www.pipelinepub.com
Volume 18, Issue 9

Fueling Momentum with Secure IoT Connectivity

By: Yoram Zerahia

The Internet of Things (IoT) has received a lot of hype since 2009, when the number of 'things' connected to the Internet surpassed the number of people online worldwide. IoT utilizes processors, modems, software, and other technologies to connect devices to the Internet to gain access to the useful data they can provide. Connected products can be updated with new features and be remotely monitored for performance. In 2010, Ericsson's former President and CEO Hans Vestberg predicted cellular IoT to reach 50 billion connections in 2020. Yet, according to IoT Analytics market update "State of IoT 2021" from Sept. 22, 2021, IoT only reached 11.3 billion connections in 2020.

The IoT connectivity challenge

For IoT to succeed, the connectivity of the device to the Internet is crucial—no connectivity, no data. IoT requires reliable, secure, and continuous connection for devices, wherever they are located. A secure IoT connectivity solution must be scalable, simple to configure, set up, deploy, and manage. As IoT devices have a lifespan ranging from five to 10 years, some even longer, assurance of continuous connectivity throughout the lifetime of the device is required.

Enterprises often want to support more than one IoT application and each application may have different connectivity requirements or different attributes. For example, static devices located indoors may work better on a fixed or Wi-Fi network, but mobile devices will be better supported on a cellular network.

Cellular connectivity, however, has its challenges. Cellular coverage is not uniform across all regions, usually due to lack of necessary infrastructure. A carrier may provide great coverage in one area and spotty or absent coverage in another. Because IoT devices can be deployed in different areas, including remote locations and temporary work sites, providing good coverage in all areas is crucial. Additionally, IoT devices may also be stationary or constantly moving, adding to the challenge.

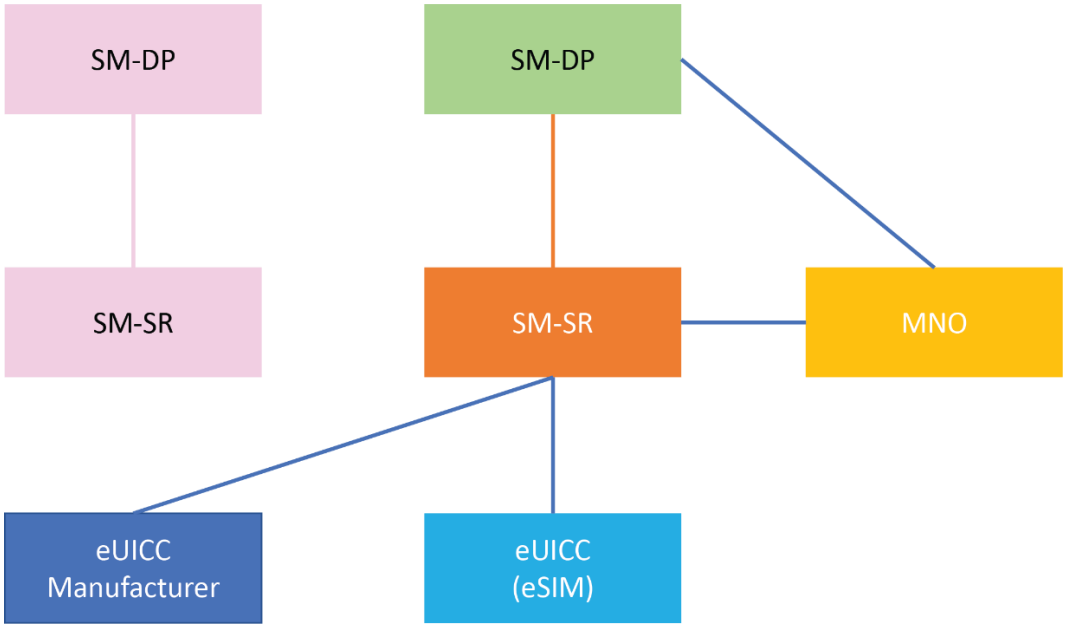

Figure 1 GSMA M2M architecture

The SIM card challenge

Cellular connectivity requires the use of SIM cards. Early adopters of IoT used traditional SIM cards. However, traditional SIM cards are not designed to meet the challenges of IoT connectivity. Carrier provisioning is done at the manufacturing level, hosts only one profile and is not reprogrammable. This is why you need a new SIM when switching cellular providers. This is not ideal for IoT deployments, especially global ones. Once the SIM has been implemented and the device deployed, it is impractical to change SIM cards when you want to change wireless carriers for thousands and even millions of devices. Doing so requires a site visit, and the card may be physically difficult to access. In addition, to comply with the global trend to enforce regulatory requirements on communication services and data management, global enterprises need localized deployments with local wireless carriers. This requires warehousing, managing, and deploying several wireless-carrier-specificproduct SKUs, which drives up production and logistics costs. An additional caveat of using traditional SIM cards for IoT is the carrier lock-in, as the SIM card hosts only a specific carrier profile and is limited to the local carrier or their roaming mobile network operator (MNO) partners for cellular connectivity. A local carrier's service is limited to the geographical range of their home network. Thus, an IoT solution vendor with global offerings is required to manage its devices in numerous areas with different wireless carriers. By itself, this is a real challenge. Although carriers offering roaming-based services can provide comprehensive coverage globally, this usually comes with high latency issues and less competitive rates.

With the emergence of global full mobile virtual network operators (MVNO), the challenges of working with a local or roaming carrier were resolved. A full MVNO manages and maintains its own core network elements and infrastructure, providing its IoT customers with complete control over all network services and offerings. The MVNO usually has service agreements with MNOs for use of their radio access network and therefore can easily provide access to several local networks to ensure continuous connectivity for devices wherever they are located. The MVNO can also have global data centers to reduce latency.

Transitioning from SIM to eSIM

The GSMA M2M architecture can be seen in Figure 1 on the previous page. It uses an SM-DP (Subscription Manager - Data Preparation) and SM-SR (Subscription Manager - Secure Routing) to provision and remotely manage carrier profiles.The SM-DP acts on behalf of the MNO. It creates and stores the MNO profile for the eSIM based on information received from the MNO and eSIM manufacturer. It is also responsible for installing the profile on the eSIM through the SM-SR. The SM-DP also manages profile enabling and deletion requests from the eSIM through the SM-SR.

The SM-SR is responsible for establishing a secure and authenticated transport channel to the eSIM to manage the eUICC platform. Only one SM-SR can be associated with an eSIM at any point in time. It loads, enables, disables, and deletes profiles on the eSIM according to the MNO's policy rules

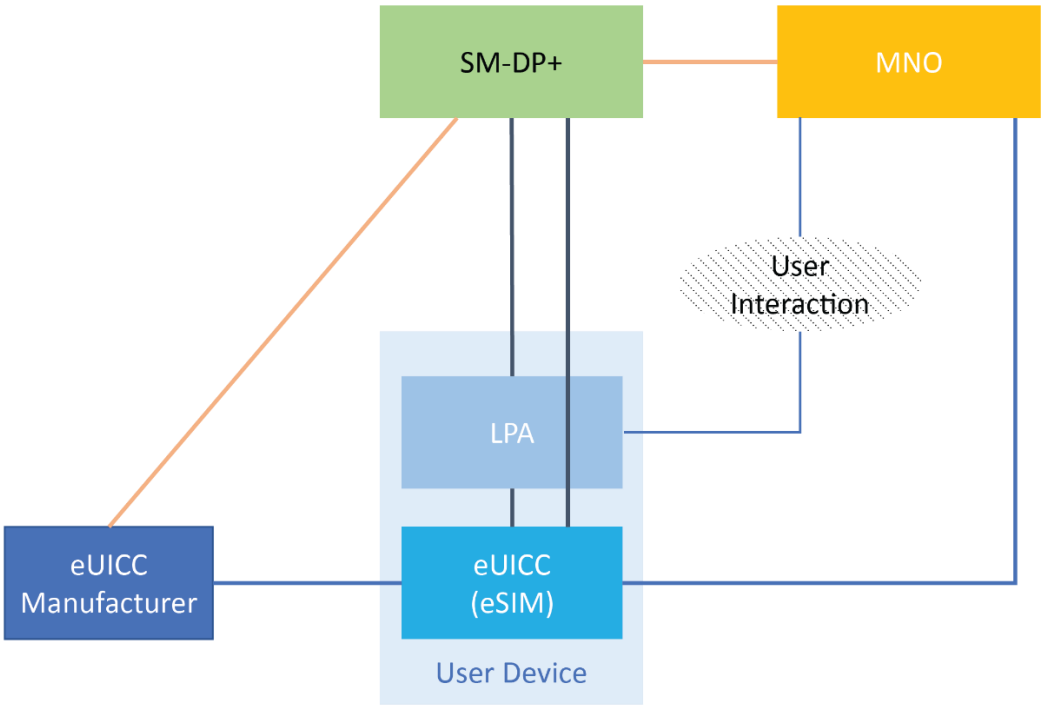

Figure 2: Consumer eSIM Standard architecture

The SM-SR and SM-DP are usually run by the wireless carriers. This means that the customer needs to collaborate with wireless carriers to integrate connectivity into their product. When the customer decides to onboard an additional wireless carrier, all parties must agree, and the new

carrier's infrastructure needs to be integrated with the eSIM platform. This can imply either connecting the serving SM-SR to the second carrier's SM-DP or performing an SM-SR swap to the second carrier's SM-SR and SM-DP. The current service carrier needs to initiate the migration to the next carrier. This can take months and costs tens of thousands of dollars. In addition, the customer doesn't have control over the management of profiles or the flexibility to switch between multiple profiles.

A simpler and more cost-effective way to overcome the M2M eSIM Standard limitations is by adopting the successful Consumer eSIM Standard into the M2M world. The Consumer eSIM Standard utilizes SM-DP+ (Subscription Manager Data Preparation +) for profile downloads (Figure 2, on pervious page). It carries out the functions ofboth the SM-DP and the SM-SR used for the M2M solution. There is no technical integration required with the carrier. The device or the eSIM contains an LPA (Local Profile Assistant) which allows for the download of encrypted profiles to the eSIM and their management.

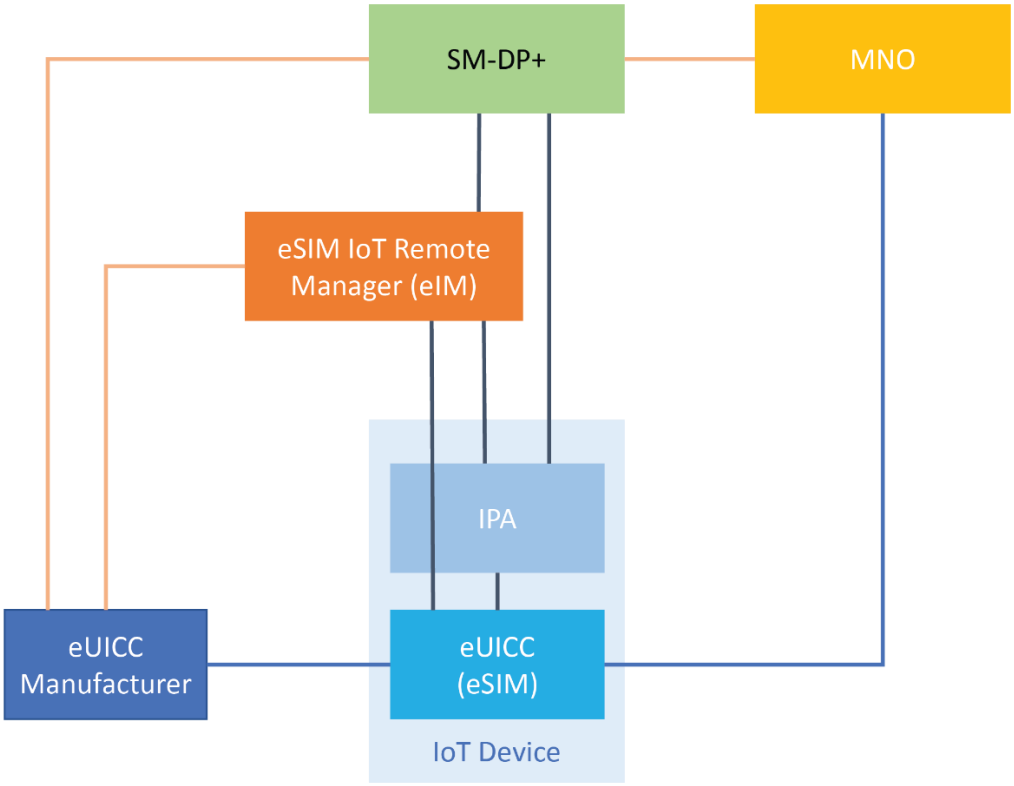

Figure 3: WG7 Adaptation

This kind of approach has been examined by the standards bodies with the outcome of the establishment of GSMA Work Group 7 (WG7) for remote provisioning of "eUICCs in Network Constrained and/or User Interface (UI) Constrained IoT Devices" (SGP.31).

In short, WG7 is adapting the current Consumer eSIM Standard (SGP.22) to provide the capability to manage an IoT device remotely (Figure 3, above). They added an eSIM IoT Remote Manager component to the architecture that interacts with the device and allows for remote management. The LPA is replaced with an IPA (IoT Profile Assistant) that allows the eSIM to be provisioned by the SM-DP+. This greatly reduces the time to market for IoT deployments and

provides companies with the same flexibility and control that consumers have. However, this new approach will only be available in a few years because it takes time for standards to be formalized and approved for use.

In the meantime, the market is offering several solutions based on pre-standard technology. Methods are being developed to remotely control and configure the LPA via a dedicated management portal, replacing the user interaction required in the current Consumer Standard. This allows enterprises to order consumer eSIM subscriptions in bulk from any cellular carrier with a SM-DP+ server. They can then upload the activation codes into a portal to provision the profiles remotely to the eSIM. Rules for managing the profiles can be configured, such as which carrier profile to use in each deployment location and defining a fallback profile in the event of connectivity loss with the default profile. The eSIM communicates with the carrier's SM-DP+ server to download and activate the subscription. The IoT connectivity will follow the defined rules, adhering to regulatory compliance requirements if present, and automatically swapping between wireless carriers as needed. This makes IoT connectivity simple and scalable.

Now, with the development of new eSIM technology, IoT's true potential can be realized. The conditions are available for IoT deployments to enable great cellular connectivity in every location, which can be managed and changed based on the business need. This ensures continuous connectivity throughout the lifetime of the device and is more tolerant to ecosystem unpredictability.