Unlocking the cellular IoT potential for chipset makers

Kigen

White Paper

The IoT adoption is accelerating rapidly with one trillion IoT devices predicted by 2035.

The potential applications for IoT span a vast number of industries, with IoT technologies advancing the development of smart cities, autonomous vehicles and connected industry technologies.

In the light of the sluggish smartphone market, chipset makers have been hungry to diversify their core businesses. So, it is no surprise that many of them are looking towards the integrated SIM (iSIM) as their next growth engine and the way to capitalize on the forthcoming cellular IoT boom.

Overview

IoT SoCs have unique requirements and are already becoming distinct from mobile SoCs and high-performance microcontrollers.

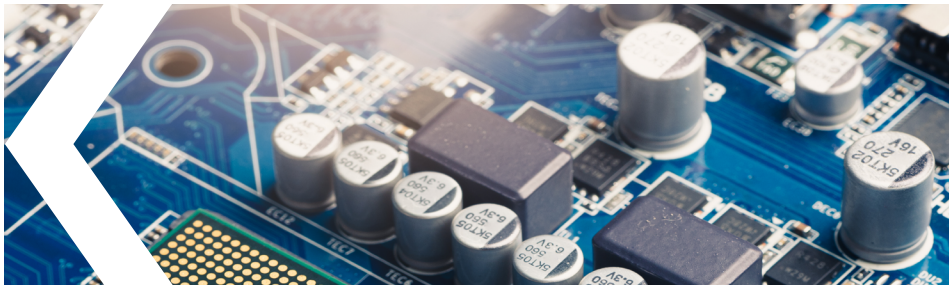
With iSIM technology now bringing SIM functions on-chip, and new IP for cellular connectivity such as LTE-M and NB-IoT, customized IoT chips can spur a new wave of innovation.

A shift to optimized, differentiated and secure iSIM-based SoCs has strong benefits for SiPs and the IoT ecosystem. Integration of iSIM technology and cellular IoT connectivity brings more opportunities for reducing device complexity, power, and bandwidth.

This whitepaper explores the key themes behind adoption of both technologies.

The topics covered include:

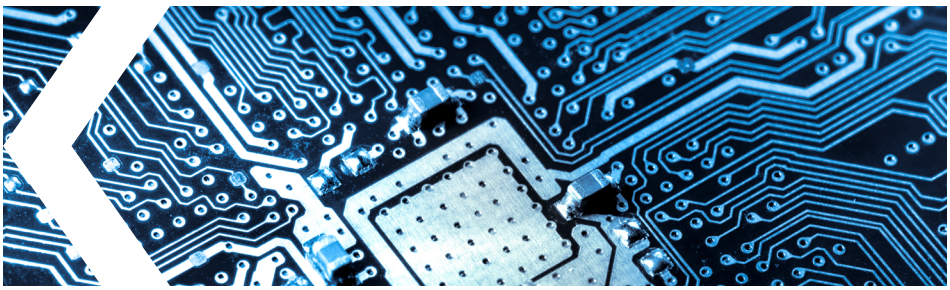
- Supporting cellular IoT connectivity
- Optimizing IoT devices
- Winning with differentiation
- Securing the solutions
- Shifting to iSIM technology



Supporting cellular IoT connectivity

In order to reach its full potential, the IoT sector has to be able to rely on scalable connectivity.

Short range connectivity (Bluetooth, Zigbee and Wi-Fi) will always have its use for IoT applications. However, it is not suitable for the numerous IoT scenarios where long-range connectivity with low bandwidth is required.



Cellular connectivity offers long-term availability and high reliability, as well as a developed ecosystem, proven ability to scale massively and industry recognized security for communications.

That's why it is widely expected that a large part of the new IoT growth will come from longer range devices using cellular connections. **Ericsson, for example, estimates 1.8 billion IoT devices with cellular connections by 2023.**

In recent years, there have been significant technological developments in cellular IoT connectivity, with multiple technologies sometimes competing and often responding to different IoT use case requirements.

Whether it's a licensed cellular (eg. Cat-M1 or NB-IoT) or an unlicensed LPWAN (eg. LoRa and SigFox) option, each technology has its pluses and minuses and the applications that it's best suited to.

For IoT architects, choosing the right mix of connectivity solutions requires careful consideration of application, performance, cost and power requirements. Smart meters and most constrained devices require small data transfers once or twice a day, so NBIoT may be perfect for them. If the nearest network access point is under 10km, LoRa and SigFox could be used.

However, these will not be suited to the applications that need high bandwidth, as with real-time surveillance. For asset tracking, data throughput is small, but there are inevitably many handovers as objects move, so NB-IoT will not be suitable as it doesn't offer seamless mobility support.

Incorporating cellular connectivity into the embedded design is not that much different from incorporating wireless interfaces like Bluetooth and Wi-Fi. Cellular and Wi-Fi connectivity are both viewed as data pipelines, ie. a communication channel from and to the analog-to-digital port.

Operators are cautious about new devices authenticating to and using their network. PTCRB (US) and GCF (Europe) are network operators' certification requirements to accept cellular enabled IoT devices on their networks. On top of that, each operator has their own verification processes.

This joined up approach ensures reliability and seamless operation of operator networks, and it is far stricter than for other, non-operator network and technologies. That is why cellular connectivity tends to be harder than Wi-Fi. This is one reason why there aren't that many cellular modem vendors while there are quite a few Bluetooth and Wi-Fi modem vendors. Except for the robustness of the cellular standards, there isn't much difference to the embedded developer.

Optimizing IoT devices

With stringent requirements, IoT devices demand further optimization beyond more efficient connectivity. Lower power consumption improves battery life and embedding or integrating a SIM enables physically smaller device designs. Hitting these marks opens more IoT use cases, driving improved volumes and lowering costs.

How does iSIM technology help developers optimize both chips and devices?

At the SoC level, power management needs a system perspective. The more features integrated onto a chip, the more opportunities to manage power holistically. When compute cores, wireless radios and iSIM functions are all integrated in a single SoC, power management can be optimized. Longer battery life translates into better user experience, higher customer satisfaction and a longer life in service.

iSIM integrated on an SoC also eliminates several external components. The familiar plastic SIM card and tray or a soldereddown eSIM chip are no longer required.

On-chip integration improves device reliability and reduces bill-of-material costs, as well as lowering total cost of operation (TCO) associated with SIM distribution, manufacturing and management. Fewer assembly steps and fewer components in the supply chain save on device manufacturing and overall procurement costs. During and after deployment, chances of mishandling are eliminated, and opportunities for physical tampering are reduced.

Standardized iSIM platform elements provide benefits in several areas. Application software is simplified through a consistent application programming interface (API) with a secure enclave containing the iSIM functions (more on this shortly).

Remote provisioning using iSIM technology eliminates the logistical and management issues associated with the traditional SIM cards. Interoperability will be enhanced as more developers adopt iSIM technology.

Design reuse is a major gain for IoT device development teams. The learning curve for iSIM technology using Kigen's software IP is short and, once understood, subsequent designs can leverage the same IP. Reuse means developers can devote more attention to optimizing their overall system implementation.

Winning with differentiation

With better optimization comes differentiation. Relying on proven iSIM technology at the heart of their IoT device design, developers can concentrate their innovation efforts on creating unique value add differentiation.

By leveraging iSIM IP, teams can bring IoT devices to market more quickly with more features. Pulling ahead of competition creates momentum and opens new application segments for device makers, which in turn creates more opportunities for chipset makers.

One critical feature for IoT applications is remote provisioning. Where M2M providers often hardwired their solutions, or used conventional SIM card technology, IoT connectivity managed over the air has distinct advantages. Legislation such as California's SB-327 comes online in 2020, heightening expectations for any connected devices having 'reasonable' security features, designed to prevent unauthorized access, modification, or information disclosure.

Remotely provisioned IoT devices are a natural fit. Remote provisioning, authentication, and subscription management can be streamlined with ready-to-use OTA capability native in iSIM technology.

Smartphone makers are desperately seeking more innovative ideas, and chipset makers offering iSIM technology can capitalize on this opportunity by providing a new differentiation path. Of course, iSIM technology directly replaces the existing SIM card model providing benefits we've already discussed.

The biggest area for innovation may be how subscriptions to cloud-based applications are supported. Bear in mind that a smartphone often serves as the gateway into the cloud for IoT devices.

Wearables and smaller phones also need iSIM technology, with increasing challenges in reducing size and power. For wearables, highly integrated cellular connectivity serves the needs of both voice and IoT data without the need for tethering to a smartphone.

Feature phones are making a strong comeback, many associated with pre-paid plans needing subscription management. iSIM technology may be essential for innovation in this next generation of mid-range mobile devices.

Automotive platforms are ideal for deploying iSIM technology. Many carmakers have already adopted eSIM technology using stand-alone chips, which helped them enormously in terms of reducing supply chain complexities and costs, gaining better control over connectivity and improving customer service.

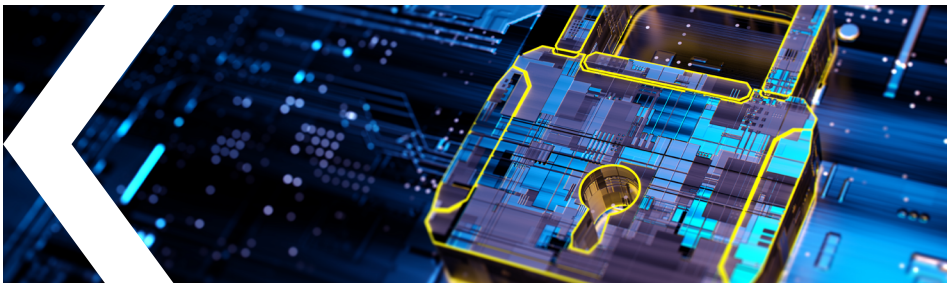
iSIM technology takes the next logical step, with remote provisioning capability and increased security paving the way for more features. For example, compliance with the ERA-GLONASS emergency calling system now requires SIM OTA testing. Integration of iSIM technology into a SoC also helps create a path to more robust ISO 26262 functional safety compliance for advanced driver assistance systems (ADAS).

Securing the solutions

In all these applications, security is becoming the defining characteristic. Without security, even the most well-designed devices can quickly lose the trust of users and fall out of favor. In cellular-grade solutions, end-to-end security is a must for protecting users and MNOs.

In cellular-connected IoT, devices must be discoverable, yet able to authenticate securely. In the future, the concept of "roaming" may be replaced by agile networks, where many devices can join and leave a network as users engage services on the go.

The security provided by the iSIM technology design is in part realized by the physical isolation provided by a secure enclave.



This secure enclave is fully partitioned from the rest of the SoC, with self-contained processing and encryption elements running a secure operating system compliant with the GSMA M2M eUICC specification. This makes iSIM technology at least as logically secure, and more physically secure, than using a discrete SIM outside a SoC.

For developers and infosec experts, there are several benefits. First is a minimized attack surface. **With the IP for the secure enclave integrated in the SoC, there is only a defined API available for accessing an iSIM implementation, as opposed to electrical contacts on a SIM or eSIM.**

Also, plastic SIM cards can be physically removed, where eSIM and iSIM are a less attractive target as they can't be physically identified and therefore are more difficult to remove and use elsewhere.

A secure enclave, with the appropriate industry recognized protection profile, hosting the iSIM OS also eases certification of the secure operating system and reduces the effort needed for creating secure applications.

Developers know exactly what they have in terms of the industry recognized levels of security afforded by iSIM and can concentrate on adding value at higher levels.

Shifting to iSIM technology

With iSIM technology, the IoT ecosystem is finally able to rally around cellular-based connectivity at scale. MNOs and OEMs can deploy and provision devices securely on almost any cellular network from 2G to 5G anywhere on the globe today.

SiPs using iSIM technology can create optimized yet differentiated IoT chipsets for a broader set of use cases enabled by smaller device size, lower power, and recognized security. Experienced SiPs and first time IoT chip developers alike rely on Kigen to lead the way with their SIM OS software IP.

Tighter integration between processing, wireless radio, encryption, and interconnect IP reduces risk and lifecycle costs for SiPs.

It's easy for developers to get started with Kigen SIM solutions. Kigen SIM OS delivers a hardware-agnostic, low footprint software stack with expected standardized functionality. This can be ported to a secure enclave hardware IP of choice.

Kigen server solutions implement standards compliant remote SIM provisioning (RSP) and SIM OTA solutions, with system integration support using REST/SOAP APIs.

For more on Kigen SIM solutions, visit:

❮ www.kigen.com

Kigen