ADUNA SUMMIT 2026 TAKEAWAYS: CUSTOMERS WANT MORE – AND FASTER

Early adopters are seeing tangible value and benefits from network APIs - but to scale adoption, customers want broader coverage, faster timelines and commercial models that work for real customer journeys. This article explores what the Aduna Summit revealed about the next phase of market adoption, from emerging proof points to the practical barriers still holding back scale.

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

APRIL 2026

Two weeks ago, we attended the Aduna Summit in Madrid, hosted by Telefónica at its headquarters. The event brought together a broad mix of telecom operators, technology partners, CPaaS players, identity and fraud specialists, hyperscale cloud providers, developers and enterprise customers — all focused on one question: **how quickly can Network APIs move from industry ambition to scaled commercial execution?**

The tone felt different from many previous events on Network APIs. Most of the conversations were not about what Network APIs could theoretically enable, they were about showcasing what early customers are already trying to do with them, where early proof points are emerging, and what is preventing adoption from moving faster.

More proof points are emerging – particularly around identity and trust-based use cases

Most of the agenda focused on customer progress and success stories, primarily within identity, authentication and anti-fraud use cases. It was great to see concrete, tangible proof points being shared — especially in an area where these have felt more elusive at previous industry events.

- Meta referenced more than 500M network API calls processed successfully – a figure that was described as already out of date, so the true figure is assumed to be higher – and highlighted Silent Authentication conversion rates of 80-90%, improving performance compared with previous SMS OTP methods.
- FICO and JT also shared findings from their work on Scam Signal, which uses real-time network intelligence to help detect whether a customer is on a call during a high-risk transaction. The results were impressive: 41% reduction in scams in progress, a 44% reduction in fraud losses, a 55% reduction in false positives and a 30% reduction in mobile phone handset scams. The results meant that a UK bank reportedly ended its PoC early after only 4 weeks, despite the trial originally being planned for 12, because the value was proven earlier than expected and the bank wanted to move more quickly towards deployment.

It was also encouraging to see the conversation broaden beyond fraud prevention, into a broader notion around trust. A recurring theme was about how the same identity APIs are not only about stopping bad actors; they are also about improving legitimate customer journeys. That matters commercially: reducing friction in onboarding, authentication and sign-up flows can directly support higher conversion, lower drop-off and ultimately greater revenue for customers.

- mBank, a Polish bank, highlighted the evolution of its mobile app sign-up process. Previously, the journey involved multiple handoffs across different applications and eight separate screens or stages. Adding SMS verification from the bank improved security, but created friction and led to a 27% drop-off rate on first attempt. With SIM Swap and Number Verification, security became a more invisible layer, reducing the journey to three screens and achieving a 97.6% consent-page acceptance rate.
- Vonage highlighted that one FinTech customer saw an 8.5% increase in conversion of authentication traffic versus SMS, alongside a 75% reduction in authentication time.
- Sign-up rates were also promising: Vonage cited a banking customer that saw a 26% increase in sign-up rates, while Honey Badger cited a 30% uplift in customer onboarding from a combination of Network APIs.

FICO also made an important point about the “blind spot” banks face: they may understand transactions and some merchant context, but they often know much less about the customer context surrounding those transactions. Network APIs can help provide a more holistic view.

Customers want three things from the industry: coverage, speed and commercial viability

The proof points demonstrated that demand is real. But across the presentations and panels, customers were also clear about what still needs to change before network APIs can scale. The early adopters – particularly the identity specialists, fraud platforms and authentication providers – emphasised three practical asks from the industry.

1. Broader coverage

Coverage came up repeatedly. Partial coverage makes it hard for partners and enterprise customers to build reliable propositions. One comment captured the problem well: it is difficult to go to end customers with only 50% coverage — the conversation quickly goes quiet. Several participants suggested that 70–80% coverage is closer to the minimum needed to make propositions commercially compelling.

That said, the coverage challenge should not be overstated. In background conversations at the Summit, several participants noted that APIs can still improve fraud scores or authentication journeys even if only two out of three operators in a market are live, depending on the specific market footprint and use case. Partial coverage may therefore not prevent early adoption. But it can become a barrier to scaling these propositions further – particularly for early adopters that need sufficient market coverage to productise the capability and take it to more customers.

This matters because most enterprise customers do not want to design fragmented journeys around which operator happens to support which capability in which market. They want consistent, predictable reach. For global customers in particular, coverage is not a nice-to-have; it is a prerequisite for scale.

2. Faster speed to market

The second message was speed. Customers are not operating on telecoms planning cycles. As AWS noted, planning cycles that once lasted a year can now become irrelevant in three months.

That creates a real tension with how operators are working today. One example shared involved a customer conversation about SIM Swap and Number Verification. In a 15-minute discussion, the customer wanted to launch that afternoon (the typical speed of a digital-first enterprise). The conversation hit a standstill when typical telco timelines were discussed: approvals took 26 days on average in North America, and in some European markets around three months.

Some of this complexity is understandable. Contracting, privacy management, data protection and risk controls are not trivial, especially when dealing with sensitive identity and authentication use cases. But from the customer's perspective, long lead times create a simple outcome: if they cannot get what they need quickly enough from mobile operators, they will look elsewhere.

3. Pricing and commercial models that work for customers

The third challenge is commercial viability. Pricing came up in several discussions, not just as a cost issue, but as a barrier to designing workable propositions.

Meta, Google Firebase, LexisNexis, amongst others argued for pricing models that align with outcomes. Per-verified or per-successful-outcome pricing was raised as a preferred model. This reflects a broader point: enterprises do not want to pay for technical API calls in isolation; they want to pay for business value. Paying for API calls where no useful data is returned prevents broader use.

Another challenge is the price point itself. Key customers already consume a wide range of data sources, including credit bureau data, device intelligence, digital identity data, behavioural signals, transaction data and other risk intelligence sources. Network APIs cannot be positioned as solving the entire authentication or anti-fraud workflow on their own. Instead, different data sources and checks will be used at different stages of the journey.

For example, a low-cost signal may be used early in a digital sign-up journey to remove friction or check for obvious risk. More robust checks may be used later if there is already a mismatch with address data, device data or other risk indicators. The challenge is that, if Network APIs are priced too high, they will only be used for the highest-risk or highest-value moments in the workflow.

LexisNexis' presentation highlighted this point clearly. One of its customers, a Tier 1 UK bank, processes 450 million transactions monthly, but phone intelligence currently accounts for only 0.089% of its overall transactions. The question for operators is whether they want Network APIs to be used only in select, very high-risk transactions at a premium price, or whether they want to target a much larger base of transactions at a price point that enables broader adoption.

Commercial design also interacts with technical performance. FICO noted that Scam Signal currently takes around one second, which means it is reserved for the highest-value transactions or highest-risk cases. If latency were reduced to 10–50 milliseconds, the capability could be used in different parts of the architecture and across more customer journeys.

This is a reminder that adoption is not determined by whether an API technically exists. It depends on whether the API is fast enough, affordable enough, reliable enough and simple enough to fit into real enterprise workflows.

Reflections and recommendations: what telcos need to do now

The Summit left a clear set of implications for operators. The opportunity is becoming more tangible. The risk is that the demand side is now moving faster than the supply side; and might move without them. We have five recommendations for operators and the wider industry.

1. Accelerate coverage and move from commitment to execution

The first priority is coverage. Customers and platform partners cannot scale propositions if APIs are available only operator by operator, market by market or with inconsistent timelines. Hesitant operators need to move from public commitment to active execution, particularly where there is already clear demand and visible proof points.

This is especially important for the first wave of identity, authentication and trust-based APIs. Much of the Summit discussion also pointed to Number Verification 2.0 as a potential "game changer" for the industry and a capability that all operators should be building now. For operators still deciding where to start, this matters. The first move does not need to prove the whole Network API opportunity. It needs to be focused, commercially relevant and aligned with where demand is already forming. Number Verification, SIM Swap and adjacent trust-related APIs are obvious starting points because they map to clear customer problems, visible use cases and a credible route to market.

This is a key theme in our recent report, *Building a network API business: What does it take?*, developed in partnership with Aduna and launched at the Summit. The report explores how operators can move from strategic interest to execution: securing executive backing, building an investable business case, choosing the

right first move and designing an operating model that can support scale. For operators still asking how to turn commitment into action, click here to find out more.

2. Adopt a collaboration mindset and leverage benefits from the ecosystem

Operators also need to recognise that, in many Network API use cases, they are not competing in the traditional sense. Customers need coverage and consistency across operators. Fragmented roadmaps, different approaches and inconsistent availability will slow the whole market.

Socure highlighted that operators should follow the best practice approach demonstrated by the UK models. Operators meet quarterly to align on roadmaps because they recognise they are not competing for subscribers in that context; they are building a market together. More markets should take the same approach.

3. Sell customer outcomes, not APIs

No one is buying APIs for their own sake. Customers buy reduced fraud, higher conversion, lower friction, faster onboarding and better customer journeys.

This should change how operators and aggregators talk about Network APIs. Whilst API-led language works well when only the supply side are in the room, beyond that the conversation should start with the customer problem, not the technical capability. Silent Authentication, for example, may need more education because some customers can misunderstand the value of an authentication process they cannot see. The proposition needs to explain not only what the API does, but how it improves a journey and why that matters.

The same applies to emerging use cases beyond identity. The Fireside chat with Optimizely around geofencing was a useful reminder that the value of a Network API may not always be immediately obvious from the API name. In a retail marketing context, one of the benefits is that customers do not necessarily need to download an app. For businesses where app penetration is low, that can be highly valuable.

4. Use Network APIs internally and create your own use cases

Telcos should be some of the first users of their own Network APIs. They face many of the same challenges as their enterprise customers: fraud, onboarding, identity verification, customer experience and digital trust.

Using Network APIs internally would help operators build stronger proof points, identify operational issues earlier and demonstrate confidence in their own capabilities. It would also move the conversation from theory to practice. If operators can show how these capabilities reduce their own fraud or improve their own customer journeys, they will have a much stronger story to tell externally.

5. Think beyond individual APIs to platform strategy

The discussion at the Summit was rightly focused on near-term demand, especially around identity and fraud. But telcos should also avoid thinking too narrowly.

Network APIs are not only a new product line. They should become part of a broader platform strategy, exposing network capabilities in a way that strengthens existing products, enables new propositions and creates more agile and faster ways of working. Operators should not only ask, “Which API can we sell?” They should also ask, “How can APIs make our existing business stronger?”

For example, if telcos integrate network APIs into existing B2B services (e.g. identity APIs integrated into a wider cybersecurity offering for SMEs), they can move beyond just selling the “ingredients” and move towards the higher value position of “selling the cake”. This is a theme we covered in our STL presentation at the Summit, which you can download 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' Edge Hub
https://stlpartners.com/naas-network-apis/