Mastering eSIM IoT at scale: key insights from SGP.31/32 early implementations

Overcoming implementation challenges and driving seamless integration with the SGP 31/32 specification.

CONNECTIVITY

POSTED ON 11.25.24

The introduction of the SGP.31/32 specification marks a pivotal advancement in the eSIM IoT connectivity market, unlocking a number of new opportunities.

Offering greater flexibility and openness, the SGP.31/32 standards intentionally provide freedom in certain areas, allowing for diverse implementations tailored to specific needs. To ensure the success of real-life deployments, early trials have revealed that **additional guidelines and best practices** are required. This article outlines key insights and solutions to facilitate seamless integration, interoperability, and optimized performance across various devices and networks.

The genesis of the eSIM IoT SGP.31/32 specification

While the existing M2M specification, SGP.01/02, is effective for always-on powered devices on unconstrained networks, such as connected cars, it is unsuitable for low power devices like gas meters, water meters, or battery-powered appliances.

The GSMA proposed the new eSIM IoT SGP.31/32 specification to meet the needs of massive IoT connectivity and enable the remote management of IoT device fleets. Numerous stakeholders collaborated to address new eSIM IoT use cases and verticals with this new specification.

An overview of the eSIM IoT specification components

The IoT eSIM standard is derived from the Consumer eSIM standard (SGP.21/22) with some distinctive differences tailored to IoT applications.

The Subscription Manager – Data Preparation+ (SM-DP+) retains its role from the Consumer eSIM standard, handling the hosting, preparation, and download of eSIM profiles.

Two new components are introduced: the eIM and the IPA.

- The **eSIM IoT Remote Manager (eIM)** is the remote controller of the IoT device fleet. It is responsible for managing profile state operations on the eSIM (i.e. on the eUICC, or embedded Universal Integrated Circuit Card): remote profile enabling, disabling, deletion, and triggering profile downloads.
- The **IoT Profile Assistant (IPA)** acts as a mediator between the eSIM and the eIM, facilitating the download and installation of eSIM profiles through the SM-DP+.

Proofs of concept of SGP.31/32 end-to-end solutions

Over the past two years, numerous proof-of-concept projects have been launched to test the new SGP.31/32 specification before large-scale commercial deployments expected by the end of 2025. Major device manufacturers and Mobile Network Operators (MNOs) have collaborated with service providers to identify the most effective and efficient solutions in the field and determine necessary complements. The objective is to achieve IoT deployments in the simplest and most effective manner possible.

Key challenges of the SGP.31/32 specification

Challenge 1: No migration path from M2M to IoT

Existing M2M deployments will continue to operate under their current models until they reach the end of their lifecycle. This will create challenges in **simultaneously managing both legacy systems and new IoT deployments** —for instance, this will be the case for car manufacturers who have already implemented the M2M specification and will switch to the eSIM IoT specification to benefit from its simpler and less restrictive deployment architecture.

A centralized management system for all devices, whether IoT or M2M, is needed. This system will provide a single point of contact for managing all devices, allowing rules to be created based on business needs. This could include, for example, the ability to set up remote and automatic change of connectivity providers for a fleet crossing a border—without worrying about the eSIM specification (M2M or IoT) used to connect each individual car or device composing that fleet in the first place.

Challenge 2: Huge diversity of IoT devices

To address the diversity of IoT devices, which is set to grow exponentially, the eSIM IoT specification offers flexibility in the placement of the IoT Profile Assistant (IPA). The IPAe is located within the eUICC, whereas the IPAd is integrated directly into the device.

- **The IPAd (IoT Profile Assistant in the Device)** is suitable for devices with robust operating systems and sufficient computational power. The device maker is responsible for developing the necessary software and meeting the protocol requirements.
- **The IPAe (IoT Profile Assistant in the eUICC)** is ideal for devices that can't support the IPAd such as low power devices or when the device maker chooses not to develop it. The eUICC provider handles the development, making it a simpler option—without additional work for the device maker.

While IPAe and IPAd offer the same functionalities, **integrating the IoT Profile Assistant into the eUICC (IPAe) brings significant advantages** for OEMs and provides the smoothest path towards eSIM remote management capabilities.

To effectively accommodate diverse device characteristics, OEMs should also consider selecting an eSIM management supplier providing **just-in-time eSIM profile generation capabilities**. This allows for the adaptation of eSIM profiles at the last possible moment.

Challenge 3: Interoperability between eIM and IPA

For greater flexibility, the SGP.31/32 specification allows device makers the freedom to choose **communication protocols** between eIM and IPA supported by their devices. A modular architecture for the eIM component, capable of communicating with various IPAs (IPAe or IPAd) provided by different vendors, can guarantee interoperability whatever the device.

Challenge 4: Scalability

Enterprises must be able to support the connectivity of numerous devices and handle fluctuations in activity, such as a logistics operator moving an entire fleet of high-worth asset trackers across borders. Platforms must have a global reach to ensure the availability of these critical systems. **Deploying eSIM solutions in the public cloud** can enhance scalability and allow for effective management as loads increase.

Challenge 5: Security

Public cloud deployments also offer greater security, including regular system updates and patches, robust DDoS protection, built-in redundancy and disaster recovery, strong access control, and data encryption.

The eIM introduced by SGP.31/32 requires specific security protocols with the eUICC, which will only accept requests from authorized and authenticated eIMs. **SAS (Security Accreditation Scheme) certification for eIMs**, although not mandatory, provides an additional layer of security.

As many IoT devices will remain in the field for decades, it is also important to anticipate the eventuality of quantum threats by selecting an eSIM solution supplier that supports **post-quantum cryptography**. Existing cryptographic solutions need to be assessed, and preventive actions should be taken to upgrade device connectivity security in the field.

Challenge 6: Low-end devices with very limited space and power

Fully integrated into the device's main chipset, iSIM (integrated SIM) will answer the needs of devices that are especially constrained by size and energy requirements, as well as those deployed in hazardous environments. **An SGP.31/32 certified iSIM** will integrate seamlessly with a comprehensive eSIM IoT management solution.

Ensuring efficient and streamlined eSIM IoT implementation

The first implementation trials of eSIM IoT solutions in accordance with the SGP.31/32 specification have confirmed the flexibility and openness of the new GSMA specification and its potential to transform IoT connectivity and boost eSIM adoption. They have also helped identify several key challenges.

By proactively adopting best practices and with gathered insights, the IoT ecosystem can fully leverage the promise of eSIM IoT technology.