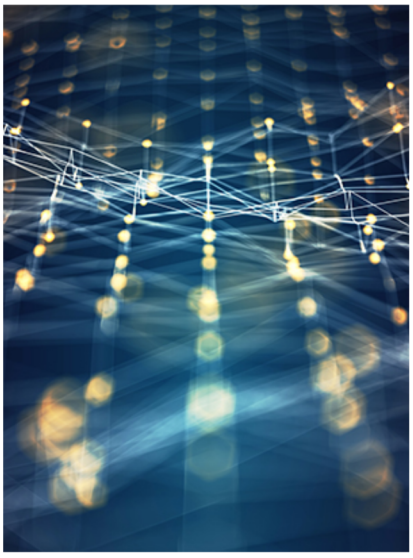

www.pipelinepub.com
Volume 20, Issue 9

# IoT, 5G, and Escaping the eSIM Crunch

By: Chris Jahr



The expansion of 5G networks is expected to enable an explosion of new IoT devices that require mobile network authentication. Currently, cellular network authentication happens via SIM technology, which itself is undergoing a transformation from physical SIM cards to digital eSIMs.

Regardless of the form factor, however, the reality is that the SIM industry is not set up to scale to meet the explosion in volumes expected, especially the needs of an ever-growing number of companies in the IoT market that will require smaller quantities of eSIMs.

Let's explore the genesis of this impending eSIM crunch and what alternatives might exist for enterprises, IoT platform providers, and IoT device makers.

## IoT Market Fragmentation Hinders Adoption

For years now, IoT pervasiveness has been heralded as "just around the corner." Somehow, however, that corner seems to stay at the same distance ahead. One reason is that today's IoT market fragments in multiple directions, with a major dividing line being the ways in which IoT devices communicate.

Today many connected devices communicate over Ethernet, Wi-Fi, and other local-area networks including Zigbee, Z-Wave, Bluetooth, Thread, and Matter. IoT devices using these communication avenues include smart light switches, HVAC systems, security systems, watering systems, and various smart home products.

The most common network, Wi-Fi, poses several limitations, especially for industrial use. To overcome these limitations, more companies are investing in 5G cellular private networks and deploying remote connected devices such as water and gas meters and street lights, as well as connected scooters, eBikes, and cars. As demand for private cellular networks and remote IoT devices grows, so does the need for 5G connectivity, which in turn pushes demand for SIMs.

From a carrier's perspective, IoT devices' cellular communications volume and transmission

© Pipeline Publishing, L.L.C. All Rights Reserved.

Not for reproduction or distribution. © Pipeline Publishing, L.L.C. All Rights Reserved.

frequencies fall along a spectrum. At one end is streaming data, such as with always-on security applications. At the other end are devices that send little snippets of data at programmed intervals, such as smart gas meters that report consumption hourly or daily.

The spectrum ranges trigger significant implications for carriers' calculations of ARPU (average revenue per user). For example, a remote video security camera using a 5G modem requires a high-volume data plan, which might provide a carrier with $25 *plus* per month in subscription fees. The IoT device transmitting occasional data snippets might generate as little as 50 cents a month in revenues, which is too little to merit much attention from the carriers. Carriers' business models require that they focus primarily on the major cellular users — the big spenders — rather than the more modest users.

# Lack of eSIM Automation Creates Bottlenecks

A similar attention differential is at work in the eSIM market.

First, a bit of background on the Subscriber Identity Module (SIM) market. A SIM chip — technically a UICC, or Universal Integrated Circuit Card — is a specialized security device with a microprocessor, memory and I/O functionality. Together with the carrier-specific information stored on it, the SIM contains a unique identifier linked to a specific user account, allowing the device to securely access the cellular network. The purpose of the SIM is to authenticate a device to the network to ensure that cellular resources consumed by the device are associated with an actual subscriber that is paying for them.

SIMs have been part of mobile telephony since the deployment of the first GSM mobile networks, starting in 1991. The electronic SIM, or eSIM, is a digital version of the physical SIM card; the UICC is now embedded in the device itself. Any IoT device that connects to a cellular network needs SIM technology. And that's where problems begin.

Since the early days of physical SIM cards, the expertise and processes for designing, developing and deploying SIMs — including receiving mobile network operators' secure authentication keys, International Mobile Subscriber Identities (IMSIs), and other files to create profiles and generate individual, secure SIM contents — have rested with a small handful of SIM vendors. These SIM vendors, located in Europe, Asia or Brazil, also control the generation and deployment of digital eSIMs. (There are also a number of SIM vendors in China and India, but they mostly serve their local markets, operating much as the European vendors do.)

The GSMA, a trade association that represents the interests of the global wireless carrier community, estimates that the number of companies creating eSIMs is limited to fewer than 20 in all, with three of them having a combined market share in excess of 70 percent. Accompanying the limited number of SIM vendors is a serious shortage of SIM expertise. Creating SIM profiles, especially, is a highly complex endeavor requiring very specialized expertise. It's estimated that worldwide, only about 2,000 or 2,500 individuals can be considered SIM experts. In North America, as few as 150 people possess the expertise needed to create profiles and generate SIMs.

Although SIM vendors are working to develop more scalable systems, it seems that the legacy companies use the same processes for generating eSIMs, and the profiles that lie at the heart of secure network authentication, as they use for physical SIM cards. It's largely manual, cumbersome and time-consuming, which is the antithesis of what creating a digital product should entail.

In many ways, SIM generation today parallels the early days of wired communications with the telegraph. Text had to be handed or dictated to specially trained operators who keyed the codes into the telegraph machine for transmission to another machine, where the codes were transcribed into readable text

Similarly, carriers today have to submit requirements for profile development and transmit files with IMSIs and other authentication information, in various formats, to the SIM vendors. Using these, the vendors generate SIM cards or eSIMs. Because of the way the SIM vendors work with their customers, real automation is a challenge.

*© Pipeline Publishing, L.L.C. All Rights Reserved.*

Not for reproduction or distribution. © Pipeline Publishing, L.L.C. All Rights Reserved.

Their business model and process requirements leave the SIM vendors with limited ability to serve customers that have lower-volume needs. Many IoT companies require only 50 or 100 or 1,000 endpoints. They can't use generic SIMs, because IoT makers need to incorporate functionality that differentiates their products from those of their competitors.

Such differentiation highlights a third issue: the need for mass customization. The SIM profiles of cellular IoT devices must reflect each company's or product line's individual capabilities, both to authenticate the devices correctly to the right network and to ensure that the carrier or network operator is being billed accordingly. Even the most popular cellular IoT applications — deploying 100,000 smart streetlights, for example — can't come close to the eSIM volume requirements of Tier 1 and other large carriers. As a result, it might take many months for cellular IoT devices to gain access to the eSIMs they need, as they wait in line for the SIM vendors to fulfill their orders. Then, when the eSIMs finally arrive months later, IoT companies probably also have to pay a premium for them.

Such delays are especially concerning in light of the anticipated scale required for the deployment of new highly differentiated 5G and cellular IoT devices; it's estimated that global **cellular IoT connections will exceed 6 billion** by 2030. If nothing in the SIM world changes, these large-scale but highly individualized deployments could soon severely tax the system and create bottlenecks in IoT companies' ability to get their products to market.

# Escaping the eSIM Crunch

The solution to the eSIM bottleneck for cellular IoT devices can be found by asking some pointed questions of the status quo. Why is the generation of eSIMs, a digital product, still using manual processes and flat-file transfers? Why is all this not automated? Given that eSIMs are digital entities, why should anyone be paying more than five to ten cents to obtain an eSIM? Why are eSIMs not available essentially on demand, created at the same time a device is deployed?

Most discussions of eSIMs tend to focus on smartphone subscriptions or, more specifically, smartphone network connections for travelers. Currently, the issues around eSIMs might be most obvious in this arena. But the underlying problems with the current eSIM generation process apply equally to the IoT market. The growth and success of IoT, which has already had so many fits and starts, is destined to be further constrained by the inability to get eSIMs when they're needed. If this issue is not rapidly addressed, the full promise of private 5G cannot be realized.

Another less-discussed problem is that producing eSIMs, like physical SIM cards, entails multiple steps, in multiple geographic locations, from order to delivery. The major SIM vendors have headquarters in Europe, and parts of their SIM generation process happen in other parts of the world, largely in low-labor-cost areas such as India, Asia, Brazil, and Mexico. As a result, network operators' credentials and security keys must traverse several national borders before the eSIMs are delivered. So unless a company is located in one of the countries where the eSIMs are generated, it is fair to say that 100 percent of their credentials will be generated abroad. This lack of sovereignty over SIMs, which are cybersecurity tokens, can be a significant issue for government, military, and some industrial IoT projects, in particular.

The solution to all the current problems with eSIMs lies in completely rethinking the entire SIM creation process, automating it and putting eSIM development, management, and orchestration capabilities into the hands of every network operator, enterprise or IoT platform provider that needs them, regardless of the size of the network, its volume or its business model.

In the IoT realm, I foresee a near-term future where an energy company can deploy a few hundred utility meters, a rural network operator can support local residents' smart home cellular connections, and Tier 1 carriers can build profitable IoT businesses, all equipped with eSIMs that they've generated themselves, on demand, for a few pennies each.

Not for reproduction or distribution. © Pipeline Publishing, L.L.C. All Rights Reserved.

*© Pipeline Publishing, L.L.C. All Rights Reserved.*