eSIM MARKET REPORT

Can eSIM be the enabler of massive IoT connectivity?

SPONSOR

Kigen

Can SIM be the enabler of massive IoT connectivity?

By 2025, GSMA Intelligence forecasts the total number of IoT connections will grow to 25.2 billion. Breaking these numbers down, Ericsson projects 5.2 billion cellular IoT connections also by 2025. This means that, by the mid-2020s, cellular IoT connections are expected to number more than 60% of mobile handset subscriptions and growing faster.

The largest proportion of these IoT connections are expected to be low-cost devices that are small in size, have limited processing power and storage, are battery driven and expected to run for 10 or more years, write Beecham Research's Robin Duke-Woolley and Bob Emmerson. These devices must remain connected to deliver sensor data and act upon commands from remote locations, and they must do this securely. Secure identities are required to identify these devices and their data, as well as protect them from misuse by remote attacks. The sort of use cases this covers are sensors, trackers, wearables and other low-cost devices that will increasingly form the backbone of the IoT – a myriad of data sources providing real time information on our world and how we live

As part of 5G, these are represented by the 'massive IoT' characteristic – the other 5G characteristics being high bandwidth and ultra-low latency – and will be used for those applications requiring vast numbers of low data rate, low power devices. **Figure 1** shows expected growth of these connections globally to 2028, adjusted to include the impact of the pandemic, with an annual growth rate of 48% in the period.

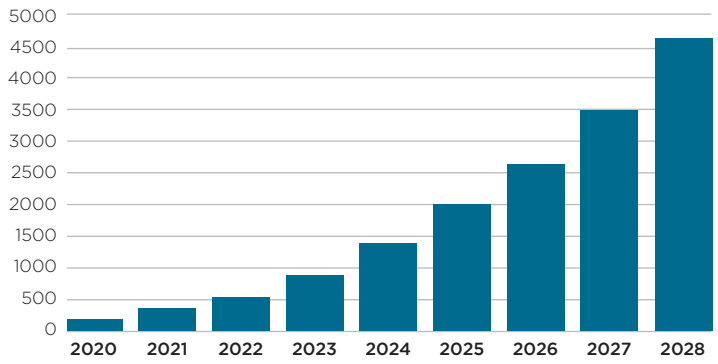
Massive IoT as part of 5G is designed to support one million such devices for every square kilometre (0.386 square miles), so there will be plenty of network capacity available. This raises some vital questions:

- How will these all be connected?
- How will they be powered?
- How much will the connection cost?
- How do you ensure the data from them is sufficiently secure to trust it?
- Most of all, how do you make this easy for users to implement in the very large numbers envisaged anywhere in the world?

Taking this last point, for such high numbers of devices, connecting them securely must be a completely smooth operation where the user does not need to understand the technology – just switch on and go.

Kigen, a wholly-owned subsidiary of **Arm Holdings**, believes that standards-based eSIM technology and it's integrated form factor iSIM, provide a particularly appropriate basis for answering these questions.

Figure 1: Massive IoT Global Forecast



(Source: Beecham Research 2021)

Firstly, this is because the eSIM approach provides the means for embedding the SIM during manufacture with a single stock keeping unit (SKU) and replacing the plastic SIM used in mobile handsets together with its physical tray. The correct network profile for the location the device will be used in is downloaded over the air when installed. This removes the logistical difficulties of working with two different supply chains and the operational management of disparate network agreements. By removing the physical tray and plastic SIM card, it also removes the need for a physical slot in the side of the device – thus improving its robustness. A slot in the side for a plastic SIM is completely inappropriate for any sensor or device that is installed to work with dust, damp or chemicals – particularly those that pose safety hazards. In

SPONSORED REPORT

An integrated SIM solution then includes an secure iSIM OS that is within the secure enclave of the SoC and uses the device's non-volatile memory

addition, many IoT devices are installed in remote, outdoor locations with the endpoint being the last and first mile in security, so making it tamper-proof is essential. A further advantage of this approach is that the physical form factor of the whole device can be reduced.

In addition to these physical advantages, the Kigen eSIM approach also includes a highly scalable Architecture of Digital Trust that is needed for this massive IoT growth. Kigen believes that IoT devices should be considered first-class or equal citizens especially when looking at security and that a tuned-for-IoT approach is needed. This means that the cost of getting connected must be very low and it must be easy to connect wherever needed globally.

This very low cost needs to be significantly lower than where eSIM costs have come from. This is because many of the devices in this category that will need to be connected in the future are themselves very low cost, and in turn constrained on battery life, size or memory . The breakthrough comes when the combination of costs of device hardware, connectivity and federated network access, can be brought down as low as tens or even just a few dollars. This low cost level is typical for IoT devices and solutions. Additionally, establishing trust is key to building services which will increase the attach rate at which eSIM solutions are used in devices. Address choice and models of driving services together, and the market potential is very large. Such a tuned-for-IoT eSIM approach, led by the standardisation and interoperability in mind brings IoT to the fore innovation in smart cities and urban mobility. Enabling fleet management of e-scooters, or e-bikes or micro-mobility solutions are drivers of fast growth for eSIM deployments and the attachment of trusted services. These booming markets did not exist a few years ago, and demand the widest possible choice of chipsets and modules as well as networks and cloud, all needing trusted devices.

The eSIM solution provides not just the hardware element that is soldered to the board inside a device but the whole solution for connecting and updating that element remotely over the air.

To address these needs, the solution that Kigen is progressing with its partners is encouraging an ecosystem at all parts of the hardware, including what is called a secure enclave. This is a secure chip in the corner of a system on-chip (SoC) that provides a dedicated area on the SoC to handle security related workloads and provide self-contained processing and encryption elements. The SoC in turn provides all the necessary electronic circuits and parts for a system on a single microchip. As we consider the proliferation of digital services in our lives, it's more than important that the devices and information across vital streams of application data remain safe and secure – from the little data to the big data.

Integrating the eSIM increases performance, reduces power usage

In its standardised hardware form, eSIM (also, called an embedded universal integrated circuit card or eUICC) extends the strong security foundations of the traditional SIM card to the challenges of the world of massive IoT. But how do you further simplify and streamline the manufacturing and logistics of reliable out-of-the-box connectivity to serve local markets? The solution required to achieve this is an evolution of the eSIM, which is the integrated SIM (iSIM).

An integrated SIM solution then includes an secure iSIM OS that is within the secure enclave of the SoC and uses the device's non-volatile memory. This removes the need for device makers to work with two supply chains that have traditionally been very separate.

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 ▶

As part of the eSIM/iSIM ecosystem, Kigen provides the SIM OS used by the iSIM element

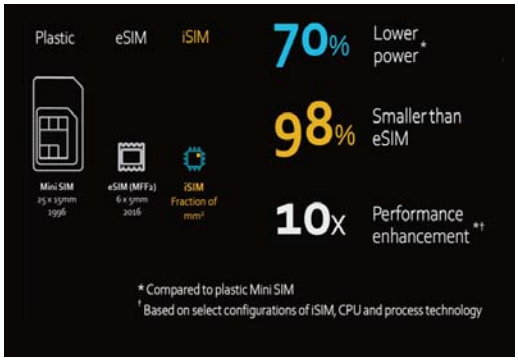


Figure 2: Comparison of Plastic SIM, eSIM with iSIM

power consumption, as the power for the iSIM element in the secure enclave is now derived from the SoC itself. It also increases 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. Just like the SIM and eSIM, iSIM can act as the root of trust for payment, identity and critical infrastructure applications.

Figure 2 shows a comparison of power usage, size and performance of a traditional plastic SIM and an eSIM element with an iSIM element. Note that the eSIM element is also rather called an embedded universal integrated circuit card (eUICC) – and the iSIM element an integrated UICC (iUICC). In addition to these advantages, the iSIM element is also significantly lower cost that the eSIM element, which as noted above is of particular significance for enabling massive IoT devices.

GSMA IoT SAFE Initiative

As part of the eSIM/iSIM ecosystem, Kigen provides the SIM OS used by the iSIM element. Closely associated with this is the IoT **S**IM **A**pplet **F**or Secure **E**nd-to-End Communication (IoT SAFE). IoT SAFE is a GSMA initiative that recommends the industry should use the SIM as a hardware secure element or root of trust to achieve end-to-end, chip-to-cloud security for IoT products and services. It is widely accepted that the SIM is particularly well-suited for this purpose: it is one of the hardest of all identifiers to spoof, with advanced security and cryptographic features, it is fully standardised, and has been deployed in huge numbers of devices for the past 30 years. Key characteristics of IoT SAFE include:

- Use of the SIM as a mini crypto-safe inside the device to securely establish a transport layer security (TLS) session with a corresponding application cloud/server
- Compatible with all SIM form factors (SIM, eSIM, iSIM)
- Provides a common application programme interface (API) for the highly secure SIM to be used as a hardware root of trust by IoT devices
- Helps to solve the challenge of provisioning millions of IoT devices

The IoT SAFE applet runs on Java OS, which in turn runs on the iSIM OS.

Enabling new IoT use cases

Earlier last year, we saw the example of an innovative tracking solution used by Bayer from Kigen's ecosystem partners around iSIM, akin to a printable shipping label. This is just one example of what is possible using the iSIM solution. A wide range of solutions across many different sectors, including buildings, energy, consumer/home, healthcare, industrial, transport, retail and public safety can be envisaged.

The low cost of such devices makes it economically feasible to enable many new applications that were too expensive before, even using an eSIM solution. **Figure 3** 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 ▶

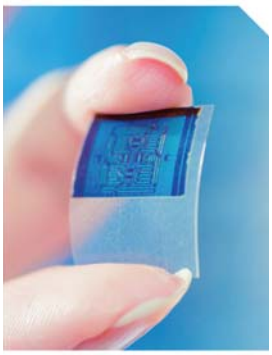


Figure 3: Low footprint, tamper resistant and quickly scalable

The key challenge in assembling these partners is to make the resulting solution easy to use wherever it is used

www.kigen.com

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.

Whilst these are striking examples of how iSIM benefits devices operating in tight constraints, there are many more full-functionality products that have applications for iSIM. One such area is smart cities, where a very large number of robust sensors are required to monitor environmental and other situations, including for example transport infrastructure.

Developing the ecosystem

To develop the ecosystem for these solutions, Kigen is working with most of the suppliers in the solution value chain. These include the following:

- Major silicon vendors
- SIM suppliers
- Cellular module suppliers
- Leading product manufacturers (OEMs)
- MNOs and MVNOs to provide the connectivity coverage globally.

The module suppliers are an important element, since for iSIM the most logical first stop is the module: the radio plus the SIM together. Such modules include an SoC within which the secure enclave and iSIM can be located.

The key challenge in assembling these partners is to make the resulting solution easy to use wherever it is used. Whether the user is a consumer or in a business, they should not need to know how the various elements work. They should just be able to take it out of the box and use it. To provide that simplicity is challenging but the only way to ensure that the huge volumes and promise of massive IoT will be achieved.