Brought to you by:

Kigen

eSIM & iSIM

for dummies®

A Wiley Brand

Reduce size and ensure security

Enable remote provisioning

Reduce total cost of ownership

Brian Underdahl

Loic Bonvarlet, Kigen

Patrick Biget, Kigen

Jean-Philippe Betoin, Kigen

Kigen 2nd Special Edition

About Kigen

At Kigen, we are making the future of securing connectivity simple. As simple as can be. Together with our partners and customers, we are at the forefront of unlocking a new era of secure IoT as Integrated SIM (iSIM) and eSIM become the mainstream choice for connected devices. Our industry-leading SIM OS products enable over 2 billion SIMs. Our GSMA certified remote SIM provisioning and eSIM services drive this momentum further placing us amongst the top 5 SIM vendors globally. As an Arm founded company, we bring an ecosystem approach to driving innovation and collaboration. For more information, go to kigen.com or speak to us on @Kigen_Ltd on Twitter and LinkedIn about #futureofSIM.

eSIM & iSIM

Kigen 2nd Special Edition

by Brian Underdahl
Loic Bonvarlet, Kigen
Patrick Biget, Kigen
Jean-Philippe Betoin, Kigen

for dummies®
A Wiley Brand

eSIM & iSIM For Dummies®, Kigen 2nd Special Edition

Published by
John Wiley & Sons, Inc.
111 River St.
Hoboken, NJ 07030-5774
www.wiley.com

ISBN 978-1-394-15502-6 (pbk); 978-1-394-15503-3 (ebk)

Publisher's Acknowledgments

We're proud of this book and of the people who worked on it. Some of the people who helped bring this book to market include the following:

Project Manager: Rebecca Senninger

Acquisitions Editor: Ashley Coffey

Senior Managing Editor: Rev Mengle

Senior Client Account Manager: Matt Cox

Kigen Subject Matter Experts: Bee Hayes-Thakore, Mayank Sharma, Paul Bradley, Said Gharout, Tom Burke, Jerome Allard, Charlie Harrison, and Kigen's ecosystem partners

Production Editor: Mohammed Zafar

Table of Contents

Introduction

With ever-accelerating deployment of the cellular Internet of Things (IoT) and other connected devices, it's becoming apparent that there's a growing need for security. The most well established is found in smartphones — the familiar SIM, or the standard subscriber identity module. SIMs need to be replaced with something that's smaller, more versatile, and more efficient, or even dematerialized for the end user, while maintaining the identity and security levels that SIMs provide. As IoT devices begin to fulfill more and more functions in smaller packages, ensuring seamless connectivity, saving space, and reducing power consumption are becoming even more critical parts of the design process. As those devices become ever more ubiquitous and present across the globe, there is a growing need to keep the devices and their data securely managed in field in a scalable manner economically. eSIM and iSIM evolve SIM technology to achieve this affordably and open the benefits of global, secure connectivity without the need for prior expertise in cellular.

About This Book

eSIM & iSIM For Dummies, Kigen 2nd Special Edition, introduces you to *embedded SIMs (eSIMs)* and *integrated SIMs (iSIMs)*, two new form factors of SIM that provide all the advantages of traditional SIMs while offering enhanced physical security, lower power consumption, reduced size, and remote provisioning capabilities. In addition, this book shows you that eSIMs and iSIMs offer the promise of cost savings in handling, activation, and keeping connnected — the total cost of ownership (TCO) associated with the billions spent on handling SIMs.

Icons Used in This Book

This book uses the following icons to call your attention to information that you may find helpful.

REMEMBER

The information in paragraphs marked by the Remember icon is important and therefore you should give it special attention.

TECHNICAL STUFF

Sometimes we need to introduce a bit of technical information to more fully explain a particular topic. The text marked with this icon is your chance to pick up a bit of jargon you can use to impress your boss.

TIP

The Tip icon indicates extra-helpful information. Tips can save you some steps, give you a better way to get the job done, or make your life a bit easier.

This book also has its share of technical terms. You can find definitions for the terms shown in *italics* by turning to the Glossary at the end of the book.

Where to Go from Here

You can read this book the traditional way, straight through from front to back, if you prefer. Otherwise, you can dive in anywhere if that's your style. Each chapter is written to stand on its own if you'd like to jump directly to a topic that interests you.

Or if you want more information than can fit in this book, explore further on `kigen.com`

IN THIS CHAPTER

- Understanding how eSIMs evolve capabilities of SIM technology
- Seeing how iSIMs represent the future

Chapter 1
Introducing SIM Technology

IoT devices bring the promise of many new possibilities, but only if they can be connected and identified securely. This chapter shows how the evolving SIM is designed to meet those needs.

Understanding SIMs

In the early days of telecommunications, telephone companies could easily identify who was using their networks. There weren't very many users, and all connections were hardwired. Fast forward to the era of cellular phone networks, and network operators needed a reliable method of identifying users, checking the authenticity of endpoint devices, and securing their data. This need spurred the development of the *subscriber identity module (SIM)*.

Over the years, SIMs have shrunk from the original plastic card 1FF (FF stands for *form factor*) to 2FF (Mini SIM), 3FF (Micro SIM), and finally 4FF (Nano SIM). (See Figure 1-1.) Regardless of the packaging, all SIMs are built on smart card (*UICC*) technology similar to bank cards. The UICC is a secure computing chip that contains memory and provides identification services. SIMs

store operator "profiles," a set of files with essential applications and sensitive data, that enable authentication of a subscriber to authorize access on cellular networks and charge for the provided services. Traditional SIM cards have the operator-defined profile programmed during manufacture.

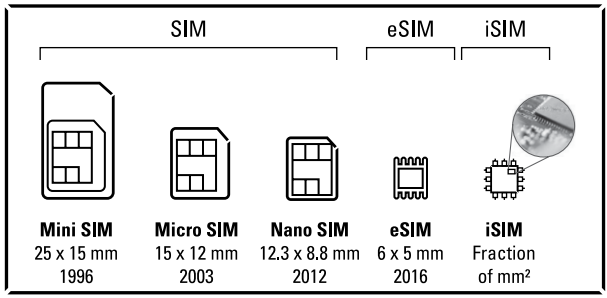

FIGURE 1-1: eSIM and iSIM evolve the SIM technology for compact, energy efficient, and remote IoT devices.

Discovering eSIMs

Despite being the most adopted and well established security standard globally, the SIM technology has limitations for new IoT devices and their data. Some of these issues include:

- **Size:** Even Nano SIMs, along with their socket, take up too much space in very small devices.
- **Fragility:** User-replaceable SIM cards are easy to damage.
- **Physical security:** A pluggable SIM is easily accessed and stolen to deny service or to connect another device.
- **Management and cost:** Because traditional SIM cards are replaceable, they must be inventoried, shipped, and installed in devices. Each of these processes adds associated costs.

Embedded SIMs (eSIMs) are an evolution of the SIM card designed to address the limitations of traditional SIMs. They take a step further with new functionality that's needed to enable trusted IoT devices. eSIMs are typically physical SIMs that are soldered into the device and enable storage and remote management of multiple network operator profiles (*remote SIM provisioning*), offering the following advantages:

- **Seamless global connectivity:** Networks can be switched easily and without physical handling, anywhere in the world.
- **Size:** Because eSIMs are about half the size of Nano SIMs and don't require a socket, they easily fit in very small devices.
- **Durability:** Users can't reach eSIMs so they can't damage or lose them.
- **Physical security:** A SIM soldered within a closed device is hard to locate, remove, and reuse.
- **Cost:** eSIMs reduce the total cost of ownership of the device because they optimize and eliminate costly supply chain and management costs.

REMEMBER

The term *eSIM* can refer to either the embedded SIM form factor or the ability to store multiple profiles and remotely provision them. An *eUICC* is a UICC capable of supporting remote provisioning. Typically, the terms *eSIM* and *eUICC* are used interchangeably. This book uses the term *eSIM.*

Introducing iSIMs

Kigen recognized that, although eSIMs addresses many traditional SIM challenges, the technology could benefit from further optimizations to achieve scale. The *integrated SIM (iSIM)* moves the SIM from a separate chip into a *secure enclave* alongside the application processor and cellular radio on a purpose-built *system on a chip (SoC)*. Delivering these three building blocks in one embeddable component greatly reduced the circuit board footprint (see Figure 1-2), component sourcing, and IoT device manufacturing costs.

eSIMs and iSIMs are hardware-backed security, dedicated physical circuits rather than *soft SIMs* (or software). This is an important distinction because unlike software, secure physical circuits resist advanced hacking. Device manufacturers and network operators can't afford the risks that would be associated with implementing SIMs in software. Kigen's standards-compliant SIM *operating system (OS)*, combined with the secure hardware design of a System on Chip (SoC), gives iSIM its security assurance.

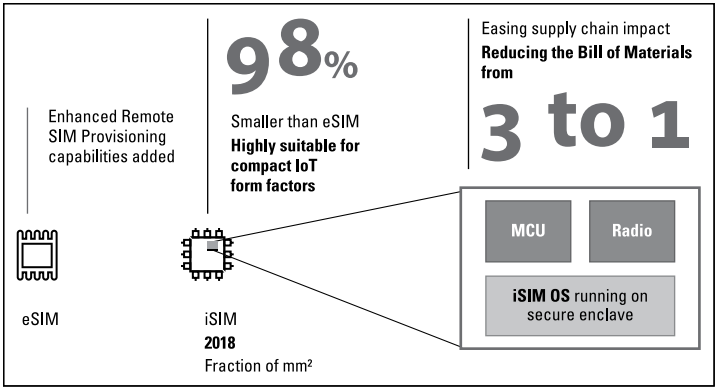

FIGURE 1-2: iSIM builds on the eSIM enhancements reducing the size and bill of materials.

IN THIS CHAPTER

- Seeing how profiles work
- Understanding the key features

Chapter 2
Understanding Remote SIM Provisioning

Provisioning is the act of installing the initial data and software that a device needs to start functioning. For a SIM card, this is essentially the programming of the mobile operator profile in the memory of the chip for the SIM to be ready to connect to a cellular network.

The emergence of new IoT devices, which require cellular connections, are driving a re-evaluation of SIM provisioning to ensure they too can have their connections enabled remotely. This chapter discusses how eSIMs and iSIMs take advantage of remote SIM provisioning, which is simpler and more economical.

Remote SIM Provisioning

To understand *remote SIM provisioning (RSP)*, it's helpful to consider how traditional SIM cards work. Imagine that you've just bought a new cell phone. The next thing you need is a SIM to

connect to a network. The SIM you get will be preprogrammed for the network you've chosen by storing your network operator *profile* (also referred to simply as a *profile*).

This preprogramming is done as part of card manufacturing using specialized equipment to inject the right data into the SIM, also referred sometimes as *personalization*. You insert the SIM in your phone and follow instructions to begin making calls or using data services. If you want to change to another provider, you must physically swap your old SIM for one from a new provider.

Now, consider a scenario where your company wants to deploy tens of thousands of IoT devices that are globally distributed and all need a cellular connection. You wouldn't want to be the unlucky person who had to insert each SIM into the correct device. What if these devices need to be moved outside the original network or can't be reached easily?

To serve these needs, it is possible to deliver the required operator profile and other data essential for connection, remotely to change the profile on a eUICC or integrated UICC already in field. This removes the need to physical change the SIM hardware, and is called *remote SIM provisioning*. This capability is particularly important for the IoT sector, where individual physical device management is often cost prohibitive because of the deployment scale, remote locations, or inaccessibility of devices.

For large IoT deployments, a *subscription manager* allows you to securely and remotely manage the profiles to deliver a seamless customer experience for eSIM-enabled devices.

RSP comes in two flavors, as shown in Figure 2-1. The first is a consumer solution that offer an end-user's cellphone device the ability to request or pull the required profiles, on the user's demand. The second flavor is an M2M (machine to machine) solution, where the fleet owner can push a SIM profile and needed data to an unattended device in the field. This is suitable for many cellular IoT deployments. This book focuses on the M2M solution.

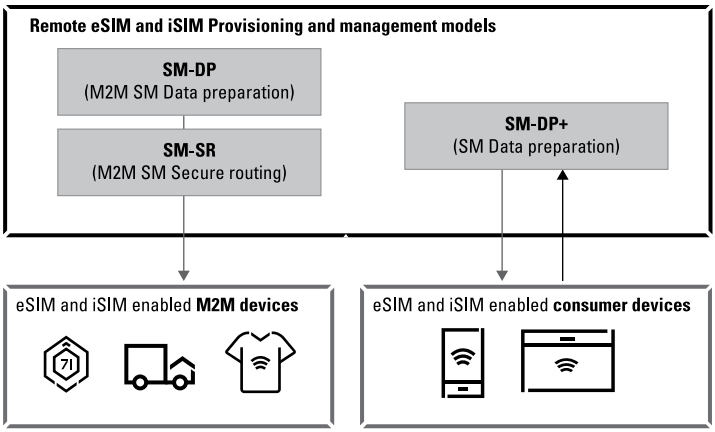

FIGURE 2-1: The two flavors of RSP.

Understanding Profiles

SIM cards enable network access through the use of *profiles* that contain information about the related *subscription*. This information includes the operator's credentials and other unique identifiers.

eSIMs and iSIMs implement the eUICC's ability to store multiple profiles in a secure storage. These multiple profiles are especially useful for IoT devices that must be provisioned for multiple networks, such as tracking tags for international shipments. A traditional SIM usually contains only one profile matching only one subscription. If necessary, iSIMs can also operate with a single profile permanently associated to one network, but are not limited to such implementation.

Considering the Key Features

Remote SIM provisioning opens the door to a range of use cases not supported by conventional SIMs. For example, a device manufacturer can embed eSIM or integrate an iSIM into devices and install the operator profile at the production factory. When the device is turned on, it can connect to a local cellular network, making the device ready to use immediately regardless of location (this is also called out-of-the-box connectivity). Instead of the

manufacturer holding stocks of SIM cards for multiple network operators across the globe and coordinating which card should be inserted into which device, every device can have the correct profile remotely provisioned at the point of delivery.

Remote SIM provisioning allows manufacturers to drastically simplify their procurement arrangements. It allows remotely connecting devices and provisioning them securely over the air, across the globe, and over their entire lifetime.

The GSM Association (GSMA; originally Groupe Speciale Mobile) has introduced specifications to address remote SIM provisioning. They cover the following elements:

- **For M2M:**
  - *Subscription Manager-Data Preparation (SM-DP):* This is responsible for preparing, storing, and protecting profiles. It also downloads and installs profiles onto the M2M eSIM.
  - *Subscription Manager-Secure Routing (SM-SR):* This is responsible for managing the status of profiles on the eSIM. It also secures the communications link between the eSIM and SM-DP.
- **For Consumer:**
  - *Subscription Manager-Data Preparation + (SM-DP+):* This is responsible for preparing, storing, and protecting profiles. It also downloads and installs profiles onto the eSIM, along with binding it to unique identifiers and provides a register of the hardware.
  - *eUICC (eSIM): eUICC* is used interchangeably with *eSIM.* These terms indicate a secure element that is not easily accessible or replaceable and is designed to remotely manage multiple network operator profiles in accordance with GSMA specifications.
  - *Compliance:* A set of established criteria ensures that the necessary security protocols and required functional aspects are delivered.

See Chapter 6 for help deciding what to include in your adoption plan.

IN THIS CHAPTER

- Seeing how eSIMs and iSIMs offer benefits by solving some key technical challenges
- Considering how eSIMs and iSIMs can work for MNOs
- Understanding what OEMs will gain

Chapter 3
Looking at Benefits

This chapter looks at how eSIMs and iSIMs offer tangible benefits to enterprises, Mobile Network Operators (MNOs), and device manufacturers.

Benefits for Enterprises

The emerging IoT marketplace enables more innovation and faster access to information. eSIMs and iSIMs provide enterprise benefits such as:

- **Flexibility:** Rather than putting up with the limitations of generic devices, organizations can employ inexpensive connected devices designed for specific tasks, or even specific products.
- **Cost reduction:** The total cost of ownership of devices (covering provisioning, product tracking, and procurement arrangements) is reduced.
- **Durability:** Because eSIMs and iSIMs aren't removable, losses due to damage, vibration, and extreme temperature are eliminated.

Futureproof investment in IoT: Enterprises can commit to IoT deployments with confidence that they will be able to easily manage their IoT device connectivity remotely at a global level.


TIP

iSIMs take a leap forward from eSIMs by being integrated into the silicon an existing system on chip, so they provide significantly reduced device costs and lower power consumption. They simplify manufacture because of the reduced component count.

Looking at Benefits for MNOs and IoT Service Providers

Mobile Network Operators (MNOs) also stand to gain numerous benefits from eSIMs and iSIMs. Compared to traditional SIM cards, MNOs can expect changes such as:

- **Reduced costs:** For devices that use eSIMs or iSIMs, MNOs will see the elimination of the distribution and inventory practices associated with traditional SIM cards. MNOs won't have to purchase, stock, or ship SIM cards. They'll also see reduced support costs because of greatly simplified remote SIM provisioning.
- **Increase in network connections:** Remotely provisioned eSIMs and iSIMs will enable MNOs to capitalize on the wider adoption of cellular IoT devices by serving already deployed devices that previously would have been permanently attached to another MNO, thus increasing revenue opportunities. IoT devices represent a new, fast growing market that promises to continue growing for quite some time into the future.
- **Maintain security:** GSMA standards compliance ensures that subscriber and network security remains strong and interoperability is achieved.


REMEMBER

eSIMs and iSIMs aren't limited to being used in IoT devices. Cell phone manufacturers are increasingly incorporating remote SIM provisioning support in their new designs to reduce costs, so supporting eSIMs and iSIMs will increasingly become necessary to remain competitive.

Considering Benefits for OEMs and Module Makers

Device or original equipment manufacturers (OEMs) and module makers will see great benefits from the move to eSIMs and iSIMs. These include:

- **Reducing supply chain complexities and costs:** The number of global product variants is reduced because there is no longer the need to implement multiple product lines or Stock Keeping Units (SKUs) for different networks around the world, leading to cost reductions.
- **Control over connectivity and better customer experience:** Device makers can have a greater influence over their device connectivity and may offer connectivity for free or as global data packs.
- **Product improvement:** The new technology offers significant size reductions by freeing up space on the printed circuit board (PCB), meaning resulting devices can be extremely compact. Deeper integration improves power performance (in the case of iSIMs) and reliability.
- **Differentiation and capitalizing on IoT growth:** Incorporating eSIMs or iSIMs can become an element of differentiation from competitors or the route to tap into the full potential of IoT by offering devices that can be managed easily and remotely.

REMEMBER

8 out of 10 leading module makers have already adopted and announced iSIM modules, and momentum is growing. Industry analysts report that almost three out of four cellular devices by 2030 will support eSIM and iSIM.

iSIM has also been acknowledged and approved by multiple global Tier-1 MNOs and leading Mobile Virtual Network Operators (MVNOs) worldwide.

Going to Market with iSIM IoT

Typically, a device maker would have to work separately with a module vendor and the operator as well as a SIM vendor to place multi-party agreements to add cellular connectivity to its connected product. Figure 3-1 shows the procuring changes with iSIM. The critical change is that the device maker can receive the right combination of its identifiers pre-installed in its chosen module. This can be personalized in-field to the OEM's requirements with the selected operator profile.

Based on the design, silicon manufacturing process, and other optimizations, iSIM can deliver better performance. On specific combinations of the iSIM operating system and secure enclaves tested by Kigen, this advantage was as high as ten times compared to eSIM. This has benefits in many use cases discussed further in Chapter 4.

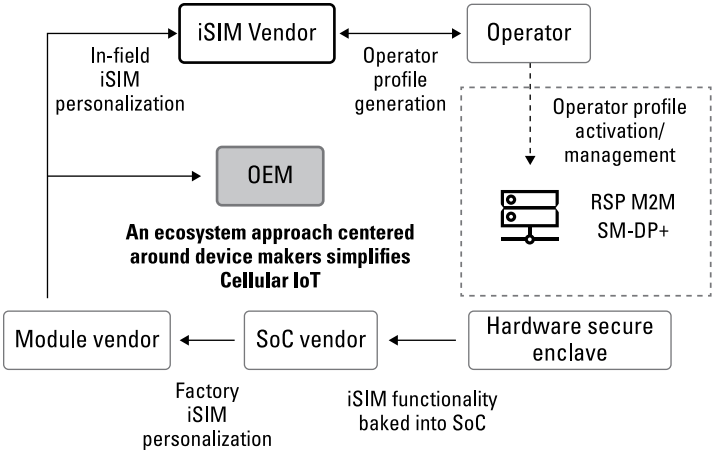

FIGURE 3-1: An ecosystem approach to iSIM manufacturing improves time to market for OEMs.

IN THIS CHAPTER

- Realizing the potential of IoT
- Showcasing some use cases
- Opening new paths

Chapter 4
Understanding Changes and Emerging Opportunities

New technologies such as eSIM and iSIM create new opportunities even for those businesses that have no prior experience or expertise in cellular. This chapter takes a brief look at this emerging market.

Understanding the Potential of IoT

Low-cost, low-power IoT devices that can communicate via cellular networks offer a huge range of brand new possibilities. Tasks that were impossible or too expensive to consider suddenly become easy and cheap.

For example, consider a manufacturer who needs to control costs by only having parts on hand that will be used quickly. In the past, shipment tracking was imprecise at best, so parts had to be ordered in advance to ensure they'd be there when needed. With cellular IoT-based tracking devices, it may be possible to use more precise tracking information to maintain a leaner inventory.

REMEMBER

Almost any task where something can be counted, measured, or tracked offers the potential for automation through IoT devices. Automation can be enabled with cellular IoT independently of local connectivity options.

Looking at Use Cases

The emerging marketplace for cellular connectivity includes thousands of possibilities, all of which share some common needs: Devices must be securely identified and authenticated, and they must be able to share important information. Consider the following examples:

- **Automotive:** The automotive industry has been eager to embrace this new technology because it provides exciting, new ways to increase flexibility and after-sale support. For example, mandated emergency call or e-call functionality has resulted in the use of eSIMs with a permanent emergency profile. This connectivity is only used for incident triggered location and assistance support alerting in cars, heavy good vehicles and increasingly other vehicles such as motorbikes.
- **Agriculture:** With global food supply, tracking food product safety throughout the entire supply chain becomes more important every day. eSIMs and iSIMs can be provisioned for multiple networks, enabling real-time monitoring of storage and transit environments to ensure food freshness.
- **Asset tracking:** With real-time logistics gaining more importance as the critical enabler of how goods and services successfully reach customers when they are needed, eSIM and iSIM enabled asset trackers can offer enterprises real-life inventory intelligence.
- **Banking:** The SIM or embedded Secure Element is already used in smartphones as authentication for any mobile banking or biometrics app. But it isn't suited from a cost, size, and power comparison for the wider range of IoT wearables or other more compact size devices that need resilient connectivity. Such devices are no longer limited to Bluetooth tethering to a smartphone or on small area Wi-Fi networks and can benefit from eSIM or iSIM technology.

- **Digital mobile passports or IDs:** With the robust security that iSIM can offer, a smartphone, home, or wearable can use a dedicated device root of trust placed within the iSIM as the authenticator of the user's data, forming the basis of mobile ID, digital wallets, and personal health or travel records.
- **Electric vehicle and renewable energy sources:** Largely, the growing number of renewable energy sources are IoT connected assets. Once authenticated and secured by a root of trust protected within the iSIM, the data streams from these devices can be used for financial level transactions to open new applications that move us to a zero-carbon economy. Such examples can extend to other models where an Economy of Things can be enabled through robust and resilient security.
- **Healthcare:** Remote patient care is another fast developing model for the use of devices and data that demands stringent security and can benefit from remote management with eSIM and iSIM.
- **Micro-mobility:** Comprising of journeys less than 15 kms, micro-mobility transport vehicles such as e-bikes, e-scooters, and more offer greener ways to travel and make cities more sustainable. Due to the compact nature, and need to maximize the battery life between charges, these solutions benefit from eSIM or iSIM technology.
- **Service-oriented business models:** The combination of being able to add connectivity into a device along with security allow manufacturers to offer a service that users can subscribe. Such rent-instead-of-buy models are gaining more prominence in retail, healthcare, and more. These typically require resilient connectivity that can be achieved through remote SIM provisioning capabilities.
- **Utilities:** eSIMs and iSIMs offer new possibilities, such as solving the problem of operator lock-in and reducing the need for site visits. Smart metering is a particular area of growth where eSIMs allow businesses to meet with evolving regulations, support smart energy grid and address energy or resource theft.

Seeing How eSIMs and iSIMs Open Differentiation Paths

eSIMs and iSIMs enable devices to be smaller and operate on less power while still containing secure cellular communications capabilities. These attributes mean that manufacturers can create new types of devices that are less obtrusive, easier to use, and include new options.

Imagine, for example, that a company like Amazon or UPS wanted a solution for the "porch pirate" problem of packages being stolen from people's front steps after delivery. Those packages contain a barcode that's scanned when the package is delivered, but the shipper has no method of following the package after delivery. A low-power tag containing an eSIM or iSIM could provide short-term cellular connectivity to allow the package to be located if it were moved to another place. Such a smart tag would only be possible because it contained the eSIM or iSIM.

Considering New Value-Added Services

The transition to remotely provisioned eSIM and iSIM technology will offer the potential for a whole array of new services. For example, MNOs and IoT providers can offer a single managed service for deployed IoT devices, leaving OEMs to focus on their core activities.

On the other hand, OEMs can choose to add customer value on top of the existing core (device) products, for example, by offering add-on services delivered locally. OEMs will also be able to tap into the connectivity wholesale market, bundling connectivity with device rental plans or offering basic connectivity for free with other services — as a premium.

IN THIS CHAPTER

- Conforming to standards
- Understanding the GSMA

Chapter 5
Ensuring Standards for Connectivity and Data Security

Interoperability of devices from different manufacturers with other actors such as vendors or users is vital to the success of any new technology. This chapter discusses how interoperability is ensured through the establishment of and conformity with industry-wide standards.

Conforming to Standards

SIM technology and cellular network authentication are founded on the standards evolved by the European Telecommunications Standards Institute (ETSI). More recently, additional industry groups such as Global Platform, the SIMalliance, and the GSMA have enabled new technology concepts, including those supporting the remotely provisionable SIMs.

The GSMA has encouraged the industry in formulating documents and processes to ensure the RSP technology is interoperable and the ecosystem is secure.

These include the GSMA technical permanent reference documents (PRDs), which outline the architectures and functionality and set out how a product or service should be built to allow it to work successfully and support the RSP ecosystem.

The GSMA also created compliance and testing guidance documents that ensure providers can demonstrate that their products or services adhere to the PRDs. The compliance documents outline the steps needed to achieve GSMA certification, including accreditation.

Understanding Accreditation

The GSMA has set up two security accreditations schemes to promote best operational practices:

- **SAS for UICC Production (SAS-UP):** The voluntary scheme through which UICC manufacturers subject their production sites and processes to a security audit
- **SAS for Subscription Management (SAS-SM):** The scheme for security auditing and accreditation of the providers of eUICC subscription management services

Once RSP accreditation and compliance have been achieved, the platforms, services, or products are issued certificates allowing them to function with other accredited actors in the GSMA controlled RSP ecosystem.

Addressing Data Security in a Standardized Manner

As IoT devices proliferate into the billions, it's vital for all users and network operators that each of those devices has a secure identity. Not only is this necessary to maintain needed privacy, but secure identity is also important in maintaining public safety.

IoT devices typically employ a number of isolated and trusted components on their processers that are called Root of Trust (RoT). Often proprietary, they're spread across hardware, firmware, and software elements, performing specific critical functions. This creates inconsistency. As the SIM or eSIM or iSIM benefit from GSMA's defined and widely accepted standards, the industry has declared the SIM to be the most secure root-of-trust for IoT.

REMEMBER

For security of a datastream, it's important to have the assurance that the data is from the device it should be from, is secure when it was generated, and stayed secure during transmission. In other words, it can be trusted and is from an authenticated device. The GSMA has defined a standard that centers around the SIM, and uses time-tested secure communication protocols used on the Internet as best practice to help networks know that data coming in from a device is secure and can stay secure until it reaches the cloud. This has been termed IoT SAFE (IoT SIM Applet For Secure End-2-End Communication).

IoT SAFE meets the needs of IoT security for all SIM form factors: SIM, eSIM, and iSIM. But if you want to maximize IoT security, it makes most sense to bake that RoT directly into the the System on Chip (SoC), where it's integrated into the heart of a device's capabilities from the beginning. iSIM takes IoT SAFE further than any other SIM form factor as its existence in a device can be relied upon. An iSIM's security already offers industry-recognized levels of protection of network and subscriber credentials that are built-in from point of manufacture.

Enabling a Broad Ecosystem

Most experts expect a huge growth in cellular IoT. All these devices will need secure authentication, connectivity, and usually remote management capabilities. Establishing trust and interoperability in this technology will help to ensure broad and varied ecosystems.

Here are just a few examples of the vertical sectors that will benefit from the eSIM and iSIM ecosystem growth:

- **Asset tracking:** The new technology can allow more control, simplify logistics, and lower tracking costs.
- **Healthcare:** Wearable health monitoring devices need high reliability, connectivity failover, and an efficient level of redundancy to allow patients' conditions to be carefully tracked and acted upon quickly in an emergency.
- **Other industries:** Various types of sensors provide vital information via cellular connections. In each case, the needs will vary according to the criticality of the information.

In addition, the broader ecosystem will bring many new ways to offer value-added services. These services will leverage cellular connectivity and secure identity verification. For example, consider the following:

- **Smart energy:** Utility providers can use new devices to offer dynamic pricing, real-time billing, and real-time access to connected devices for remote monitoring, analysis, and control of usage.
- **Banking:** Financial institutions can use cellularly enabled verification on new devices to authorize any type of financial transaction.
- **Transport providers:** Providers can use new devices to offer targeted information or process payments.

MNOs play an important role in creating this broad ecosystem because they need to offer more targeted plans to cater to the huge variety of new use cases and price points. For example, basic IoT devices won't require a lot of data and likely not a lot of speed. New data plans will be required to accommodate these devices for the market to flourish. This changing landscape also offers new revenue streams for MNOs and unlocks entirely new types of customers who have not been able to take advantage of the combined benefits of cellular networks and SIM technology.

IN THIS CHAPTER

- Ensuring protection of network and subscriber credentials
- Understanding eSIM and iSIM security

Chapter 6
Understanding eSIM and iSIM Adoption That Is Right for You

A key driver for adopting eSIMs and iSIMs is to secure identities and open new digital revenues. This chapter discusses the basics of how identities of IoT devices are secured and what considerations help you find the best solution for your needs.

Looking at Secure Identity

Identity can be defined as a unique combination of attributes that enable you to distinguish one individual or object from all other individuals or objects. For example, to securely board a plane at the airport, you typically need a photo identity document to verify yourself, such as a passport or driving license, and a boarding pass with a name matching that on the ID. Additional means of verifying your identity, such as passwords, usernames, or even two-factor authentication, are commonly used in digital transactions such as online banking.

IoT devices also require identities that can be verified to ensure they are genuine, are trusted, and conform to a specific level of certification. Secure identity is necessary to protect society from bad actors and rogue devices.

Secure identities typically depend on credentials that are at least partially encrypted. Different types of cryptographic schemes are employed depending on the level of security that's needed. Where less security is required, a lightweight symmetric scheme using a single shared key may be sufficient. Where more security is needed, an asymmetric crypto scheme using both public and private keys may be used.

IoT devices often use what's called a *root of trust* where a series of steps must be performed correctly and in order as the device is bootstrapped. (See Chapter 5 for more on root of trust.) If any step fails to produce the proper result, the process fails, and the device's identity won't be verified. This failure prevents the device from continuing to function in possibly inappropriate ways. This method of verifying that the device has not been tampered with is sometimes called *trusted boot* or *secure boot*.

Simple IoT devices that have limited resources may use tuned protocols such as LWM2M (Light Weight Machine to Machine) protocol to authenticate the device identity. This is a method that uses very small amounts of data to communicate the necessary information.

Regardless of the methods used, establishing a secure identity is as vital for IoT devices as it is for individuals.

Protecting Credentials

To handle and manage network operators' secure identity credentials outside the operator network, you need a solution that does the following:

- Secures a high level of protection of subscription credentials
- Delivers a robust on-card software security environment that persists the protection and security of the subscriber's identity, network authentication credentials, and profile content
- Provides services designed to address the security challenges of managing highly sensitive data

- Operates from a highly secured data center fully certified by GSMA
- Uses a security-by-design approach

Seeing How eSIMs and iSIMs Provide Security

For years, SIM cards have provided a robust, trusted, and highly tested mechanism for secure identity for mobile phones and other cellular connected devices. MNOs have provided SIMs as the means of authenticating users for network access.

The evolution of the eSIM and iSIM form factors is essential for providing secure identity to cellular IoT devices.

As mentioned in Chapter 1, eSIMs and iSIMs are based on the UICC smart card technology used in things like bank cards. In the case of the Kigen iSIM, the combination of the specially designed secure Kigen operating system and a *secure enclave* ensures that the secure identity remains protected, and the authentication can be trusted by the subscribers, device manufacturers, and MNOs.

Because RSP capable eSIM must be interoperable and may store profiles from various operators, GSMA has enforced a product certification program. All eSIMs and iSIMs products issued on the market must be certified by the GSMA. This ensures both functional and security compliance for the eSIM. It is worth noting that while the security level of traditional SIM cards may differ from one operator to another, the GSMA eSIM compliance program ensures consistent adoption of the highest security standards.

REMEMBER

Even though eSIMs and iSIMs are not physically replaceable, they provide the same secure identity services as the removable SIM cards while reducing per-unit cost.

How should you choose what is right for your adoption? The flowchart in Figure 6-1 can help you make a decision. You can also find this flowchart at `https://kigen.com/wp-content/uploads/2021/07/KIG004_SIM_and_RSP_Infographic_updated-v3-2.pdf`.

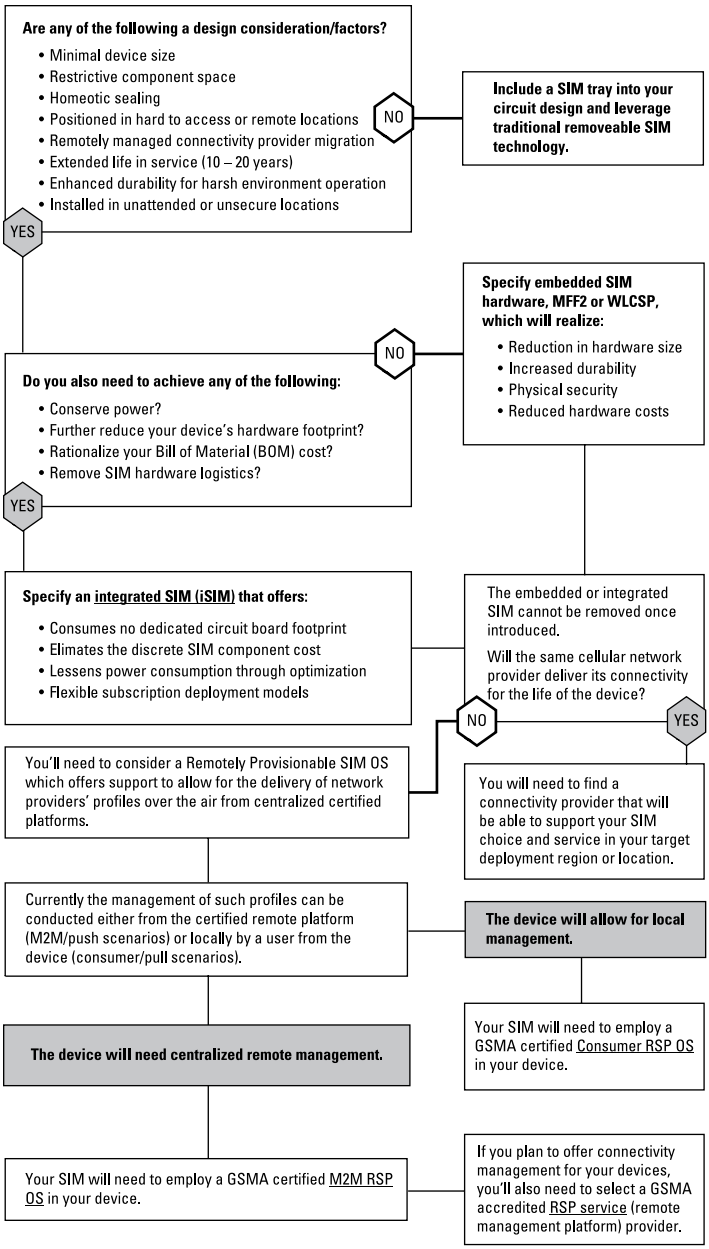

FIGURE 6-1: Key steps and considerations in choosing eSIM/iSIM fit for your needs.

IN THIS CHAPTER

- Reviewing some important points
- Understanding eSIM/iSIM advantages

Chapter 7
Ten Takeaways

This chapter provides a reminder of some of the most important points you should take away from this book:

- **eSIMs and iSIMs are not just for smartphones.** They enable scalable and secure global connectivity, which makes them perfect for IoT deployment.
- **eSIMs and iSIMs are capable of being remotely provisioned, opening a whole raft of value-adds.** The key use cases will be in areas where connectivity is required for multi-region, ultra-reliable, and secure applications.
- **Everybody will benefit.** The benefits for device and chipset makers, enterprises, and end-users include: simplifying manufacturing and supply chain, cost reductions, durability, flexibility, differentiation possibilities, and a better customer experience. MNOs will also benefit from tapping into a wider IoT base.
- **iSIM provides more reliability, size reduction, and cost reduction.** It is part of the chip, uses lower power, and offers even further procurement simplification.
- **RSP technology must offer the required interoperability.** Every RSP provider should ensure its products are assessed and validated to interact correctly within the controlled ecosystem.

- **eSIM and iSIM are relatively new to the market, so standardizing the entire ecosystem is key to its adoption.** Interoperability and security specifications from GSMA help ensure a truly standardized solution.
- **Standards on eSIM and iSIM are ready.** It is possible to maximize interoperability by conforming to GSMA's eSIM specifications. These standards also find a common approach that supports eSIMs and iSIMs and it is possible to already certify using these defined standards.
- **eSIM and iSIM provide an industry-recognized level of security.** These technologies help protect customer details and guard against attacks.
- **Secure identity is an important feature provided by eSIM and iSIM.**
- **Even if you have no prior experience of cellular product design, eSIM and iSIM adoption can be made easier with an ecosystem approach.** If you have been developing with Wi-Fi, Bluetooth, and Long Range Area network (LoRA) in the past, cellular capabilities can bring robust and global wide area connectivity.

Glossary

cellular chipset: A chip that performs a set of functions for cellular communication.

cellular IoT device: A device that communicates over cellular networks.

eSIM (embedded SIM): A physical non-removable SIM that is soldered into a device. Also, an ability to store and remotely switch multiple profiles on a SIM. Used interchangeably with *eUICC.*

eUICC: A SIM supporting the GSMA Remote SIM Provisioning specification; may be built using any form factor. Used interchangeably with *eSIM*.

FF (form factor): The size and/or form of a SIM.

iSIM (integrated SIM): eUICC software that runs in a dedicated secure enclave in a SoC to provide remote SIM provisioning capability.

iTRE (integrated tamper resistant element): A dedicated secure processor integrated in a SoC.

LoRA (long range area networks): Another wireless technology used in IoT transmissions up to 9km for uplink.

OTA (over the air): Without physical handling.

profile: A network operator profile. A combination of file structure, data, and applications stored on a SIM/UICC to enable network access.

RSP (remote SIM provisioning): The process of managing and delivering profiles on an eSIM securely and remotely.

security enclave: The dedicated secure area and processing in an iSIM that stores encrypted identity.

secure identity: Online authentication and digital signatures where the SIM/UICC works as an identity tool for the cellular network connection.

service provider: An organization that provides subscriptions or aggregates network services to customers but does not own the mobile network.

SIM (subscriber identity module): The removable card in cellular devices. It has a secure element that stores security data enabling network access.

SoC (system on a chip): A microchip with all the necessary electronic circuits and parts for a given system.

subscription: A contract between the mobile network operator and customer.

subscription manager: An entity that brokers or aggregates subscriptions from several service providers and offers a single interface to another party.

TRE (tamper resistant element): A dedicated secure processor in its own dedicated package.

UICC: A smart card that ensures the integrity of user identity data and runs a SIM application.

UICC application: An application residing on a UICC; for example, the SIM application.

Adopt eSim and iSim for your digital transformation

With accelerating development of Internet of Things and other connected devices, manufacturers face a growing need to replace the standard subscriber identity module (SIM) with something smaller, more versatile, and more efficient. This book introduces *embedded SIMs (eSIMs)* and *integrated SIMs (iSIMs),* two new forms of SIM that provide the services of traditional SIMs while offering enhanced security, reduced size, and remote provisioning (RSP) capabilities.

Inside...

- Explore new SIM technology
- Check out eSIM/iSIM benefits
- Understand remote provisioning of SIMs
- Identify emerging markets
- Ensure interoperability
- Provide secure identity
- Futureproof your design choices

Kigen

Brian Underdahl is a well-known author and technologist who enjoys making complicated topics easy for ordinary people to understand. **Loic Bonvarlet** is the VP of Product and Marketing at Kigen. **Patrick Biget** is the VP of Engineering at Kigen. **Jean-Philippe Betoin** is the VP of Business Development at Kigen.

Go to Dummies.com®
for videos, step-by-step photos, how-to articles, or to shop!

ISBN: 978-1-394-15502-6
Not For Resale

for dummies®
A Wiley Brand

WILEY END USER LICENSE AGREEMENT

Go to www.wiley.com/go/eula to access Wiley’s ebook EULA.