TRANSFORMA INSIGHTS

flo. LIVE

ANALYST REPORT

eSIM/eUICC evolution with SGP.32 and why it doesn't solve every IoT connectivity need

Matt Hatton
Transforma Insights

Introduction

Until 2016, cellular connected devices were authenticated onto a network using a removable plastic SIM card. This wasn't particularly appropriate for many IoT use cases, which required a more ruggedised form factor. The machine form factor (MFF, now MFF2) was launched, comprising a chip to be soldered onto the circuit board of the device. As a result of this change in the physical form factor, it was necessary to develop the capability to change the SIM profile through a mechanism other than physically swapping SIM cards. That mechanism is remote SIM provisioning (RSP), i.e. remotely switching profiles over-the-air without needing to access it physically. This combination of changing hardware and remote SIM provisioning service is collectively grouped under the terms embedded universal integrated circuit card (eUICC) and embedded SIM (or eSIM), writes Matt Hatton, a founding partner of Transforma Insights

Based on the requirement for remote SIM provisioning, the GSM Association developed a set of standards. The SGP.02 (or "M2M") standard was introduced in 2014, adopting a 'push' model, whereby the MNO/MVNO (or often an outsourced SIM vendor partner such as **G+D, Kigen** or **Thales**) controls the process end-to-end. This was followed in 2016 by SGP.22 ("Consumer") where the end user can 'pull' a new profile from a chosen provider down to the device.

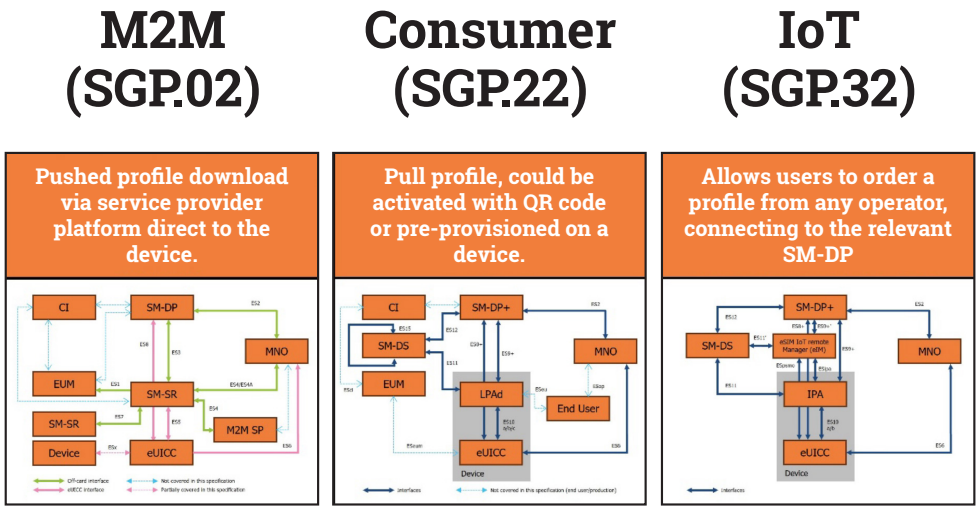
In May 2023 a third variant of the eSIM remote SIM provisioning standards from the GSMA was unveiled. The SGP.32 ("IoT") variant was aimed at resolving some of the limitations of the earlier SGP.02 and SGP.22 versions. The finalisation of the testing and certification processes is due in early 2025 and compliant devices can be expected later this year.

This report explores some of the implications of the availability of remote SIM provisioning and particularly the new SGP.32 standard.

SGP.32 gives more freedom to customers

Each of the three RSP standards establish slightly different mechanisms for the user or owner of a device to change the SIM profile while the device is deployed in the field. There were several limitations to the first two standards. SGP.02 is managed by the connectivity provider and requires its approval to initiate switches, as well as integration between the SM-DP platforms of the two operators. There is therefore a form of lock-in for the customer to the provider and a lack of control for that customer. Meanwhile SGP.22 was designed for a device being used by a person. It required the scanning of a barcode (and thus was limited to devices with a camera onboard), manual intervention via an advanced UI, and a device supporting SMS (which some IoT-oriented technologies do not).

SGP.32 solved some of these problems. In doing so it effectively adapted the SGP.22 approach to be managed remotely. Instead of a local profile assistant (LPA), which the user would use directly to initiate profile changes, it incorporates an IoT profile assistant (IPA) sitting on the device, being controlled by an eSIM IoT remote manager (eIM) which is hosted by a network operator or other third party. Using this IPA/eIM, the customer (or someone acting on their behalf) would be able to pull a profile from any MNO/MVNO (assuming that operator agrees). There is no requirement for the current MNO/MVNO to agree to the migration and/or integrate with the would-be recipient operator.



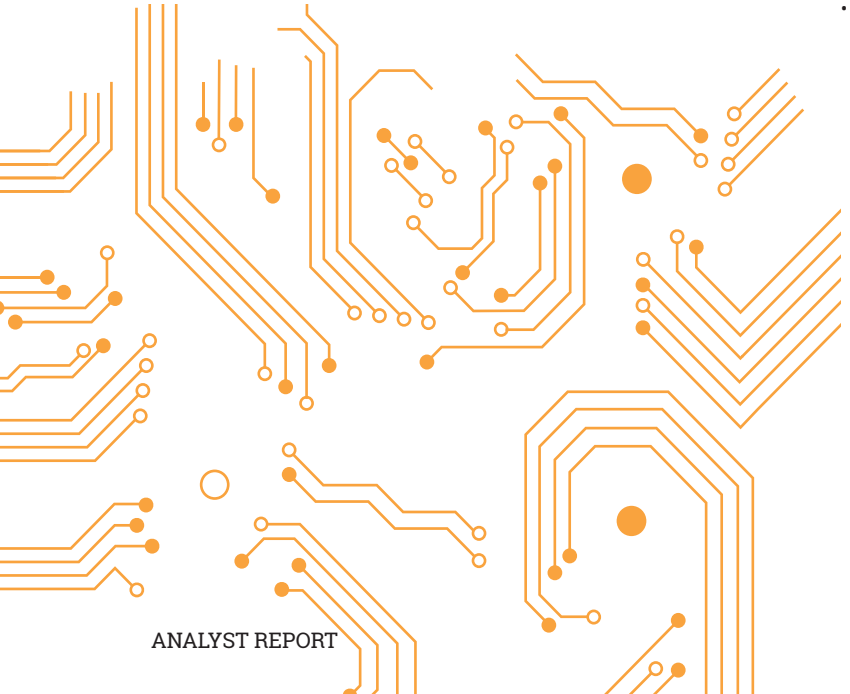
SM-DP (Subscription Management Data Preparation) – stores eSIM profiles and prepares for download
SM-SR (SM Secure Routing) – establishes secure channel to the eUICC to manage it.
SM-DP+ (SM Data Preparation and Secure Routing) – both elements handled through a single platform
SM-DS (Discovery Service) – optional add on for Consumer, where SM-DP+ address is unknown to eUICC
LPA (local Profile Assistant – local profile to communicate with SM-DP+ located on SIM or device

Figure 1: GSM Association standards for eSIM remote SIM provisioning (RSP)

[Source: Transforma Insights, 2024]

What are the implications of the arrival of SGP.32?

In this report we will focus on the impact on the shift from SGP.02 to SGP.32 for enterprise deployments. This is the most significant change, although we do note that for consumer product OEMs a shift from SGP.22 to SGP.32 does offer some alternative options for remotely managing their subscriber devices. Compared to SGP.02, SGP.32 allows a customer to switch its IoT connections (theoretically) to any connectivity provider it chooses without recourse to the operator upon whose SM-SR it resides. Nominally this change gives much more freedom to enterprise customers to 'at the click of a button' move some or all of their connections from one network to another.



Challenges with SGP.32

Transforma Insights notes many significant benefits stemming from the arrival of SGP.32. However, we also note that it is not a magic wand that will solve all the challenges of delivering IoT connectivity. For instance, any enterprise considering making use of SGP.32 should consider the following:

- **This is a brand new technology**. While there have been precursors, in the form of both SGP.02 and SGP.22 (plus proprietary versions of the latter which imitate SGP.32 very closely), SGP.32 is only finalised in Q1 2025. As such there are potential unknowns about how it works in practice. And, we should note, with nearly a decade between its initial introduction and the adoption of new standards, eSIM has been slow and limited in reacting to market changes and needs.
- **Variable support between MNOs.** The extent and mechanism for support of SGP.32 varies between MNOs. For instance, in some cases the MNO will allow a third party to host the eSIM profiles, whereas in the case of others it will not. This lack of consistency can create some complexity for deployments.
- **The need to strike network contracts.** If a device owner wishes to port its connection to another network, it must have a commercial relationship with the recipient connectivity provider. This constrains the appeal of the technology to those customers who have relationships with more than one carrier (and potentially dozens), which might be the case with car makers or other big buyers. For relatively small customers, and/or those connecting devices in many countries, this represents quite a logistical headache, managing potentially dozens of connectivity contracts. It also may require an integration with a new connectivity management platform (CMP), management of a billing relationship with each MNO, management of an inventory of profiles, and the need to maintain relationship with multiple MNO support teams.
- **Negotiating power.** A single customer for relatively small numbers of connections in each market will have limited negotiating power compared to an MNO relying or reciprocal roaming agreements or MVNOs with much larger volumes of devices within in any given market. Therefore in many cases it would be better for the buyer to procure connectivity via a third party acting on their behalf, as a managed service. This means the commercial dynamics will be quite similar to those currently seen between enterprise customers and MNOs/MVNOs today.
- **Back-end integration**. Even where a user might have commercial relationships it's not generally simply a case of switching between providers seamlessly. There will be a requirement for back-end integration and other process changes, for instance to manage VPNs, change APN settings, establish frequency of polling for new profiles, or handle different SLAs. This is a non-trivial task, and one that will need to be performed simultaneously with the eSIM profile switching.
- **Regulatory compliance.** One of the main reasons for using SGP.32 (or any form of RSP) is that it allows for localisation onto a local network and thus ensuring compliance with 'permanent roaming' restrictions. However, SGP.32 does not in itself ensure this. It requires that the profile onto which the connection is localised is itself compliant. Not only that, but there is a much wider set of compliance considerations beyond just localisation of the connection, for instance related to know-your-customer (KYC) or data sovereignty rules.
- **Cost.** There is an additional cost associated with profile switching and profile hosting, which could be as much as USD1/month per profile.

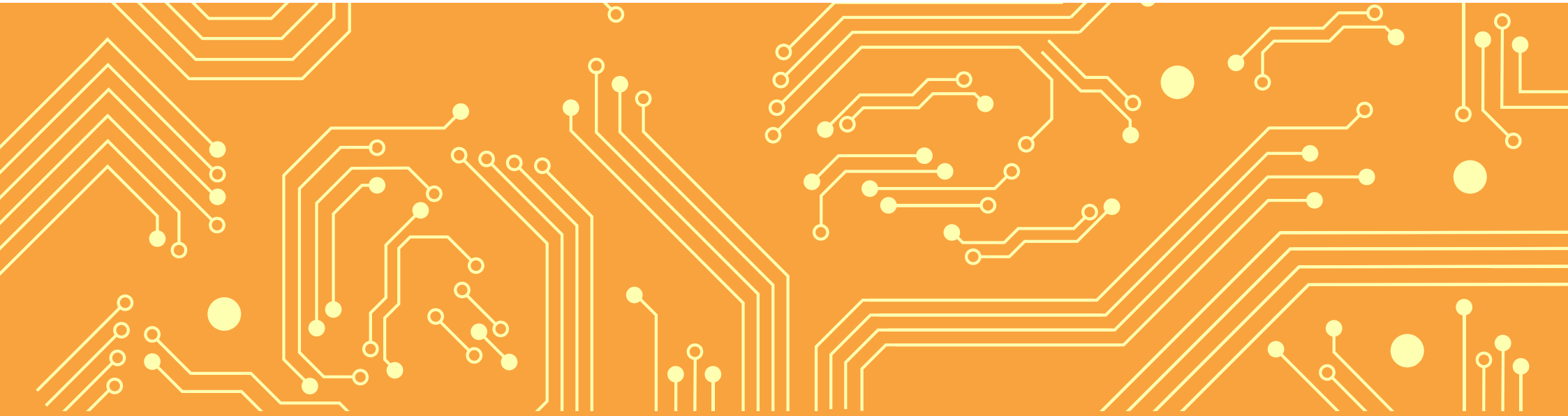
The underlying conclusion regarding SGP.32 is that it is a very useful tool, but it comes with several associated costs. Furthermore, it is one that is best delivered as a managed service with a wrapper around the remote SIM provisioning to address the issues identified above. And, furthermore, one which allows for an on-ramp to what is a new technology.

There will continue to be a diversity of approaches The arrival of SGP.32 – and the other preceding remote SIM provisioning technologies – provides a very useful set of tools for addressing some of the challenges of cellular-based IoT connectivity. However, we should note that there are numerous other options, each of which might be at least as appropriate.

The use of a single IMSI SIM will often provide perfectly adequate connectivity. In fact, in many ways it will be simpler, with all connections being managed on the same core network and via the same connectivity management platform, rather than localised onto multiple operator networks and managed through multiple platforms. This type of SIM could be a single country IMSI, using a domestic operator, but more likely it will be a roaming SIM, often using an MCC-901 non-geographic country code. Such roaming SIMs can take advantage of national roaming. There are good reasons for localising connectivity using RSP, particularly for high bandwidth use cases and/or where there is a regulatory requirement to do so. But that does not account for the majority of connections.

Beyond this is the option to use a multi-IMSI SIM. Such a SIM includes multiple operator IMSIs pre-loaded onto the device and therefore available for supporting the connection at any time. In circumstances where a device might need only a limited number of options, then the multi-IMSI can be a perfectly adequate solution. And even where there are regulatory challenges, it can include profiles that are compliant in 'difficult' markets. This is a non-standards-based approach and therefore typically not favoured by MNOs, but many MVNOs do provide such a service. However, it is a tried and tested technology in the market the flexibility of which has been proven for more than a decade. While eSIM might have advantages in terms of compliance and better performance through the use of local profiles, multi-IMSI is typically cheaper, with often better network coverage and availability.

One of the more popular approaches to delivering multi-country connectivity is by way of a multi-IMSI solution which also includes the ability to remotely provision the SIM with additional new profiles if they are required.



Conclusions: Hybrid approaches and the right partner

Transforma Insights expects that devices managed via remote SIM provisioning will grow rapidly over the next decade but will remain the minority of new connections over that period, albeit approaching 50% at the end of it. SGP.32 will become the de facto standard for remote SIM provisioning (RSP) based on the fact that it overcomes many of the limitations of SGP.02 and SGP.22. However, there will be numerous scenarios in which other approaches to connectivity will be appropriate. The same is also true of the tried-and-tested multi-IMSI, which will be appropriate for many types of IoT deployments. Combining the two can create a robust and versatile solution. Using an eSIM with a Multi-IMSI SIM as the first profile allows organisations to enjoy the extensive coverage and cost-efficiency of multi-IMSI solutions while also capitalising on the compliance, performance and flexibility of eSIM technology.

The best approach for enterprises wishing to procure cellular-based IoT connectivity is not to 'hit and hope' by trying to pull together their own SGP.32-based connectivity proposition. For all of the reasons stated above, a better approach is to seek out a trusted vendor that has a portfolio of offerings – including SGP.32 and other options – from which the most appropriate can be selected. Such a vendor should additionally be able to provide a wider set of support on topics such as compliance, data management and deployment optimisation.