How will the GSMA's new eSIM Consumer IoT specification pave the way for massive IoT?

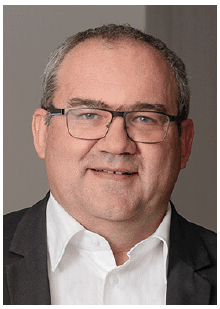
Interview with Stephane Jayet, Head of Digital Business Line in Connectivity Services Business Unit at IDEMIA

CONNECTIVITY

POSTED ON 03.06.23

In April 2022 the GSMA published the SGP.31 eSIM Internet of Things (IoT) Architecture and Requirements Specification. This new specification, sometimes referred to as the IoT Remote SIM Provisioning (RSP) specification, defines the architecture and requirements for the remote provisioning of eUICCs in Network Constrained and/or User Interface (UI) Constrained IoT Devices. We sat down with **Stephane Jayet, Head of Digital Business Line in Connectivity Services Business Unit at IDEMIA**, to better understand how this new specification will give way to the massive deployment of eSIM technology in the IoT space.

Why did the GSMA decide to create this new eSIM IoT specification?



To understand where we are going, we must first look at where we came from. On one hand, we have the existing eSIM M2M specification[1], which works well for major OEMs and MNOs in markets with minimal energy or communication constraints. On the other hand, the eSIM Consumer specification[2], which has been widely deployed by MNOs to support the adoption of eSIM technology for smartphones and other consumer devices. Neither is truly adapted to address massive IoT, which comes with specific challenges and constraints related to the large variety of IoT devices. Massive IoT connectivity requires a **simpler integration model** that also addresses low power devices and networks.

The new specification **combines the best of the existing specifications** to support constrained devices and simplify the integration between a large number of OEMs and MNOs. By leveraging the SM-DP+ (Subscription Manager – Data Preparation) and APIs (Application Programming Interface) already in use and widely deployed for the eSIM Consumer market, the new specification avoids the multiplication of proprietary solutions and the creation of yet another subscription management platform.

How will the new eSIM IoT framework better address constrained devices?

Massive IoT devices are typically low-cost devices connected to Low Power Wide Area (LPWA) networks. These can be smart meters, asset trackers used in shipping containers, and various other sensors that may be installed in smart cities.

They are often constrained in terms of **communication protocol, battery capacity and/or user interface**. As it stands today, the existing eSIM M2M specification can't address these devices as triggering an operation requires the eUICC to receive an SMS to connect to an SM-SR (Subscription Management – Secure Routing). Similarly, the eSIM Consumer specification is also incompatible since most of these IoT devices lack the user interface necessary to trigger a subscription request. Furthermore, these devices are typically scattered around a wide area, unsupervised and difficult to reach, making access challenging, if not entirely impossible.

The eSIM IoT specification introduces a new architecture that **switches from the push model used for M2M to the pull model used with the Consumer specification**. This is done via a new entity, called the eSIM Remote Manager (eIM), and an IoT Profile Assistant (IPA) which can be located in the device (IPAd) or inside the eUICC (IPAe).

What exactly is the eSIM Remote Manager (eIM) and what is its role?

Put simply, the eIM is a software that replaces the end-user and allows IoT devices to trigger subscription downloads from the SM-DP+. It can either be run on a server to manage a device or fleet of devices or could be a simple app running on a laptop or smartphone. It provides an **interface that IoT devices are missing**, making it possible to manage eSIM profile downloads remotely.

And since some low power devices don't have enough power or capacity to connect to the internet with HTTP, the eIM can also handle the HTTP interaction and serves as an **intermediary with the SM-DP+ server** to provision and manage eSIM profiles on the eUICC using lighter weight communication protocols supported by the devices. The new solution ensures end-to-end security between the eUICC and the SM-DP+, in the same way as in the eSIM Consumer model.

Will the new specification create new business opportunities for MNOs?

Over the next four years, LPWAN solutions will be one of the fastest-growing cellular IoT technologies, along with 5G. In fact, 2.2 billion cellular IoT connections will use licenced LPWAN[3] in 2027, up from 162 million in 2020[4]. Given this growth, it is clear that **massive IoT represents a huge business opportunity**.

Since the new eSIM IoT specification reduces integration complexity, it gives MNOs a new market opening with massive IoT. Without complicated integration and excessive associated costs, **every MNO with SM-DP+ in place can now position themselves** as a provider of this new eSIM IoT solution and address all the constrained devices they couldn't serve before. And the best part is, they don't need to change their infrastructure because they can leverage existing Remote SIM Provisioning (RSP) platforms and APIs to address massive amounts of low-cost devices spread in various locations.

What about the OEMs?

OEMs, who once partnered with a limited number of operators, can open up to any operator at any time, with minimum integration effort. Let's use the example of a container ship traveling from one country to another. In this new eSIM IoT ecosystem it will be much easier for the OEM to download a new profile from a local operator to avoid roaming charges or even set parameters that automatically trigger a local subscription download when their devices are roaming. In short, the new specification **multiplies the possibilities of using local connectivity providers**, reduces roaming costs and avoids permanent roaming issues.

Major M2M OEMs, such as car makers, may also leverage the new eSIM IoT specification, which is more flexible and relies on an easier integration model to **engage with a larger number of MNO partners**.

Getting back to the solution architecture, could you explain how the integration model will change?

The M2M ecosystem, as it exists today, is based on two separate servers (the SM-DP (Subscription Manager – Data Preparation) and SM-SR (Subscription Manager – Secure Routing). That means that when an OEM contracts with 10 MNOs they have to connect with 10 SM-DPs and conduct interoperability tests between SM-DP and SM-SR platforms 10 times to ensure that everything is working properly. They then have to multiply that by the number of eUICC providers with whom they are working. In this scenario, while it might be manageable for a global OEM to have 10 MNO partners, any more than that becomes very complex, if not impossible. The process is not only complicated, but can also be very expensive. This is where the new specification comes in. It relies on a single platform, the SM-DP+, that **exposes a simple API using the HTTP channel**. Depending on the device and eUICC capabilities, it either directly connects to the SM-DP+ or uses the eIM as an intermediary—which means any device can connect and receive a profile.

Are there any changes at the eUICC level?

While there is no real change to the eSIM hardware or the eSIM profile, what will change is the eSIM OS, or software. Here, the eUICC will basically use a **hybrid version** of the OS currently used in the Consumer and M2M ecosystems. While the IoT eUICC will need to directly or indirectly (via the eIM) **connect to the SM-DP+**, as the Consumer eUICC, the new eSIM IoT specification will also likely feature a **rollback fallback mechanism**, similar to the M2M eSIM specification. This mechanism is important if an IoT device needs to change network providers or load a new profile when it is out of range. This could be a shipping container in the middle of the ocean, for example. In this scenario, if the eUICC isn't able to connect to a new network, it will roll back to the previous network until it can connect to the new one. This ensures that the device will never be without connectivity—which is crucial for the majority of new IoT use cases.

How can IDEMIA help OEMs and MNOs make the most of the new IoT specification?

We are essentially reusing as much as we possibly can from the previous specifications and adapting to cater to constrained IoT devices. As we prepare for a smooth transition with the new specification, we continue to support existing specifications. Our primary goal is to **simplify and minimize any additional integration for MNOs and OEMs**. We are extending our existing M2M orchestration layer, called the Smart Connect Manager, to automatically detect the underlying eSIM technology (IoT or M2M) and redirect orders to the right platform (SM-DP+ and eIM or SM-DP and SM-SR). It also facilitates connection to multiple Connectivity Management Platforms (Ericsson, Cisco, Vodafone, etc.) and ensures complete business process management by enabling OEMs to trigger any connectivity management operation.

To further **streamline eSIM profile ordering and management** for MNOs, our orchestration layer works hand-in-hand with our Digital Personalization Service (DPS) which handles just-in-time profile generation and enables a single profile ordering mechanism. Concretely, it allows an MNO to order generic profiles, for both M2M and IoT use cases. Once the targeted device is detected, the DPS adapts the profile to the device and eUICC capabilities at the last minute, ensuring that the eSIM profile corresponds with the targeted device. This function is particularly essential given the rapidly increasing diversity and quantity of IoT device characteristics. We are also actively working on **integrating the IoT Profile Assistant into the eUICC** (IPAe), which will be a huge advantage for OEMs. Without this integration, they would need to install the IPA on the device in order to communicate with the eIM and/or SM-DP+, which could deter some OEMs from using eSIM technology.

Once everything is in place to easily deploy eSIM technology to a wide variety of IoT devices, what will really matter is the **scalability and resilience** of the Remote SIM Provisioning solution to download billions of eSIM profiles and manage their lifecycle, securely and efficiently. This is why we are hosting all our eSIM solutions in Microsoft Azure Public Cloud.

---

[1] SGP.01, SGP.02, and SGP.11
[2] SGP.21, SGP.22, and SGP.23
[3] NB-IoT and LTE-M
[4] Source: Kaleido Intelligence
