IoT at the Edge

Succeed with IoT

5G Cellular Growth
with Secure, Intelligent IoT Edge

Kigen

beecham research

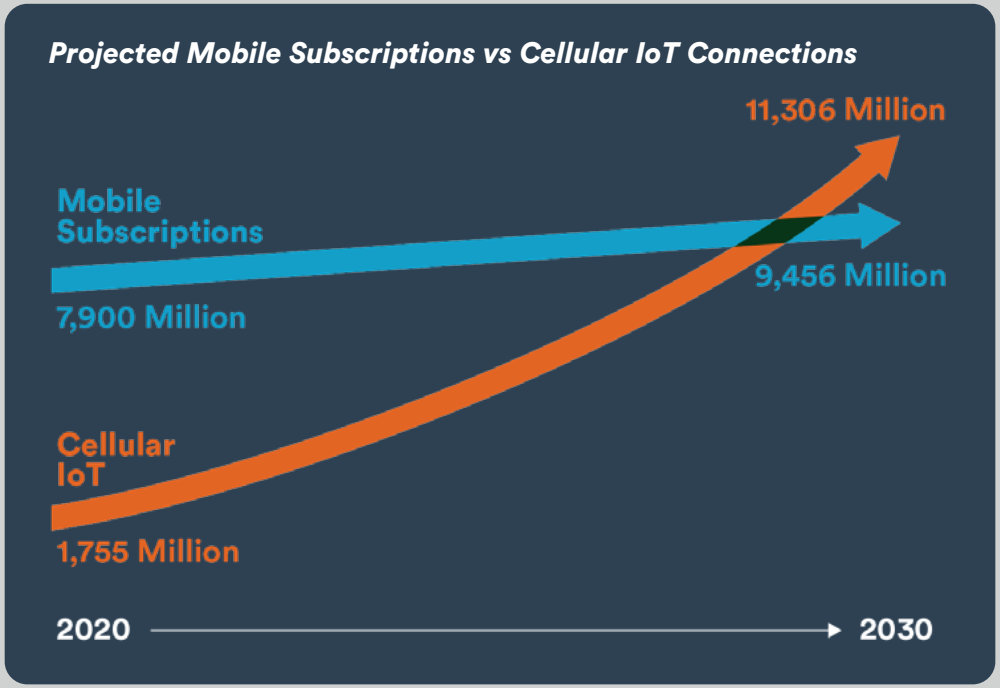
Shaping the IoT future

The coming boom in connected IoT devices

As detailed in Beecham Research's Report IoT at the Edge: Enabling the Real Time Enterprise available to download free at this link and sponsored by Kigen, IoT is now rapidly evolving from its roots in monitoring and reporting in the cloud to extensive processing at the network edge, coupled with 'light' connectivity to the cloud. This edge to cloud model is a particular feature of 5G and will dramatically open the opportunities for connected IoT devices, enabling a 'long tail' of a massive variety of devices and applications not previously feasible due to their low volumes.

As a result, the growth path for cellular IoT connectivity is now expected to average more than 20% per annum for the rest of this decade. This is compared with less than 2% per annum growth expected for mobile handset subscriptions over the same period. This is because, although 5G is bringing many valuable new services to the mobile handset and other related markets, it is doing far more for IoT. For the mobile handset market, it is more a story of upgrading connectivity of existing subscriptions to higher bandwidth services. On the other hand for 5G for IoT, is about continued rapid growth of new connections, especially for the growing variety of low power, low data rate applications, many of which are enabled by edge processing. More processing at the edge means less data to transfer to the cloud, thereby reducing connectivity costs and overall total cost of ownership.

What does that mean in terms of overall numbers? By the time we get to 2030, there are expected to be more cellular IoT devices connected to mobile networks than mobile handsets. This represents a huge opportunity for device OEMs.



What sort of connected devices will they be? Literally anything that can gain from being connected. On the one hand, more cars and trucks on the road will be connected than not, especially with the anticipated huge growth in electric vehicles. All EVs and EV charging points will be connected. On the other, many new wearable devices with low data rate requirements will come to market as value-add propositions – from wearable healthcare devices like pacemakers, to consumer devices like fitness monitors, smart watches and smart glasses. Many larger assets in the domestic market that can benefit from being monitored, including household appliances like fridges and washing machines – on which more below. In the enterprise market, a huge range of new devices are in development. For example, many large assets can benefit from being monitored. At the smaller end, remote sensors for smart agriculture, smart energy and public safety will be used to enable a wide range of new applications.

It has been said many times before that we are limited only by our imagination in thinking of what can usefully be connected. A boom in connected IoT devices is imminent– especially for small remote devices that require low data rates and long battery life. The key issue to resolve is how to provide the connectivity cost-effectively and securely.

Addressing the connectivity challenge

Picking up on the example of connected fridges and washing machines, this has been attempted before but with a focus on services that consumers turned out to be reluctant to pay for. On the other hand, product manufacturers can gain enormous amounts of valuable data from their products in the field to assist in improving product quality, performance and pinpointing areas for further product development. The problem with that has always been how to cater for the connectivity required in a cost effective way. Connecting to household Wi-Fi is a nonstarter – many domestic households do not have Wi-Fi and those that do have little incentive to connect a device to their system if it does not benefit them directly.

A far better answer is use of cellular, which offers standalone connectivity that can link directly with the manufacturer's data centre. Previous generations of cellular have been too expensive and power hungry to warrant their widespread use in such applications. New technologies like LPWA (Low Power Wide Area) have been specifically designed for low data rate, low power requirements with battery life when not connected to a power source of up to 10 years.

Focus on smart data

Edge processing can then reduce the data required to be sent to the cloud – for example sending relevant data only. This may increase power use and cost at the edge, while reducing the connectivity cost. A balance needs to be struck depending on the application itself.

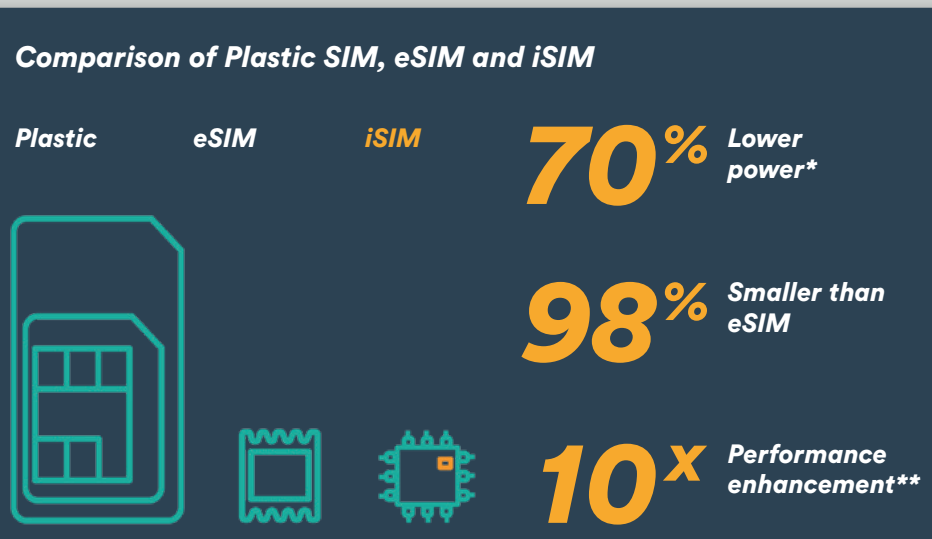
A key issue is then security for such devices. As more devices with more intelligence are connected, they become a more likely target for security breaches. The SIM (Subscriber Identity Module) offers a high level of network security. However, the traditional SIM card has been recognised as poorly designed for many IoT applications. Logistically complex to supply the right SIM in the right place at the right time, it is also prone to physical abuse, adds cost to the design and impacts on the overall device form factor. A far preferable approach is the eSIM (embedded SIM) that embeds the SIM directly into the device's circuit board. eSIM was designed specifically for IoT applications to overcome the shortcomings of the SIM card. Even better is the iSIM (integrated SIM), which provides all the advantages of the eSIM whilst also eliminating many of its disadvantages, particularly for small form factor devices.

Integrated security at the edge

The benefits of iSIM are shown in the figure opposite, sourced from Kigen, which compares the traditional plastic SIM card, eSIM and iSIM.

As is evident, iSIM technology is particularly well-suited for resource constrained devices where there is limited power and where there is a need for a small overall device form factor. The eSIM is normally built on a discrete secure microcontroller, but iSIMs are embedded in the device's main SoC (System on Chip), thereby reducing the bill of materials, optimising the supply chain and shrinking the physical size. The advantages of this approach compared with eSIM are numerous. It reduces the component count on the device circuit board, so the board can be smaller. It reduces the power consumption, as the power for the iSIM element in the secure enclave is now derived from the SoC itself. It also improves the performance, since all the signals to and from the iSIM element are now also directly on the SoC bus rather than through an interface to that bus. Security is also enhanced through the operation of the secure enclave itself.

Comparison of Plastic SIM, eSIM and iSIM



* Compared to plastic Mini SIM
** Based on Kigen iSIM, using Kigen-specific code, CPU, SE and iSIM OS
Source: Kigen

Winning in the data economy

Leveraging a hardware secure element, or 'Root of Trust', to establish end-to-end, chip-to-cloud security for IoT products and services is a key recommendation of the GSMA IoT Security Guidelines. This requires both the provisioning and use of security credentials that are inside a secure enclave within the device. The SIM is recommended as best suited to function as the hardware Root of Trust in an IoT device as it has advanced security and cryptographic features and is a fully standardised secure element, enabling interoperability across different vendors and consistent use by IoT device makers.

As a result, Kigen has added IoT SAFE (IoT SIM Applet For Secure End-2-End Communication). This is a GSMA initiative that declares the SIM to be the most secure location within a device from which to process and secure the data exchange from chip to cloud. It enables IoT device manufacturers and IoT service providers to leverage the SIM as a robust, scalable and standardised hardware Root of Trust to protect IoT data communications. IoT SAFE provides a common mechanism to secure IoT data communications using a highly trusted SIM, rather than using proprietary and potentially less trusted hardware secure elements implemented elsewhere within the device.

To this, Kigen has added advanced features that extend the benefits and reach of this initiative, making it more accessible to all stakeholders in the IoT ecosystems. OPEN IoT SAFE is the term the company employs to identify this development. Baking the iSIM within a trusted, tamper-resistant secure enclave at the heart of the device's SoC is seen as the ultimate foundation for a secure IoT SAFE device.

Enabling a secure ecosystem

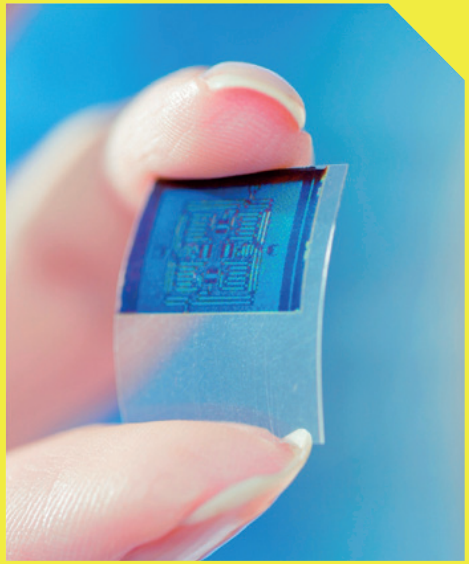
These developments enable highly portable applications that require high data security. For example, personal healthcare devices such as inhalers – to monitor if they are being used correctly. Also, insulin patches and pens, patches for monitoring allergies, diabetes and a range of other conditions. These and many other highly portable devices with wide area connectivity are anticipated, freeing up those being monitored to lead an unrestricted lifestyle.

A wide range of solutions across many different sectors, including Buildings, Energy, Consumer/Home, Healthcare, Industrial, Transport, Retail and Public Safety are also predicted.

The low cost of such devices makes it economically feasible to enable many new applications that were too expensive before, even when using an eSIM solution. Figure opposite shows typical circuitry for a low cost sensor using this technology that can be printed locally. This could for example be applied to bandages in a healthcare setting where constant monitoring is required, either for tracking of an individual patient or for monitoring vital signs, or even a physical condition such as warning of a fall. A wide range of such wearable applications become feasible.

Another area is Smart City, where a very large number of robust sensors are required to monitor environmental and other situations, including for example transport infrastructure.

While these are all of great value, traditionally such monitoring activities have been been closed systems and limited to sending their data to single destinations. Now this too can change as such data can be shared securely within an ecosystem of partners. Better remote care of patients can be achieved by exchanging such medical information, with faster coordination of resources to cater for individual needs. At a different level, it can also be used for example to provide oversight into health trends for medical research purposes.



Once data can be securely shared within an ecosystem in this way, it opens opportunities for new added value services that were previously not feasible. As a result, these technologies can provide better insights and – ultimately – gain competitive advantage. This presents an attractive market opportunity for enterprises to capitalise on serving customer centric services in a wide range of sectors.

eSIM futureproofs metering solutions to drive customer value-add services.

Adopting eSIM and iSIM brings robust security, and opens doors to new markets and value-adds for customer success.

An example of this is provided by global smart metering solutions provider Iskraemeco, which helps energy companies readily deliver customer insights and functionality. To serve the global shift to a more resilient, reliable smart grid, Iskraemeco needed a flexible and simplified route to market for smart meters destined for multiple markets across the world. For it's utility customers to unlock the potential of data insights and intelligence, these edge devices need to meet the strongest standards of security and serve long in-field service lifespans withstanding local specification changes. Robust security built specifically for IoT devices and enabled on ultra-low power connectivity were key to Iskraemeco's innovation team for the design of their modular fourth generation smart meters.

The team foresaw new possibilities in how data can generate revenue streams for utility providers, positioning them as broader service providers. As a result, Iskraemeco transitioned to an eSIM with Kigen OS software, created and supplied by Workz. Each eSIM comes personalized with a global bootstrap, enabling both factory over-the-air meter testing and out-of-the-box global connectivity from Kigen's ecosystem of partners. If a local network is preferred, the Kigen remote SIM provisioning (RSP) service can provide a local operator profile with no need for physical access to the device. Interoperability across MNO profiles as well as modular subsystems remove hurdles for utilities when integrating mobile technology for large-scale, cost-sensitive smart meter deployments. Further ease of Kigen's RSP server's application programme interface (API) brought a unified workflow for companies, a big step towards easier adoption across the smart grid ecosystem.

> ***Smart meters will process the data where the data is collected, at the edge.***
>
> Gregor Rodic,
> Innovation Manager for Connectivity.
> Iskraemeco

Edge processing can help to manage and extract more value from the data in the age of growing grid management complexity. "Meters will have more edge computing capability in the future," says Gregor Rodic, innovation manager for connectivity at Iskraemeco, "Smart meters will process the data where the data is collected, at the edge, pick the insights needing cloud processing and empower local corrective action, enabling more grid flexibility. Integrating security technology opens (these) new possibilities"

By utilizing smart metering and other technologies, utility providers can start providing value-added services such as dynamic pricing, real-time billing, and real-time access to connected devices for remote analysis and maintenance, and usage control. New services open new revenue streams for utility providers, positioning them as broader service providers. Smart meters can become hubs for interoperating with all sorts of IoT devices and sensors at customer locations.

Decarbonizing power grids with... security!

KORE, Kigen and Energy Web bring eSIM, OPEN IoT SAFE and decentralized blockchain for world's first open-source energy trusted ID exchange.

Surprisingly, the biggest blocker in decarbonizing the electric grid is the lack of connectivity and shared standards, not the lack of new renewable energy resources. The energy sector needs a secure, scalable way to identify the growing number of clean energy resources, verify attributes about them (like location, capabilities, and financial relationships), and manage permissions and/or behaviors based on those attributes. In short, modern grids need an identity and access management solution tailored for the sheer volume and diversity of clean energy resources in the market.

A recently announced collaboration between Kigen and KORE – a global leader in IoT solutions and worldwide IoT Connectivity-as-a-Service (CaaS) – uses the features of eSIM and OPEN IoT SAFE to act as a hardware wallet anchored to an open-source, publicly accessible blockchain powered by Energy Web – a non-profit that is building operating systems for energy grids. These systems have been designed to help decarbonize the global economy. Using Energy Web's technology, organizations can build their own applications via the world's first open-source technology stack focused explicitly on the energy transition towards efficiency and renewable energy. As part of the collaboration that resulted in the deployment of OPEN IoT SAFE, a purpose-built SDK designed by Energy Web was used as part of the development process.

The ability to provide trusted information to third-party IoT providers via a SIM that employs device-level security and can authenticate data for cloud services is a significant development in the creation of end-to-end security within IoT ecosystems. The energy grid is one of the world's largest ecosystems. It comprises grid operators, utility providers, device manufacturers and EV charging networks. The Kigen, KORE and Energy Web collaboration allows this huge ecosystem to ensure the data is trusted and secure, thereby accelerating applications for the decarbonized energy market.

In summary

The plastic SIM card was originally designed purely to identify and validate a cell phone when accessing a mobile network, ensuring network security. The eSIM was designed for IoT devices to do the same thing, since the plastic SIM has increasingly been seen as an obstacle to growth of IoT on mobile networks. The development of the iSIM is now further opening up the range of applications that IoT can address, making it easier to address the massive variety of relatively low volume 'long tail' applications. Combining this with edge processing and LPWA connectivity has provided the opportunity to increase value while minimising costs. Establishing the SIM as a Root of Trust has then created a trusted environment where data can be securely shared, leading to the prospect of a wide range of new, innovative information services. This is the potential of a secure and intelligent IoT edge.

Kigen

www.kigen.com

beecham research

Shaping the IoT future