

Managing eSIM connectivity
at scale for business edge
A build vs buy guide for executives

Introduction

Flexible remote SIM management technologies are emerging to support cellular Internet of Things (IoT) connectivity at a scale and cost that previously was not possible. Specifically, eSIM and SGP.32 will support flexible and globally deployable connectivity solutions for large fleets of devices that vary from full gateways to battery powered devices that may not be visible on public networks. These new technologies will introduce new complexities, but focussed vendors offering as-a-service solutions will smooth the adoption path for any end-user adopter, equipment manufacturer or connectivity provider. Executives today need to consider the time and investment required in key control points for the eSIM management stack since resilient and critical connectivity can accelerate innovations built around business intelligence, Edge AI, trusted data and cybersecurity.

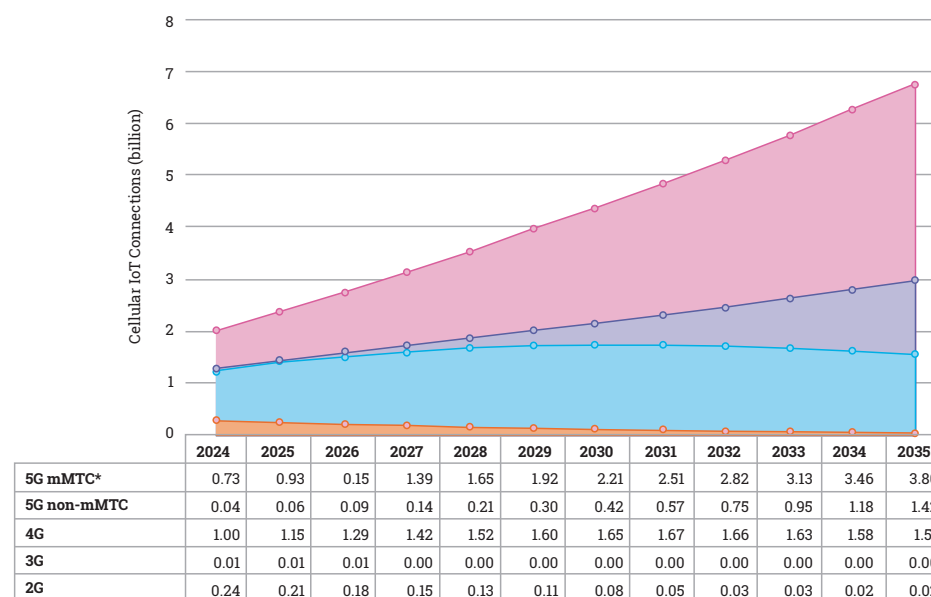
Thinking about IoT differently: eSIM and SGP.32 Remote SIM Provisioning

In the age of AI, IoT brings new context: allowing insight into assets, operations, and key business processes with data that can enhance operating profit or allow faster global expansion. Transforma Insights has forecast the growth of IoT connections and the transition from 4G towards 5G technologies including NB-IoT and LTE-M. All of these cellular technologies are well-suited to remote SIM provisioning. With the addition of AI, IoT is a critical component of business growth – here is where eSIM and the new evolution in remote management stack propositions unlocks new potential.

eSIM and SGP.32 are new terms in IoT contexts. eSIM describes a digital-first approach to deploying a mobile network operator (MNO) connectivity profile onto a cellular connected device. eSIM is independent of form factor, and the necessary credentials could be stored on a traditional SIM card, or compact embedded SIMs (typically standardised as MFF2, MFFXS or MFF4).

Transforma Insights has forecast the growth of IoT connections and the transition from 4G towards 5G technologies including NB-IoT and LTE-M

Figure 1: Cellular IoT Connections 2024-2035



*5G mMTC includes antecedent 4G technologies NB-IoT and LTE-M

A key enabler for eSIM adoption is the GSMA's SGP.32 specification, which supports secure over-the-air (OTA) remote SIM provisioning (RSP) now adapted for large fleets IoT devices and connectivity choice. SGP.32 brings connectivity choice closer to the experience of (SGP.22) consumer eSIMs. The new standard enables devices to ship with or without an initial operator profile that supports immediate out-of-the-box connectivity. This may be required in case the device doesn't provide an alternative interface to download new profiles, as many IoT devices lack user interfaces. Once connected and with device location, context, and other parameters identified, a subscription management platform can remotely download and activate a local operator

profile. This allows the device to connect to the most suitable mobile network without requiring physical SIM replacement or any kind of manual intervention. In some cases, the initial profile may be the final one used by the device.

eSIM and SGP.32 together are a boon for IoT markets since they allow for significantly simplified supply chains. With these technologies, an OEM can provision an initial operator profile in the factory (often referred to as IFPP for In-Factory Profile Provisioning) and offer a single stock keeping unit (SKU) for global markets. Such solutions can be deployed with lower initial investment, and these new technologies allow for easier remote management during a device lifecycle.

Widespread support for SGP.32

With the advantages described above, cellular and IoT industries both have been keen to adopt SGP.32 to support eSIM remote management. SGP.32 is a well-defined standard, and a wide range of

stakeholders are expected to develop their own SGP.32 capabilities, including vendors in the cellular IoT ecosystem as well as certain end-user organisations.

Seek first connectivity as a strategic decision point

For promoting the adoption of your IoT telco capability, being the first connectivity option for a device can be a key aspect of risk reduction and easing global expansion. If you already have telco capabilities, this is a point of differentiation: a way to create loyalty and customer retention or to build innovative specialisations for IoT connectivity.

Source: Kigen

Once connected and with device location, context, and other parameters identified, a subscription management platform can remotely download and activate a local operator profile

What is in an eSIM solution



The SGP.32 standards define a range of key system components which any entity developing an in-house solution will need to consider. The eUICC in the device securely stores eSIM profiles and performs authentication with mobile networks. An IPA (IoT Profile Assistant) runs either on the device (IPAd) or on the eUICC (IP Ae) and communicates with external systems to request, download, and manage profiles

for IoT devices. The eIM (eSIM remote IoT Manager) orchestrates remote lifecycle management, deciding which profiles a device should use and coordinating provisioning actions at scale. Meanwhile the SM-DP+ prepares, encrypts, and secures operator profiles end-to-end, enabling remote installation and switching of connectivity for IoT devices.

With SGP.32, the eIM will mainly do the secure delivery of profiles in three use cases:

- (1) constrained IoT networks where the device traffic is routed through the eIM,
- (2) constrained devices, where the eIM acts as a proxy to complete the messages for communication between DP+ and Device (for example, if IP Ae is used, then you need to go through the eIM if IP Ae implements only ASN.1 binding),
- (3) private networks or air gapped scenarios where the device doesn't have access to public internet and the devices can't directly reach the DP+.

Source: Kigen

Required technical interactions with other ecosystem players, including cellular operators and eSIM-enabled device vendors, and more, are also defined in the standards. However, cellular IoT environments are complex, so any entity seeking to develop their own SGP.32 capabilities to manage eSIMs would need access to sophisticated IT development capabilities, and also invest significant resources in full security certification capabilities.

But, given SGP.32's status as a defined standard, such barriers can be overcome by any entity wanting to develop their own in-house eIM capabilities, and many organisations are likely to pursue such a strategy.

Required technical interactions with other ecosystem players, including cellular operators and eSIM-enabled device vendors, and more, are also defined in the standards



SGP.32-aaS will have distinct advantages



In addition, a range of specialist vendors is expected to emerge to support evolving eSIM and SGP.32 use cases, including providers offering differentiated and market-leading capabilities delivered as a service.

Such services will be available off the shelf and with quick integration. The required certifications for compliance with SGP.32 standards will already be complete. But more importantly, such solutions should have already undergone interoperability testing with a range of ecosystem partners, including connectivity providers, vendors of supporting systems and platforms, eSIM vendors, and device vendors. This is an important consideration, since interoperability testing is not simply a technical exercise. It also relies on

commercial agreements between the relevant parties as a precondition for testing to commence and to be supported and maintained over time. Comprehensive interoperability testing with a wide range of ecosystem players also unlocks downstream operational benefits, reducing the risks associated with any IoT solution rollout and ongoing evolution.

In addition, given their focus on SGP.32 and eSIM, aaS providers in this space will have extensive interactions with end-users adopting eSIM technologies, and the full range of supporting ecosystem players and also with standards development bodies. Such comprehensive exposure to the ecosystem enables a more complete understanding of market-level dynamics, and any emerging challenges that different

players might be facing and how those organisations are seeking to overcome such challenges. Accordingly, establishing a relationship with a focussed SGP.32 and eSIM vendor can provide forward-visibility into market developments, again de-risking the adoption of these technologies. It can provide insight into innovative approaches that are developing across the industry, and also tried and tested patching and recovery techniques in the event that these are needed. Such vendors will offer comprehensive associated reporting and monitoring capabilities that will evolve over time, informed by their broad experience, with an ever-increasing corpus of specific events and associated resolutions available to train agentic AI solutions that can radically increase network and operational efficiency.

Comprehensive interoperability testing with a wide range of ecosystem players also unlocks downstream operational benefits, reducing the risks associated with any IoT solution rollout and ongoing evolution

Meanwhile, integrations to the full connectivity management software stack, including connectivity providers and Connectivity Management Platforms (CMPs) and associated OSS/BSS can reduce the complexity of integrating with an ecosystem of partners and support the maintenance of strong ecosystems.

Many such vendors will also develop value-added capabilities that are beyond the scope of contemporaneous standards. In today's market, for example, these include value-adding applications that reside on the eSIM (eUICC) that might assist with the optimisation of connection configuration, and also multi-IMSI and multi-eSIM solutions.

Lastly, it should be noted that whilst SGP32 is a standard, not all aspects of the specification are mandatory, and some defined aspects are categorised as non-mandatory. In effect, this means

that different implementations of the specification are likely to have different functionalities, with not all implementations supporting full functionality. From an adopter perspective, it is worth considering whether any specific provider's eSIM stack includes implementation of required optional aspects and has put these through the GSMA's eSA certification. The details are available from vendors through their declarations of certified products.

To develop aspects of a solution fully in-house, business leaders should carefully evaluate which parts of the eSIM stack they need to create bespoke to them. It is worth noting that while standards such as SGP32 are mature, there will be incremental changes in the future to further benefit the industry. Cyber resilience is one such theme. An aaS provider will also have good visibility of expected changes to the standards, and leading vendors may in addition have input to standards developments over time.

Bottom line: invest the effort in understanding what eIM capabilities serve well in the long run.

Standards set the conditions for all players in the market to be competitive and to operate effectively. Many of the unique features within how these standards are implemented matter greatly. Look for mandatory and optional features that suit your business needs – for example, when sourcing eSIMs, certification for eSA requires testing with an eIM as optional. If you operate a private network or within critical infrastructure contexts, choosing the eIM with certified SAS capabilities will also benefit from greater acceptance with other networks, while the indirect download capability gives you full visibility to devices that are to be protected from direct internet connection. The drivers for these may be different: better cybersecurity posture or reducing latency for connections in your processing plant.

Source: Kigen

Future proofing for market access:

For procurement executives, the emerging regulations make it essential to collaborate with IT cybersecurity firms to ensure you are getting the best fit features that will create lasting resilience. A key benefit of eSIM technology is that it is already supported by an advanced, mature infrastructure that promotes security and interoperability. A core element of this infrastructure is the eUICC Security Assurance (eSA). There are solutions on the market that have led the march to CRA-compliant updates and deliver this within eSA-certified eSIMs. Kigen's eSIMs are one example that take interoperability and compliance as a default capability across both consumer and IoT eSIMs, and patchability reporting and verification are part of [Kigen eSIM solution](#). Here, the key part for executives and procurement leaders is how you source a pre-validated and packaged stack that clearly addresses your vision today and 5 years out.

Source: Kigen

A note on regulatory compliance

Until recently, IoT has been subject to relatively light-touch regulations around the world. This is changing quickly though. One of the key emerging regulations is the European Union's forthcoming [Cyber Resilience Act \(CRA\)](#), but similar guidance is emerging in many countries around the world. EU CRA introduces horizontal cybersecurity requirements for all products with digital elements available on the EU market, ensuring a broad and consistent approach to cybersecurity. All smart cards and eSIM devices are classified as 'critical' assets and require third-party assessment. Amongst other things, the CRA specifies that onboard device software should be updatable for security patching during the lifecycle of the device in question, and that the device software bill of materials (SBOM) should be auditable, and that vulnerabilities should be monitored for and any incidents reported within prescribed timelines.

A related operational requirement is that reporting from relevant SGP.32 control and management systems to cybersecurity compliance tools should be supported, for example with Application Programming Interfaces (APIs).

CRA compliance is not yet considered as part of the mandatory features of the SGP.32 standard and work is ongoing to reflect the relevant requirements in the coming versions of the standards. In the meantime, it will be the responsibility of any company offering SGP.32 services to develop their own approach to compliance, and ideally in a way that will be consistent with the relevant standards as and when they are published.

Conclusions

eSIM and SGP.32 eSIM management together represent a major step forward in simplifying and scaling cellular IoT connectivity. By enabling secure remote SIM provisioning, bootstrap connectivity, and automated operator profile management, they significantly reduce operational complexity and enable global, factory-provisioned deployments. The SGP.32 architecture provides a structured and standardised framework for managing device connectivity across its lifecycle. Implementation of SGP.32 requires strong technical, security, and interoperability capabilities, but the emergence of specialised as-a-service providers will lower adoption barriers.

For C-Suite leaders, the question is will you build the car from scratch, or get with driving it in the fast lane?

Please also see the following report: