IOT INSIGHTS REPORT:

Connectivity and Carrier Management SME Interview

*with **Steven Baker**, Vice President of Product Management*

In his role as Vice President of Product Marketing, Steven leads product management, delivering KORE's licensed and unlicensed IoT connectivity service offerings, platform and data services, and vertical solution enablement. Over his 30-year telecommunications career, Steven has specialized in wireless and optical network technologies and has filled individual and leadership roles spanning product management and marketing, sales, business development, and software engineering. Steven has authored multiple cellular and optical network patents during his career and holds a BA in Computer Sciences from the University of Texas.

Q1: With hundreds of carrier, network, and equipment options, how can businesses ensure they are pairing the right technologies for the optimal IoT solution?

STEVEN:

The challenge in IoT is that there is not just one solution for every single situation. The technologies, capabilities, and requirements are so diverse, you really need to mix and match connectivity options and devices to come up with an effective solution, or you are going to end up with one problem or another down the road.

Choosing the right technology components starts at the beginning of the project, developing a strategy to avoid not just technology mismatches, but also business requirement mismatches. One example is where an organization deploys a standard LTE device, which is battery-operated. They soon discover that the application's communication requirements and the usage parameters cause the battery to die after two hours. This is a both technology failure and a business failure.

Organizations also sometimes fail to plan for longevity. Using the example of technology sunsetting; unless you can switch a particular device to a new carrier over-the-air while it is in the field, you will need to go out and physically roll a truck and replace it. It can be very costly. It is important to know when a connectivity option will sunset, and plan ahead.

Some organizations also overlook the fact that IoT device certifications can cost tens of thousands of dollars, only to go through the process and fail, and pay again. Working with an experienced IoT partner can help as they can guide you through the process and get it right the first time.

Q2: **Which factors should organizations consider when selecting an IoT network connectivity provider? Can you briefly contrast the advantages/disadvantages of sourcing directly with carriers vs. an independent IoT provider?**

STEVEN:

Today, almost all providers offer domestic service in their home countries. These providers also typically offer roaming capabilities in other regions, which are transitory and higher cost. This means you can, for instance select a US provider and roam in Europe, but only for a certain amount of time – often up to three months and usually at a higher price than providers in Europe. So selecting one specific service as a global deployment can be challenging, since few services support long-term deployment in the US, Europe, Asia Pacific, and Latin America in a single offering that remains operational forever. Often a better option is to select one provider in a region and augment with other in-country providers in other regions.

There are several disadvantages to sourcing connectivity directly from carriers. A single carrier locks you into their certifications, their roaming coverage, and their price points. You are also restricted to their UI, their APIs, and their platform to manage the service. When adding a secondary carrier, you have another contract, UI, APIs, and platform. Now you have two systems to manage, and two separate support services. When you have an issue, you have to identify which carrier supports the troubled device, and call the correct provider. So that's a big disadvantage to working with carriers, as opposed to an independent provider that handles relationships with multiple carriers on your behalf.

The ideal solution is to work with an independent partner that can support multiple carriers in all regions, or a single Subscriber Identity Module (SIM) that can operate and switch to be a local carrier in all regions. When working with independent providers, you have a single contract and single point of contact for your service. From a technical perspective, you have one commercial setup and one unified platform to manage everything.

Q3: **What are the most significant challenges associated with managing multiple wireless IoT connectivity providers, technologies, and platforms?**

STEVEN:

The most significant challenges are around cost, SIMs, and coverage areas associated with each connectivity option.

Long Term Evolution (LTE) is the most commonly deployed connectivity technology today for IoT. LTE provides greater network capacity and speed than legacy connectivity options. Within LTE, there are many families of LTE capabilities, each with different speeds, costs, and requirements. More specifically, the low-powered versions - Category 1 LTE (Cat 1), Category M LTE (Cat M) - and the up-and-coming narrow band IoT LTE (NB-IoT) are used most often. These LTE capabilities are built for low speed and lower cost.

These are different from the LTE options used in smartphones, which offer very high bandwidth at high costs. Many consumers pay high fees in excess of $100 per month. However, Cat 1 and Cat M were built for low speeds, ideal for many IoT devices that require short data transmissions, with connectivity costs from $1 to $5 per month. Examples of short, low-cost data transmissions include premises monitors, which only send data when a door is opened or closed.

SIMs are another challenge when you start looking across the carriers. Some carriers with Cat 1 and Cat M will use a unique SIM for that capability. So with one carrier, you may have to buy a new SIM and that SIM can only be used for that particular network technology.

From a technology standpoint, NB-IoT is the newest low speed/low cost LTE option. While it is very well marketed, it is not available everywhere today, so the geographic coverage availability will vary greatly across individual connectivity providers.

Sunsetting, or discontinuing certain connectivity options, is another challenge with carriers. AT&T recently sunset its 2G offering, and now we are coming up to the 3G sunset, so it is a moving target on these technologies. When choosing IoT connectivity options, organizations need to consider the fact that technologies are being discontinued and evolving from older options to the newer technologies. As I mentioned earlier, a single, independent provider can help you navigate these evolving technologies to make the best decisions for your business.

Q4: Could you provide an example of how business and regional requirements affect connectivity selections?

STEVEN:

Sure. Let's take the fleet management industry as an example. That industry tends to use a lot of off-the-shelf products, but many of these pre-packaged fleet management solutions are not designed for long-haul operations, they are optimized for regional requirements. Since some long-haul operations require multi-regional IoT deployments, particular device connectivity combinations for every network carrier in each region will need to be established.

So, for companies managing a fleet of vehicles – or any businesses that need to operate IoT devices across multiple regions – selecting connectivity options becomes more complex. For example, when designing for tracking capabilities in both Brazil and Mexico you need to think about connectivity options, roaming costs, certifications, and other country-specific and carrier-specific requirements.

Part of this pertains to managing SIM cards, used inside devices by cellular carriers to identify and authenticate subscribers on their networks. Brazil, for example, does not allow roaming, so you are immediately going to need more than one SIM; you will need one for Brazil and more for capabilities in other countries, such as a SIM for Mexico. So immediately, you will have decided that you need multiple types of SIMs, with different certification requirements and different regional requirements for the frequency bands they support within those areas.

Q5: Of the many potential ways to connect IoT devices, what would you say is the optimal network technology choice?

STEVEN:

There is not an optimal, one-size-fits-all network technology choice that meets every IoT connectivity need. That is one of the reasons why IoT deployments can be difficult. Each organization and vertical market have different requirements, and those requirements drive each technology choice, both for connectivity and for the device itself. Then the business-specific device selection, coverage type, and location or country may guide the appropriate connectivity choice, which could be cellular, cellular-satellite, satellite, or unlicensed.

The required connectivity technology may also dictate which carrier you will need to use. For example, if I have a business case that dictates the need for U.S. coverage with "Cat 1" (LTE Category 1 connectivity,) I'm going to need a device that is certified on the provider I select for that service. So the business need and the connectivity type are interrelated, and the resulting device options are based on those factors.

Q6: What are some of the complexities of device provisioning?

STEVEN:

Every carrier has a unique way of handling provisioning, and each introduces different challenges and complexities. Through the provisioning process, each device is authenticated as a trusted entity on the network and it is configured to send its data to the correct destination.

Some carriers require different parameters and settings for individual devices, rather than having one uniform provisioning process across all carriers. This adds additional complexity to IoT deployments, making it more difficult for businesses to maintain and scale IoT deployments over time when dealing with several carriers.

However, provisioning becomes much easier when partnering with an independent IoT services provider. Organizations can follow the same activation process for their IoT devices, regardless of which carrier is used. This normalization benefits businesses in a number of ways.

Independent providers also shield their partners from carrier protocol changes. This is important when you consider that carriers periodically upgrade and change their platforms. This meant that their customers had to re-configure all application programming interfaces (APIs), interactions, and automated processes to become compatible with the new platforms. This is not a trivial operation, as it often takes months in IT staff labor to integrate with the new platform, perform quality assurance testing, and upgrade without disrupting existing services. Multiply this by two or three providers and it becomes even more challenging and expensive. When working with independent providers, businesses do not have to change their models just because the carriers change theirs.

Q7: How does security factor in when selecting IoT connectivity technologies and providers?

STEVEN:

Security is a huge element both from a key management and a transport perspective for providers. In the past, IoT devices were not particularly smart, but they're getting smarter. They are beginning to have the ability to support web services right on the device, for access and diagnostics, and organizations are putting these devices on public IP addresses, like you would normally do with a router. However, a lot of people do not change the administration user name or password, making it too easy to hack.

So the government is working to mandate what we call "key management" for their IoT devices. In California and also in the U.S. Senate, legislation has been introduced requiring higher security on IoT devices used by the government.

Key management will help provide end-to-end security and protect payloads as they move up through the network. With cellular networks, everything is encrypted. The data is always encrypted, but the second it hits the Internet, then you require that payload to be encrypted. So we are seeing a lot more drive to encrypt payloads from the device all the way to the servers and through firewalls in order to make sure it is locked down.

Q8: What impact will multi-IMSI and eSIM capabilities have on the IoT connectivity landscape?

STEVEN:

With multi-ISMI and eSIM, a three-month limit on roaming will no longer be an issue. You can literally have a true global SIM that can be installed and switch to a local domestic carrier, with local domestic pricing, which is less costly than roaming.

It begins to expand the flexibility of IoT, with fewer SKUs, more economical deployment, and more of a cooperative environment than a competitive environment across providers.

I have been in the industry for about ten years, and I remember moving to multi IMSIs about eight years ago. It is very similar to eSIM. They both operate on the concept that you can put a SIM in a particular place forever, and switch the carrier in place through SIM-based logic or over-the-air as needed when connectivity technologies change.

For example, if a device is in a country that is about to sunset a 3G technology, eSIM allows the organization to switch it to another carrier who is extending the sunset for several more years. They can now extend the longevity of that device by a number of years just by switching the carrier on the SIM itself.

Q9: You've described the advantages of working with an experienced IoT provider. What should organizations look for in an IoT partner?

STEVEN:

Think about their expertise in IoT applications and their ability to understand your end business goals, as well as the business logic required to solve problems. From a technical standpoint, it is important that you select a partner that can understand connectivity technologies, and perhaps as importantly, has deep relationships with the carriers. These relationships will be critical in their ability to learn about network changes in advance, and to shield customers from the effects of those changes. It also helps to have a provider that understands data technologies and can provide additional services, such as life-cycle management, on an à-la-carte basis.

When you look behind the curtains and see what really makes up an IoT project, you realize the need for a partner that can navigate the many technologies involved. This is what makes IoT difficult to bring to market, and why working with a trusted, independent provider is so important.

It is also important to select an agnostic partner, with no bias toward certain connectivity or hardware options. An independent, agnostic partner will examine your business goals and recommend the optimal solutions. In some cases, single providers - such as hardware manufacturers that also sell connectivity – are incented to recommend their own solutions. Independent providers, instead, look across a broad spectrum and assemble the solutions that best fit your needs. It can be a similar situation working with individual wireless carriers, who are often focused on consumer accounts.

Reach out to KORE today to learn how we can simplify the complexity of IoT for your business.

korewireless.com