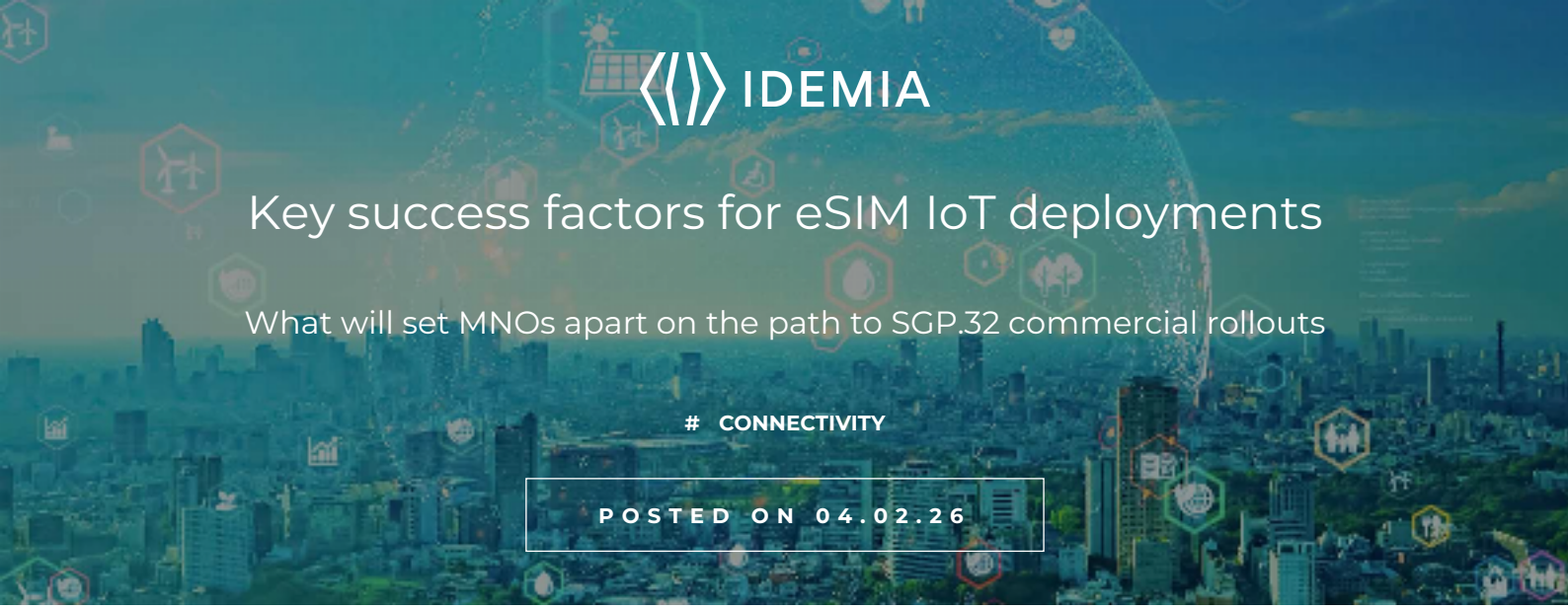

# Key success factors for eSIM IoT deployments

What will set MNOs apart on the path to SGP.32 commercial rollouts

# CONNECTIVITY

POSTED ON 04.02.26

A recent eSIM IoT market study[1] conducted by Kaleido Intelligence for IDEMIA Secure Transactions (IST) confirms that MNOs have unanimously decided to adopt the GSMA SGP.32 specification to advance their IoT roadmaps: 100% are already on the path to deploy it. While some are already running proof-of-concepts or preparing for commercial launch, most are still in early development phases, targeting launch in 2027 (or later).

**This report highlights:**

- The main drivers for eSIM IoT adoption among MNOs and IoT device makers
- Key challenges anticipated by MNOs as they prepare SGP. 32 rollouts
- Go-to-market strategies and emerging monetization opportunities

Get your copy

If you're still refining your strategy and evaluating the different eSIM IoT solutions on the market, here are our recommendations so you don't miss this pivotal moment.

## 1/ Streamline your SGP.32 integration model, focus on your core business

While the SGP.32 specification was designed to simplify architecture and reduce the technical integration burden compared with the previous M2M standard (SGP.02), **80% of MNOs still foresee long-term costs and complexity as their main deployment challenge**. This caution reflects margin pressure in the IoT connectivity market and the limited track record of SGP.32 so far. Yet these concerns are largely offset by strong demand from IoT customers, who see the opportunity to expand eSIM usage across a broader range of devices, including low-power ones.

To fully realize the benefits of the new specification and turn it into a driver of your IoT business growth, consider the following key levers:

- **Minimize integration friction with OEMs and your enterprise clients**
- **Leave the certification burden to your eSIM solution vendor**
- **Streamline eSIM digital workflow integration with your legacy systems**
- **Drive interoperability tests to scale with confidence**

Avoiding unforeseen, additional software integration costs starts with a turnkey eSIM solution that enables **direct exposure of eSIM management services to your IoT ecosystem partners and clients through a single API and intuitive user interfaces**. An agnostic platform supporting all device types, multiple card form factors (SIM, eSIM, iSIM) and single eUICC and profiles Stock Keeping Units (SKU) will simplify your operations and allow you to focus on what you do best: providing connectivity.

Choosing an **eSIM vendor providing end-to-end solutions certified by the GSMA**, like IDEMIA Secure Transactions[2], can help you streamline deployment and reduce the impact of evolving compliance and security requirements. Reducing integration and certification efforts allows you to focus on **modernizing BSS**[3] **legacy systems** to enable fully digital and highly efficient eSIM workflows—a second challenge reported by 71% of our study respondents. It also frees up resources to **resolve any remaining interoperability bottlenecks**, a critical step before eSIM IoT adoption truly scales.

## 2/ Shield your IoT operations from fraud, cyberattacks and quantum threats

Security and fraud risks are the third challenge highlighted by our study respondents, cited by 52% of them—and rightly so. As IoT connectivity expands, so will the attack surface. Cybersecurity in general, and **strong cryptographic defenses** in particular, along with **advanced detection capabilities** will be critical to protect your IoT systems and your clients. Unauthorized eSIM profile downloads or provisioning could compromise network security, integrity, and service continuity. Improper or outdated cryptographic implementations at the eSIM management platform level or at the end-point device level could also result in massive service disruption in a foreseeable future. To future-proof your operations against these risks it is important to:

- **Apply zero-trust principles** (check device identities, authenticate every user and requests, apply least privilege access rules and ensure continuous monitoring)
- **Detect unusual eSIM download patterns with AI-powered data analytics**
- **Stay ahead of emerging cybersecurity threats with crypto-agility**

While GSMA Security Accreditation Schemes (SAS-SM and SAS-UP) set the baseline for secure eSIM management and eUICC production, the extended lifecycle of IoT devices – sometimes exceeding 20 years – makes **ongoing security capabilities** a strategic imperative. Encrypted data is already being harvested today, and within 15 to 20 years, quantum computers are expected to break today's asymmetric cryptographic protocols. End-to-end quantum-readiness across the eUICC, eIM, and SM-DP+ platforms is critical to stay ahead of emerging security risks and protect your eSIM IoT deployments. This starts with quantum-ready chips designed to **support the transition to hybrid cryptographic protocols** combining classical and post-quantum cryptography. It also requires remote **eSIM OS update capabilities** that will enable long-term device crypto-agility, allowing cryptographic systems to adapt in the field as cybersecurity threats evolve.

## 3/ Bring value to your OEM and enterprise customers beyond airtime

As Matthew Iji, Director of Forecasting & Modelling at GSMA Intelligence clearly puts it in his "*IoT: Big Growth, Bigger Questions*" (August 2025) blog post *: "Success won't come from scale alone — it will come from those who can simplify complexity, deliver measurable value, and make IoT indispensable to the industries they serve."* [4] This view is shared by 97% of respondents in our study, who confirm that declining ARPU (Average Revenue per Device) is shaping their strategy and pushing them to **pursue new monetization levers** beyond connectivity. This includes offering professional services (such as consulting, integration, and support), delivering value-added services (such as business

intelligence, cybersecurity, and device management), or combining all of these into end-to-end turnkey IoT solutions.

At IDEMIA Secure Transactions we look beyond eSIM IoT specification implementation. We tap into our expertise in post-quantum cryptography, AI and data analytics and advanced OTA services, and we leverage our close relationships with OEMs to help you **build differentiating IoT services**.

---

[1] Online eSIM IoT Survey conducted by Kaleido Intelligence for IDEMIA Secure Transactions in summer 2025 with 154 MNO, MVNO, and MVNE participants.
[2] https://www.gsma.com/solutions-and-impact/industry-services/assurance-services/security-accreditation-scheme-sas/sas-accredited-sites/
[3] Business Support System
[4] https://www.gsmaintelligence.com/blogs/iot-big-growth-bigger-questions

---