Electronic Design

By BEE HAYES-THAKORE, VP of Marketing at Kigen, www.kigen.com

What Designers Should Know About iSIMs

iSIM technology, or the integrated version of SIM and its functionality, is broadening the path for secure embedded design. What are the differences between iSIM, eSIM, and SIM?

A decade ago, if someone had told you that a printable, flexible smart shipping label would be able to track the condition of a package for months during its shipment across land and ocean, would you have believed it? Or that a humble and inexpensive wristband could detect cardiac arrests and gain medical emergency assistance to save lives?

Even those with a strong allegiance to technology would certainly have been doubtful. Yet, such devices and many more are possible today. At the heart of these innovative solutions is a transformation in one of the core components of security—the SIM and its functionality, now available as an integrated capability into such devices.

Often familiar to us as the plastic SIM "card" from smartphones, the Subscriber Identity Module stores information about the associated network subscription. But physical SIM cards are being increasingly replaced by smaller eSIMs, which can be remotely provisioned. The latest evolution of this technology is the integrated SIM or iSIM, which incorporates the eSIM functionality into the mobile processor.

SIM, eSIM, and iSIM: What's the Difference?

SIMs are plastic, discrete removable cards. An eSIM requires a dedicated chip to be soldered on the device's circuit board. An iSIM, in contrast, is hosted within a tamper-resistant element (iTRE) on a device's system-on-chip (SoC) and can be provisioned or activated wirelessly using standard protocols.

Scope of iSIMs: Why is Designing with iSIM Relevant?

Research firm Kaleido Intelligence forecasts global iSIM shipments to reach 300 million by 2027. More than 260 mobile operators and connectivity service providers now support eSIM capabilities. With wide adoption of eSIMs, we can also see many operators effortlessly enhancing their systems to support iSIM.

Within the past five years, all top three network operators across North America, Europe, and Asia, along with all top five MVNOs in these regions focusing on IoT applications, have adopted iSIM into their roadmaps.

Resilient global connectivity is a critical feature requirement of today's devices and services. Baking the iSIM into a device means that insertion and activation of that connectivity become easier at the manufacturing stage and further in-field. Many device makers are increasingly driven to this model for better reliability in the field, creating a clear business demand for network operators and MVNOs to support iSIM technology.

Knowing the Benefits of iSIM

Size

An iSIM is minuscule, measuring a fraction of one millimeter squared in silicon surface area. Because an iSIM doesn't take up as much size within the device footprint as a physical SIM or an eSIM, this space is freed up for more functionality or to make the device more compact.

Security

The iSIM is enveloped within a secure and trusted area inside a device's SoC. The security of the iSIM complies with the GSMA eSIM M2M specification standard and can be augmented to include a certified EAL5+ level as created by Common Criteria. Specifications for the tamper-resistant element (TRE) are recognized by the Trust Connectivity Alliance (TCA) and will be crucial in setting a consistent standard for iSIM security.

A TRE is an individual and independent area within the hardware of the SoC. It runs low-level software to defend the iSIM against physical or virtual attacks.

Energy efficiency

Integrating the SIM into the silicon itself brings significant benefits in energy efficiency. Based on combinations of process nodes and secure iSIM OS tuned for IoT, iSIM

draws 70% lower power consumption than a traditional physical SIM.

Furthermore, compared with its predecessor, the eSIM, it boosts a 50% lower power usage, which is ideal for devices that require a long battery life. In many growing IoT markets, this is a significant design consideration. For example, smart meters may be mandated to have a field life of over 10 years without the ability to replace batteries.

Just-in-time provisioning

IoT devices are now designed with built-in connectivity to minimize unit costs for high volume, especially when addressing markets such as smart metering or healthcare. Production lines are typically producing tens of thousands of devices daily, and simplified logistics around anticipating network profiles and credentials reduces complexity and improves reliability.

With iSIM, (much as with eSIM), such binding of operator profiles can occur on the factory production line itself, referred to as just-in-time provisioning. This is a significant advantage over traditional SIM, reducing recalls or needing to swap SIMs through expensive truck rolls when deployed in the field. iSIM directly supports ease of manufacture of ready-to-connect products and applications, which has long been the barrier for growth around IoT scale.

Total Cost of Ownership

Complexity, reliability, and cost go hand in hand. Any enterprise or end customer needs to consider the overall lifetime cost of the device, with consideration of both direct bill-of-materials (BOM) and development costs, and indirect costs of using various iSIM/eSIM and Remote iSIM/eSIM provisioning techniques.

Recent research from Transforma Insights deduced that on average, eSIM devices cost 8% less over the device's lifetime on a like-for-like basis than those using plastic removable SIMs. Even greater benefits come from iSIMs, which on average is 13% cheaper than plastic removable SIMs averaged across multiple use cases.

Standards and compatibility

iSIM is now defined and incorporated throughout the cellular industry's specifications as an accepted form factor while maintaining existing SIM functional standards' requirements. GSMA now routinely includes iSIM support throughout the Remote SIM Provisioning (RSP) and SIM Security Accreditation Scheme (SAS) specifications they're generating. Furthermore, iSIM is included in the accepted methodologies for assessing a SIM's security and is recognized by the TCA.

Designing Embedded Systems with iSIM

As an embedded design engineer, designing a secure IoT device with an iSIM requires careful consideration of several factors, including hardware, software, and communication protocols.

- *Choose a secure hardware platform:* Selecting a secure hardware platform is the first step in designing a secure IoT device with iSIM. The hardware platform should have built-in security features like secure boot, hardware-based encryption, and tamper detection. The good news is that the wait is over, and a range of secure hardware platforms are available as evaluation kits or even hardware-acceleration platforms complete with test UI. All use leading chipsets and come with a choice of cellular modules that address different connectivity technology combinations.
- *Use a secure operating system:* Selecting a secure operating system is also crucial in designing a secure IoT device. The operating system should have built-in security features like secure boot, memory protection, and access control. In addition, the operating system should be capable of running security protocols, such as SSL/TLS, DTLS, and IPSec.
- *Implement strong authentication and encryption:* Authentication and encryption are vital in securing an IoT device and help leverage iSIM advantages. The device should implement robust authentication mechanisms, such as mutual authentication and PKI, to prevent unauthorized access. Also, the device should use strong encryption algorithms, such as AES, to protect data in transit and at rest.
- *Use a trusted execution environment:* A trusted execution environment (TEE) is a secure area within the chip isolated from the main operating system that provides a secure execution environment for sensitive applications. This partitioning could be extended to enable remote provisioning of secure functions (with iTREs or, more generally, integrated secure environments (iSEs)) to securely store and process sensitive data, such as cryptographic keys and user credentials.
- *Implement secure communication protocols:* Implementing secure communication protocols is essential in securing an IoT device with iSIM to achieve end-to-end secure data flows. The device should use secure communication protocols, such as SSL/TLS, DTLS, and IPSec, to encrypt data in transit and authenticate communication partners. iSIM works with the GSMA IoT SAFE standard to authenticate chip-to-cloud security, and this combination has the potential to enable massive-scale IoT. In addition, the device should implement secure communication protocols, such as MQTT or CoAP, to ensure secure communication between the device and the cloud server.
- *Use over-the-air (OTA) firmware updates:* OTA firmware updates are essential in maintaining the security of an IoT device, and this requirement is also true with iSIMs. Firmware updates should be delivered over a secure channel and be signed with a trusted certificate. Also, these updates should be encrypted to prevent tampering and protect against man-in-the-middle attacks.

• *Implement remote management:* Remote management is essential in maintaining the security of an IoT device with iSIM. The device should be able to receive remote commands from the cloud server to perform tasks such as firmware updates, device configuration, and diagnostics. The device should also implement secure protocols, such as HTTPS, to ensure that remote-management commands are authenticated and encrypted.

• *Conduct regular security audits:* Lastly, regular security audits are essential in maintaining any IoT device's security. This becomes increasingly important as we start seeing IoT device deployments evolve. Not all devices will immediately be able to move to integrated form factors, and varied levels of security implementation from prior generations shall co-exist. Security audits should be conducted by independent third-party security experts to identify vulnerabilities and recommend remediation strategies. In addition, security audits should be conducted regularly, such as annually or biannually, to ensure the device's security posture is up-to-date and aligned with industry best practices.

In conclusion, designing a secure IoT device with iSIM requires careful consideration of several factors, including hardware, software, and communication protocols. The device should use a secure hardware platform, implement strong authentication and encryption, use a TEE, implement secure communication protocols, utilize OTA firmware updates, implement remote management, and conduct regular security audits. By following these best practices, embedded design engineers can ensure that their IoT devices with iSIM are best positioned to out-think future challenges.

An engineer turned marketeer with over a decade of focus on IoT, Bee Hayes-Thakore is VP of Marketing at Kigen.