reduce reliance on passwords and one-time passcodes (OTP). SMS OTP in particular introduces friction into onboarding and login, can be vulnerable to interception and social engineering, and comes with a recurring cost each time a user needs to authenticate. This is creating demand for ways to verify users that are both more secure and less intrusive.

Silent Authentication offers one potential answer. STL defines Silent Authentication as a use case that verifies a user without requiring manual password entry or one-time passcodes. Network APIs are one way of enabling this, by drawing on the relationship between a phone number, the SIM and the network to confirm who the user is, invisibly and in the background.

Part of what makes the Silent Authentication opportunity so attractive is the breadth of potential demand. Adoption today is concentrated in new customer onboarding and login, but the same capability can extend into ongoing re-authentication and transaction verification. The opportunity also spans a wide range of verticals, from banking and fintech today to growing traction across e-commerce, gaming, media, content and gig-economy platforms.

On the telco side, the primary network API enabling Silent Authentication under the CAMARA standards is Number Verification, which confirms whether the phone number matches the SIM or device currently in use. Terminology across the market is not always consistent: some providers refer to Number Verification-based propositions themselves as “Silent Authentication” APIs or services, although technically Number Verification is the network capability being used to enable the Silent Authentication experience. At its simplest, this makes it a like-for-like replacement for SMS OTP. But operators are also combining Number Verification with anti-fraud APIs that strengthen the trust signal. SIM Swap – confirming there has been no recent change to the SIM linked to a number – is the most advanced of these today, while other identity and fraud signals can add further layers of confidence.

Figure 1: What is API-driven Silent Authentication?



The proof points are stacking up

Momentum is now visible on both sides of the market. On the supply side, operators are prioritising the APIs most directly linked to Silent Authentication: based on our latest analysis of the GSMA Open Gateway launch

tracker, Number Verification and SIM Swap already account for more than half of deployments so far in 2026, and we expect that share to keep growing into 2027 as operators and aggregators progress planned deployments. There is a reason these APIs are moving first: they address an established authentication and fraud market, are comparatively straightforward to deploy and monetise, and lend themselves well to standardisation and aggregation across operators. The arrival of Number Verification 2.x should accelerate this further.

On the demand side, adoption is concentrated in the same place – and the scale being reported by early movers is becoming harder to ignore. At the Aduna Summit in April, Meta reported more than 500 million Number Verification API calls, a figure it described as already out of date. At MWC Barcelona 2026, Twilio stated on a panel that it is processing 30.8 million Network API transactions per day. While coverage is still far from universal, these figures point to the scale that can emerge once APIs are available across sufficient markets and operators.

More importantly, early deployments are beginning to demonstrate tangible customer outcomes:

- Vonage: a fintech customer saw a 75% reduction in authentication time
- Honey Badger: a 30% uplift in customer onboarding
- mBank (Poland): a 97.6% acceptance rate through silent authentication

For more on these early customer proof points, and what they tell us about the wider Network API market, read our takeaways from the Aduna Summit 2026 here.

The business case is clear, if operators get the pricing right

Early evidence confirms that there are real customers with clear and increasingly urgent demand for Silent Authentication – and that many want to scale it faster because the business case is compelling. When customers assess whether to adopt, and more importantly whether to scale, a new capability like this, the decision typically comes down to four questions: does it improve trust, improve the user experience, grow revenue and reduce cost? API-driven Silent Authentication performs strongly against the first three, while the fourth – cost – remains more dependent on how operators choose to price it.

1. **Trust**: *does this improve our security processes and our ability to evidence compliance?*

   Compared with OTP, Number Verification is harder to spoof and harder to intercept. That matters increasingly for regulated sectors such as banking, which face growing scrutiny to demonstrate that they took reasonable steps to verify a user's identity.

2. **User experience:** *does this improve how customers interact with the platform?*

   OTP can take upwards of ten seconds to complete, and in some markets the SMS does not arrive on the first attempt, especially where vendors route messages through other countries to manage cost. That friction is real. We have heard that the CAMARA approach still has some latency challenges to resolve, but early deployments already show it running around ten times faster than OTP – and critically, the user never has to leave the platform interface.

3. **Revenue:** *does this improve conversion and grow revenue?*

   This follows closely from user experience: a smoother journey drives materially higher completion and conversion. Where Silent Authentication is deployed at onboarding, that improvement in conversion translates fairly directly into new customer revenue. The opportunity is therefore less about reaching wholly new markets and more about converting more effectively within existing ones – which can still have a material financial impact at scale.

4. **Cost**: *does this reduce the cost base?*

   This is the least clear dimension of the business case as it depends heavily on how operators approach API pricing. Some view Number Verification as a better product than OTP and therefore expect it to command a premium. Others see the priority at this stage as building the market, where achieving volume and scale matters more than defending a premium against SMS.

   STL's view generally leans towards the latter. Pricing APIs at too great a premium risks limiting their use to a relatively small number of high-value or high-risk transactions, while customers rely on alternatives such as passkeys, authenticator apps or lighter-weight checks elsewhere. The telco then becomes a secondary, step-up authentication provider rather than part of the default authentication journey – weakening the opportunity to keep the phone number at the centre of digital identity.

   However, this varies market by market. In markets such as the US, where SMS is already inexpensive, we have heard that Number Verification can still reduce the overall cost of a successful authentication even at a modest unit-price premium. If several OTPs need to be sent before one is successfully delivered, the relevant comparison is not necessarily the price of one API call against one SMS, but the total cost required to achieve the same successful authentication outcome.

The bigger risk is protecting SMS for too long

For many operators, one of the biggest barriers to moving faster on Silent Authentication is internal rather than technical. For onboarding and login, Number Verification can be a close substitute for SMS OTP, creating an understandable concern around cannibalisation: are operators genuinely creating new revenue, or simply moving existing SMS revenue from one pocket to another?

That concern is contributing to slower progress on Number Verification – and, in many cases, the wider network API opportunity – than the underlying demand would justify. But STL believes operators need to look beyond the immediate SMS revenue trade-off. The more important question is whether telcos can remain relevant in digital identity and capture a share of a growing authentication and fraud market. Four counterpoints are worth making.

1. **SMS is already declining.** In many markets, SMS and SMS OTP volumes have already reached maturity, while pricing pressure is beginning to push customers towards alternatives. There are exceptions where volumes are still growing, but over a five-year horizon STL expects meaningful price and volume erosion across most markets. Protecting today's SMS revenues therefore risks optimising around a market that is likely to shrink.
2. **Customers are actively looking for ways around OTP.** Improving digital customer experience is a priority across sectors, and OTP is a well-known source of friction. Major digital platforms, including Google, have publicly signalled ambitions to move away from OTP. Regulation is reinforcing the shift too – the Philippines and the UAE have both mandated a phase-out of SMS OTP, and STL expects more markets to follow. If operators do not establish the mobile number as part of the next generation of authentication, other technologies and providers will fill that role instead.
3. **The addressable opportunity extends beyond SMS.** Much of the industry discussion – including this article – compares Number Verification with SMS OTP because it is the most immediate substitution opportunity. But the authentication market is much larger. Email OTP, authenticator apps, passkeys and other authentication methods represent transactions from which operators currently capture little or no value. If the price, latency and proposition are right, network-based authentication has the potential to compete for a share of this broader market, rather than simply replacing existing SMS revenue.

4. **This is the entry point into the wider anti-fraud proposition.** Silent Authentication does not need to stop at Number Verification. Operators can layer in capabilities such as SIM Swap, KYC Tenure, Number Recycling and other fraud signals to provide additional confidence for higher-risk transactions. For identity specialists and authentication providers, being able to access both the basic authentication check and additional anti-fraud signals through the same relationship can create meaningful value and make the telco proposition more deeply embedded in the authentication workflow.

Operators should think of Silent Authentication (or at its core Number Verification) as a land-and-expand motion rather than an end point – which is also why the pricing question matters: building volume and pervasiveness first makes it far easier to expand into the next layer of capability than trying to do so from a low transaction base.

What operators should do now

STL sees four practical starting points for operators.

1. Learn from those who have already moved

A number of leading telcos deployed Number Verification and SIM Swap years ago and have been iterating ever since – visible in the evolution from NV1 to NV2. Newer entrants do not need to repeat that learning curve: they can build on what early movers have already learned about the capabilities, commercials and go-to-market models that work. There is also growing recognition that reaching meaningful revenue will require a collective-action mindset across the industry, rather than operators acting in isolation.

2. Use a maturing vendor ecosystem to derisk the move

The supply side is maturing quickly. Operators with existing infrastructure – API gateways, entitlement servers – face very little build-out cost; others may need more capability and upfront investment. A growing number of exposure and enablement players now offer out-of-the-box propositions and revenue-share models designed to get operators to monetisable volumes in days rather than years. The same is true on the aggregation side, where players are further ahead in building demand ecosystems and distribution networks, and are increasingly well placed to bring telco partners volumes from day one.

3. Build channels into specialist identity players, not just generic marketplaces

Horizontal marketplace players can offer reach by reselling APIs, but the more valuable partners are those already embedded in authentication workflows and packaging solutions today. Authentication is a complex, mature space, and specialists such as Socure, LexisNexis, XConnect and Telesign already have the expertise and the customer relationships to address it at scale. Operators should treat these players as key channels to sell into, whether directly or through aggregator partners, rather than relying only on horizontal players that work across many ecosystems at once.

4. Don't default to cost-plus pricing

This point is worth repeating, because it comes up constantly: don't price this as if Number Verification is a margin-driven, stand-alone product. STL has heard directly from early customers that, while they are impressed with the value of these APIs, pricing is often still too high to scale across high transaction volumes. This is the start of the API journey, not the end of it. The mobile number is the platform on which operators can build a much wider identity business – but only if the entry point is priced to reach the volume that makes the rest of that journey possible.

Silent Authentication is no longer just a theoretical opportunity: customer demand, transaction volumes and early commercial outcomes are beginning to prove the case. The bigger risk is that operators move too slowly to capture it, while vendors, aggregators and digital platforms build the identity layer around them instead. The technology, proof points and ecosystem are increasingly in place. What remains is a decision on pricing, partnerships and pace – and that decision now sits with operators.

This article draws on STL Partners' presentation in the *API-driven Silent Authentication: Can telcos risk being too slow?* webinar, hosted with LotusFlare in June 2026. Watch the recording and download the presentation slides here.

Miriam Sabapathy is a Senior Consultant at STL Partners, specialising in network API commercial strategies.

Get in touch with the author to learn more

miriam.sabapathy@stlpartners.com

Or visit STL Partners' NaaS and Network APIs Hub

stlpartners.com/naas-network-apis