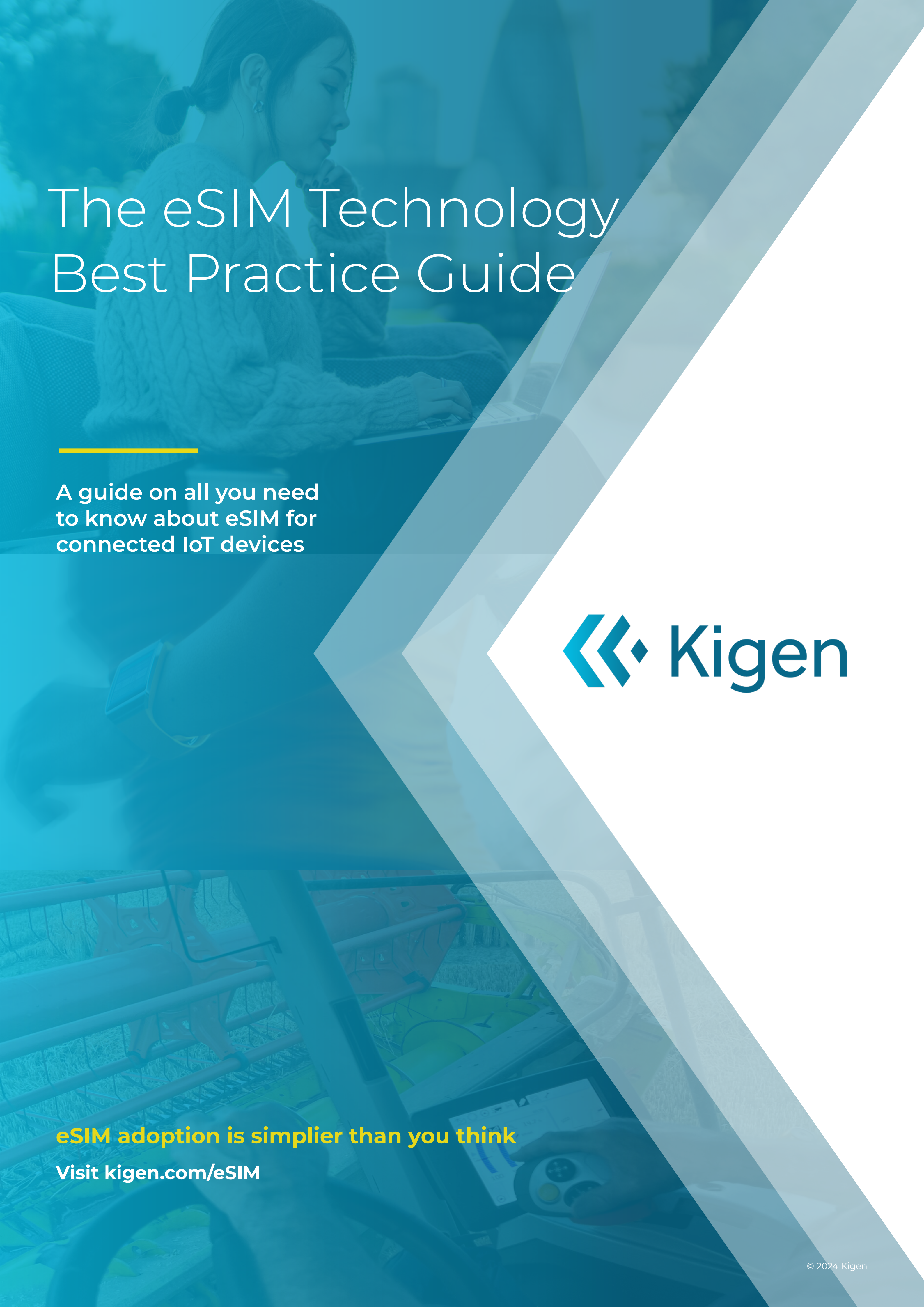


The eSIM Technology Best Practice Guide

A guide on all you need to know about eSIM for connected IoT devices

Kigen

eSIM adoption is simplier than you think

Visit kigen.com/eSIM

Industry Insight

“Kigen has been ranked among the top eSIM enablement, provisioning, and orchestration players. Most recently, it has been featured in Counterpoint’s CORE eSIM landscape, which includes the ‘capability’ parameter, which covers criteria such as firmware, compliance, interoperability, and supply chain process.”

- Ankit Malhotra, Senior Research Analyst at Counterpoint Research

Contents

Executive Summary

By 2030, nearly 70% of all cellular devices shipped will be eSIM/iSIM capable driven by smartphones and cellular IoT modules. **eSIM/iSIM-capable devices are expected to grow at a CAGR of 22% between 2024 and 2030.**

eSIM technology enhances connectivity and security in IoT devices whilst streamlining the logistics and manufacturing processes of IoT products. IoT applications such as utility meters, asset tracking, logistics, and consumer devices are rapidly expanding. The growth of connected devices can be attributed to the advancements in new technologies like LPWA and 5G combined with recent industry specifications, which provide increased flexibility and scalability for IoT deployments.

We are witnessing the development of increasingly rich functionality focused on extracting significant value from connected devices and the data they transmit. Examples of this rich functionality include cloud and edge computing, machine learning, and mobile private networks, which are empowering new business models. This advancement presents opportunities for stakeholders in the IoT ecosystem to innovate and capitalize on new revenue streams.

This guide is designed to give business stakeholders a comprehensive overview of eSIM technology including how to implement, deploy, and manage eSIM-enabled devices.

The IoT ecosystem addressed in this guide:

- Secure IC vendors, module and chipset providers
- Mobile network operators (MNOs) and mobile virtual network operators (MVNOS)
- Manufacturers of IoT devices, modules and consumer devices
- End users and enterprises

C1 - eSIM Technology Fundamentals

The growth of IoT applications across business sectors

The growth in adoption of connected IoT devices that collect data is due to the improved operational efficiencies and customer experiences they deliver across various sectors, including logistics, transport, energy, smart cities, healthcare, and manufacturing.

As IoT devices become more compact, reducing power consumption is critical to the design process. It is also vital to keep the devices and their data securely managed in the field in an economically scalable manner. eSIM technology can achieve this affordably and open the benefits of global and secure connectivity.

eSIM capable IoT devices for consumers

Creating a set of specifications for consumer devices has become vital as small companion devices, like smartwatches, continue to gain importance. The existing IoT architecture was adopted for specific consumer scenarios and begins with a contract between the device user and network service provider.

Once established, the eSIM installs MNO/carrier profiles on a consumer's smartphone, tablet, or laptop. In this scenario, the end-user receives a QR code to download the MNO profile, which triggers the download of the subscription data (ICCID, IMSI) to the eSIM. One primary use case of the consumer eSIM is travel, where local operator profiles can be purchased in the destination country to avoid excess roaming fees.

How does eSIM technology benefit MNOS?

- **Digitalization:** With services such as SM-DS, MNOs can seamlessly migrate their customers to eSIM and drive the digitalization of the Telecoms industry. The SM-DS provides a universal and fully digital user experience, where the eSIM can automatically query the SM-DS server for any MNO profile that has been allocated for the device. eSIM mitigates user intervention and MNO overheads, though QR codes and customer support are necessary.

- **Reduced costs:** For eSIM devices, MNOs will eliminate the distribution and inventory practices associated with traditional SIM cards. They 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 eSIM will enable MNOs to capitalize on the broader adoption of cellular IoT devices by serving already deployed devices that previously would have been permanently attached to another MNO, thus increasing revenue opportunities.

- **Maintain security:** Complying with 3GPP standards ensures subscriber privacy and network security and achieves interoperability for all SIM/eSIM of a particular release.

How does eSIM technology benefit original equipment manufacturers?

- **Reduces supply chain complexities and costs:** The number of global product variants is reduced because multiple SKUs for different networks worldwide no longer need to be implemented, leading to cost reductions.

- **Control over connectivity and better customer experience:** Device makers will have significantly more influence over their device connectivity and may offer connectivity for free or as global data packs.

- **Product improvement:** The new technology frees space on the device PCB.

- **Differentiation and capitalizing on IoT growth:** Incorporating eSIMs 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.

How does eSIM technology benefit enterprises?

The emerging IoT marketplace enables more innovation and faster access to information. By including eSIM or iSIM in an IoT device, an enterprise can realize 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 SIM theft or damage from vibration, spoilage and extreme temperature are eliminated.

- **Futureproofed investment in IoT:** Enterprises can commit to IoT deployments with confidence that they can easily manage their IoT device connectivity remotely globally.

Introducing eSIM security for connected devices

To help recognize the full benefits and capabilities of eSIM (the term originating from “embedded SIM”), it is helpful first to introduce and define the SIM technologies that have evolved over the last 30 years, both in terms of form factor and functionality.

What are sim form factors and specifications?

- **SIM (Subscriber Identity Module)** is a generic term for all form factors and features. Originally, SIM was the 2G application inside the Universal Integrated Circuit Card or UICC. People use the word SIM card to refer to UICC, which ETSI standardizes.

- **SIM cards** are made from plastic and devices must include a slot/tray into which they are inserted. They can come in various grades (Consumer, Industrial, Automotive) and sizes (4FF or Nano, 3FF or Micro, 2FF or Mini, where FF stands for form factor).

- **eSIM** is a separate component usually soldered onto the device board (it is possible to have removable eSIM in some cases), eliminating the tray assembly from the Bill of Materials (BOM). Due to being solderable, they come in various sizes (MFF2, USON, WLCSP). They are often called ‘solderable’ SIMs and are typically delivered in reels, ready for PCB assembly. As for the SIM card, people use eSIM to refer to the embedded Universal Integrated Circuit Card (eUICC), the technical name for the component. eUICC is standardized by GSMA.

C2 - Managing eSIM Subscriptions on Networks

The capabilities and functionality of the eSIM

A mobile network subscription is embodied in a profile containing a file system with network configuration parameters, identifiers, and corresponding authentication credentials to authenticate the subscription to the mobile network. Moreover, some applications are optionally defined by the connectivity provider: the SIM stores operator profiles, files, applications and sensitive data. It is important to note that the SIM form factor can be developed to provide either UICC or eUICC capabilities.

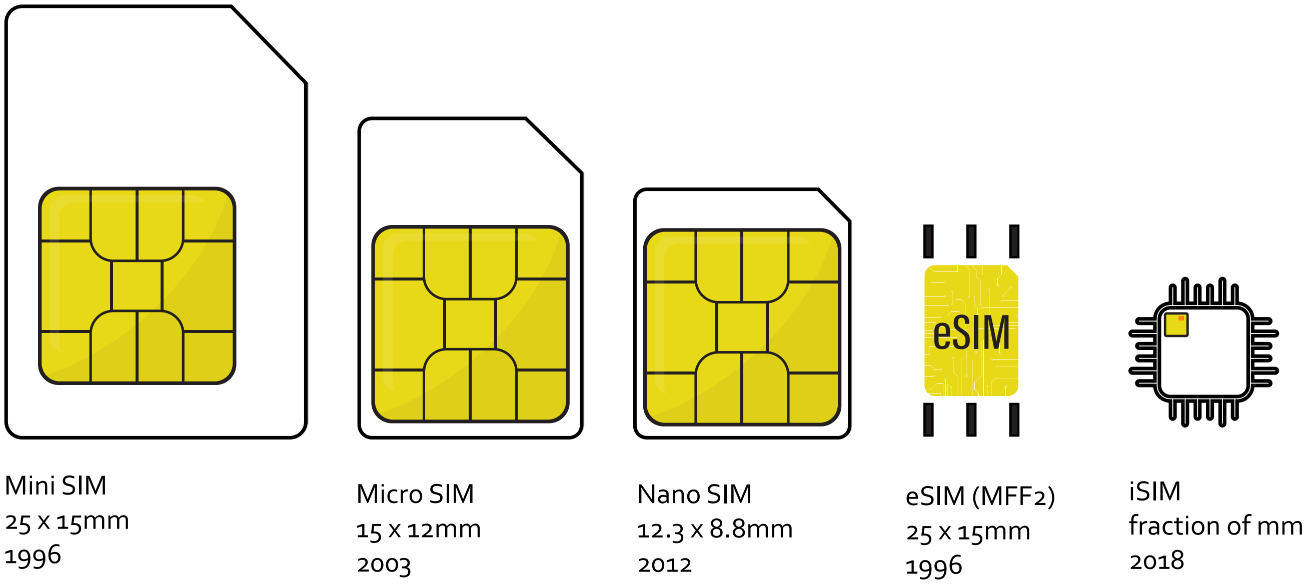
When clarifying the capabilities and functionality of a SIM, the variants of the term UICC (Universal Integrated Circuit Card) are used:

- **UICC** refers to a SIM card permanently locked to a specific M(V)NO by hosting only one profile. The term was introduced during 3G standardization to denote the multi-application support for both SIM (2G) and USIM (>3G) applications within the same physical card.

- **eUICC** refers to a UICC that can be changed from one MNO subscription to another in the field (also known as the eSIM feature) and uses a Subscription Management infrastructure commonly referred to as RSP (Remote SIM Provisioning).

What are subscriber identity modules or SIMs for?

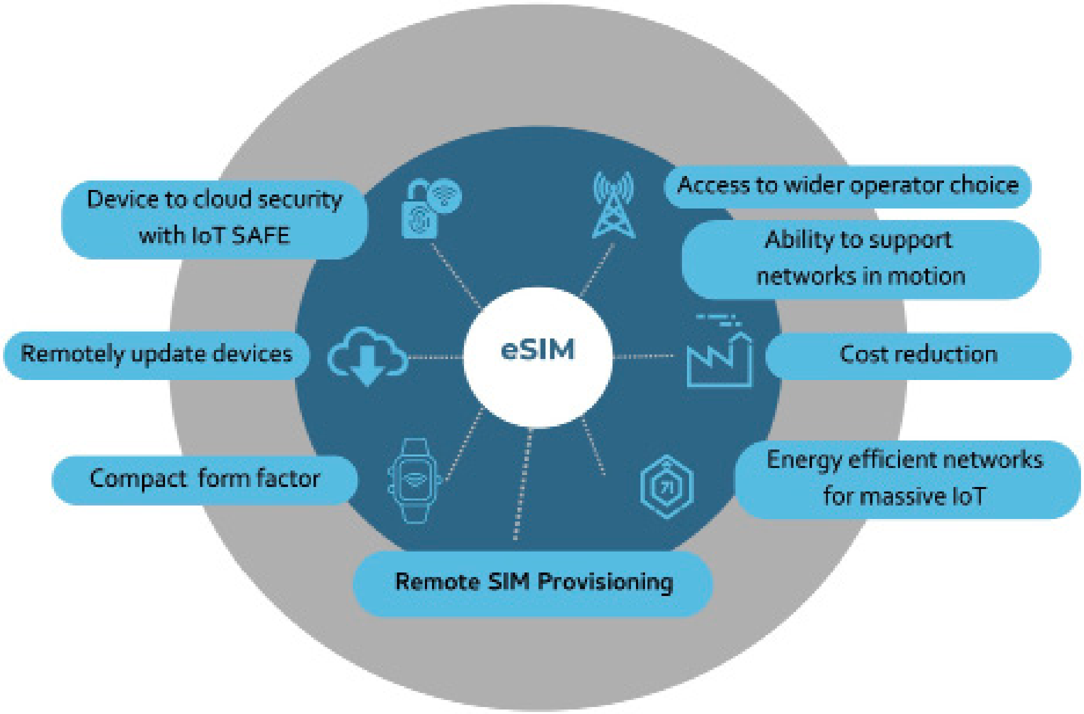
SIMs have shrunk from the original plastic card 1FF to 2FF (Mini-SIM), 3FF (Micro SIM), and finally 4FF (Nano-SIM) as per the visual below. All modern SIMs are built on smart card (UICC) technology regardless of the packaging. The (e)UICC is a secure computing device that contains memory and provides cryptographic and identification services. Traditional SIM cards have the operator-defined profile programmed during manufacture.



Store profiles securely on the device

eSIM is soldered into IoT devices and can incorporate new functionality to enable IoT devices across multiple applications such as smart meters, tracking devices, e-bikes, and smartwatches. It is an evolution of the SIM card and was conceived to - the limitations of traditional physical SIMs. The eUICC was designed using the MFF2 smaller format to ease integrations into more compact IoT devices.

IoT devices with an eSIM can be adjusted to gain the best network service within the limits of its supported radio technology.


Device to cloud security with IoT SAFE
Access to wider operator choice
Ability to support networks in motion
Remotely update devices
eSIM
Cost reduction
Compact form factor
Energy efficient networks for massive IoT
Remote SIM Provisioning

eSIM IoT subscription management

IoT devices can switch connectivity through subscription management functionality, which prevents connectivity lock-in for the IoT service provider. The IoT eSIM should always have an active profile and an initial profile must be present on the eSIM during production. This initial profile can be the final provisioning profile, also known as the bootstrap profile, and should be able to download an operational profile once the device is active.

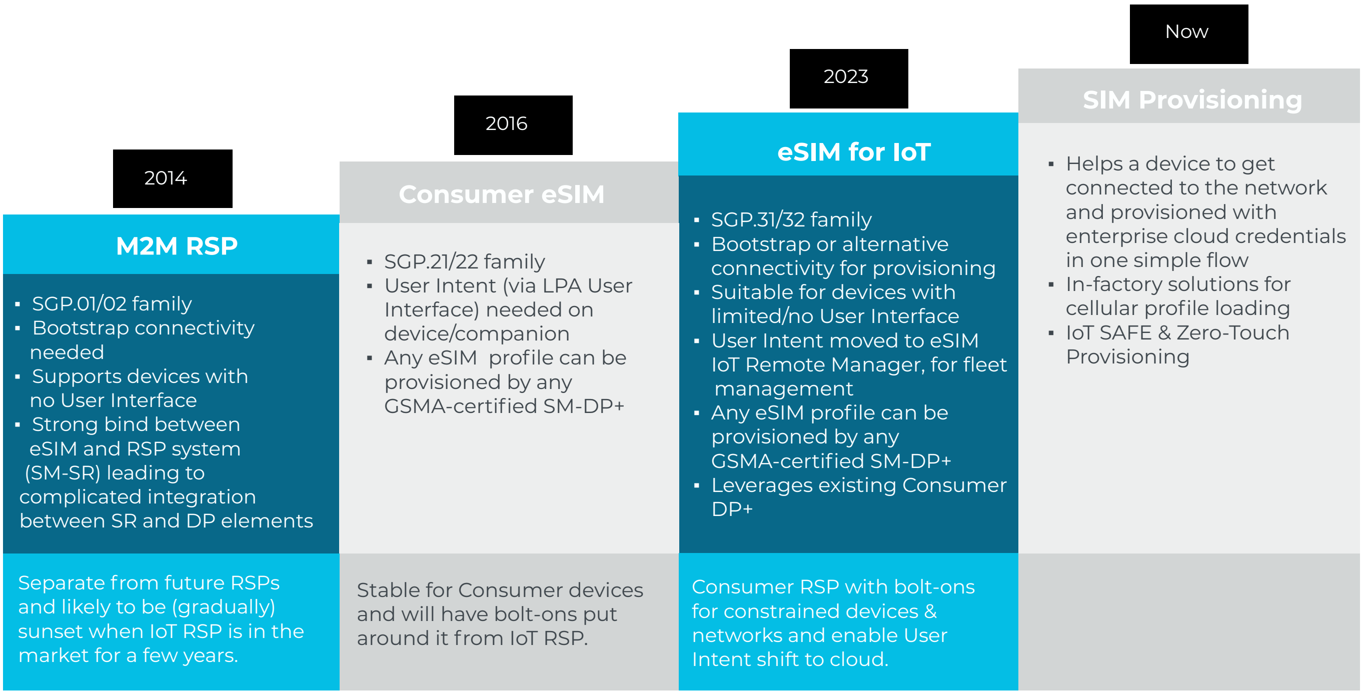
Advantages of eUICC form factor and functionality

Criteria	With eUICC form factor and functionality	Without eUICC form factor and functionality
Size	eSIMs are about half the size of Nano SIMs and fit into small devices.	Larger, requires a physical slot in the device.
Flexibility	Can store multiple carrier profiles; easy to switch carriers remotely.	Supports only one carrier profile at a time; requires physical swapping for changes.
Durability	Increased durability as users can't reach eSIMs to damage or lose them.	More prone to damage and wear due to physical handling.
Provisioning	Remote provisioning and management of carrier profiles.	Manual insertion and removal for provisioning.
Environmental Resistance	Better resistance to harsh conditions due to embedded design.	More exposed to environmental factors due to physical slots.
Cost Efficiency	Reduce cost of device as supply chain and management costs are optimized.	May incur additional costs for physical SIM cards and swapping.
Security	Enhanced security features due to integrated design and remote management.	Physical security depends on the device's SIM slot design.
Connectivity	Networks can be switched remotely worldwide for continuous coverage.	SIM cards need to be swapped for switching networks.

C3 - eSIM Management Architecture

Remote SIM provisioning (RSP) for Consumer and M2M eSIM

The main distinction between Consumer and M2M eSIM is the activation process to connect to the network. While Consumer eSIM can be activated remotely, M2M eSIM usually comes with preloaded network profiles. This enables fast and simple deployment of devices on specific networks, streamlining the setup process for large-scale M2M deployments.



2014

M2M RSP

- SGP.01/02 family
- Bootstrap connectivity needed
- Supports devices with no User Interface
- Strong bind between eSIM and RSP system (SM-SR) leading to complicated integration between SR and DP elements

Separate from future RSPs and likely to be (gradually) sunset when IoT RSP is in the market for a few years.

2016

Consumer eSIM

- SGP.21/22 family
- User Intent (via LPA User Interface) needed on device/companion
- Any eSIM profile can be provisioned by any GSMA-certified SM-DP+

Stable for Consumer devices and will have bolt-ons put around it from IoT RSP.

2023

eSIM for IoT

- SGP.31/32 family
- Bootstrap or alternative connectivity for provisioning
- Suitable for devices with limited/no User Interface
- User Intent moved to eSIM IoT Remote Manager, for fleet management
- Any eSIM profile can be provisioned by any GSMA-certified SM-DP+
- Leverages existing Consumer DP+

Consumer RSP with bolt-ons for constrained devices & networks and enable User Intent shift to cloud.

Now

SIM Provisioning

- Helps a device to get connected to the network and provisioned with enterprise cloud credentials in one simple flow
- In-factory solutions for cellular profile loading
- IoT SAFE & Zero-Touch Provisioning

The mobile operator profile is programmed in the chip's memory to connect the SIM to a cellular network. IoT devices require cellular connections and remote SIM provisioning (RSP) is the method of in-field installation of operator profiles and switching profiles over the air (OTA), which changes the eSIM primary cellular carrier remotely.

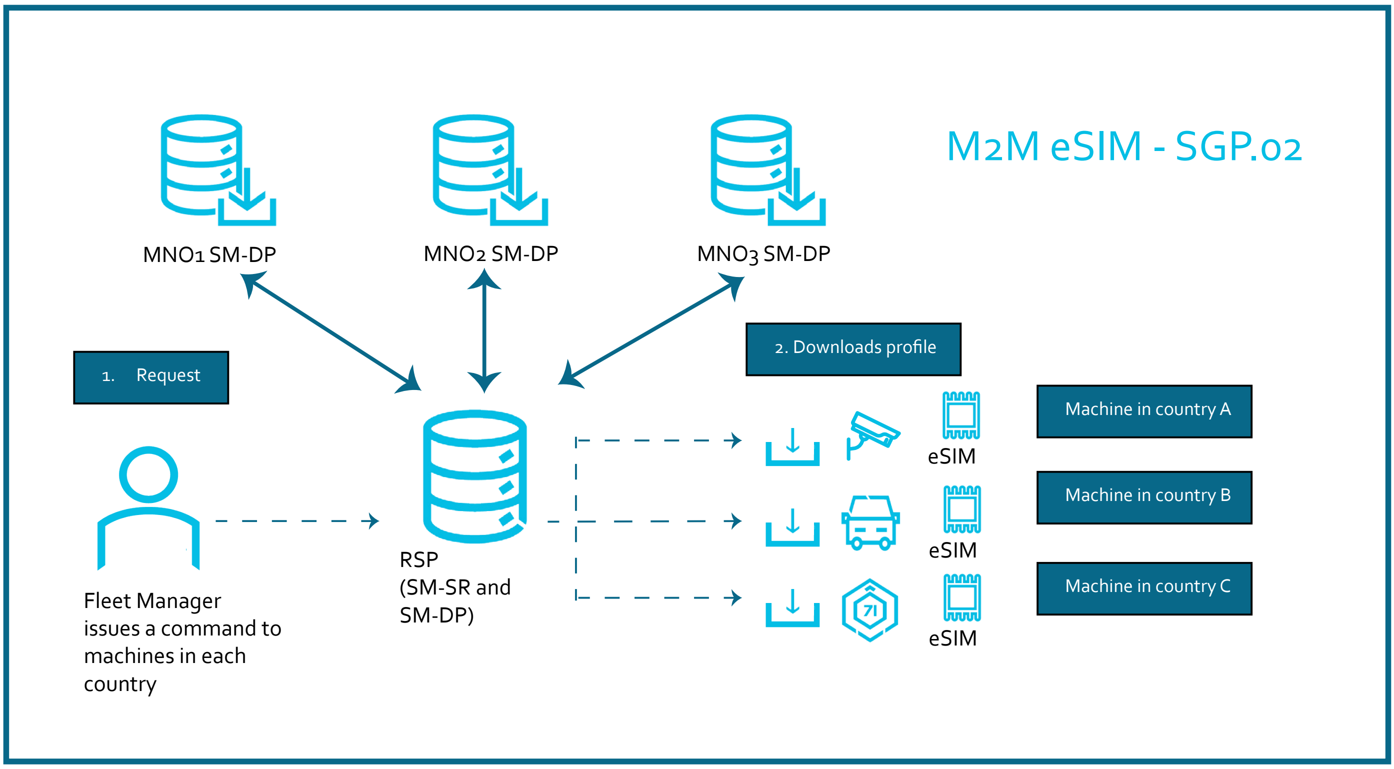
As a result, as soon as the IoT device is turned on, it connects to a local cellular network, and it can be provisioned securely over the air, across the globe, and over the device's entire lifetime. Subsequently, this makes the device ready to use immediately, regardless of location.

The RSP capability allows for remote connectivity lifecycle management of fleets of IoT devices, where individual physical connectivity management (e.g., change of physical SIM) can be costly due to production scale or device inaccessibility. The embedded Universal Integrated Circuit Card (eUICC) is a SIM component that allows a carrier to add a new SIM profile.

C4 - Moving to eSIM for IoT with SGP.32 standard

M2M eSIM – SGP.02

Download SIM profile by push mechanism to device



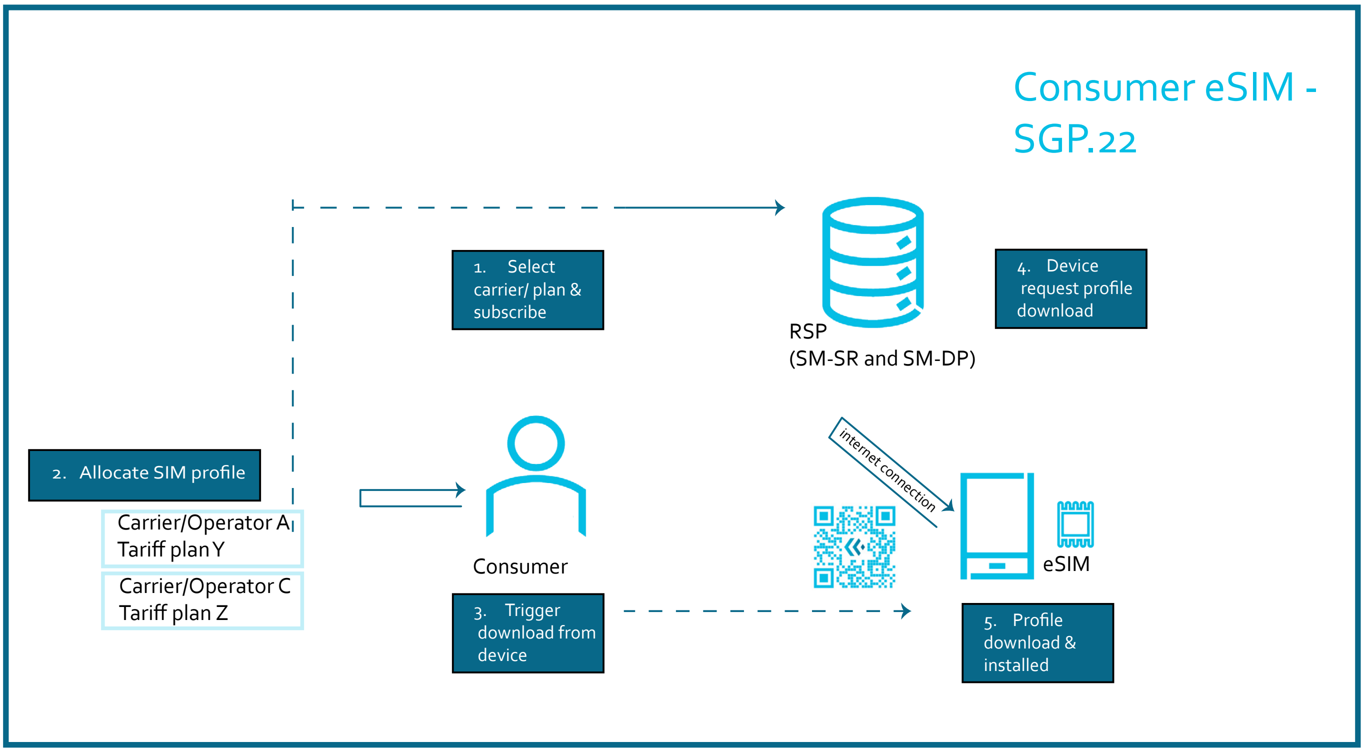
- Complex integrations for profile, not suitable for constrained devices on LPWAN networks (CAT-M, NB-IoT)

- **Subscription Manager-Data Preparation (SM-DP)** stores, protects and makes profiles available for download onto the M2M eSIM.

- **Subscription Manager-Secure Routing (SM-SR):** manages the lifecycle of the profiles on the eSIM and secures the communication between the eSIM and RSP. It is responsible for routing the profile downloads that the SM-SR retrieves from the SM-DP.

Consumer eSIM – SGP.22

Pulls the profile from the SM-DP+ and can be triggered with a QR code or application.

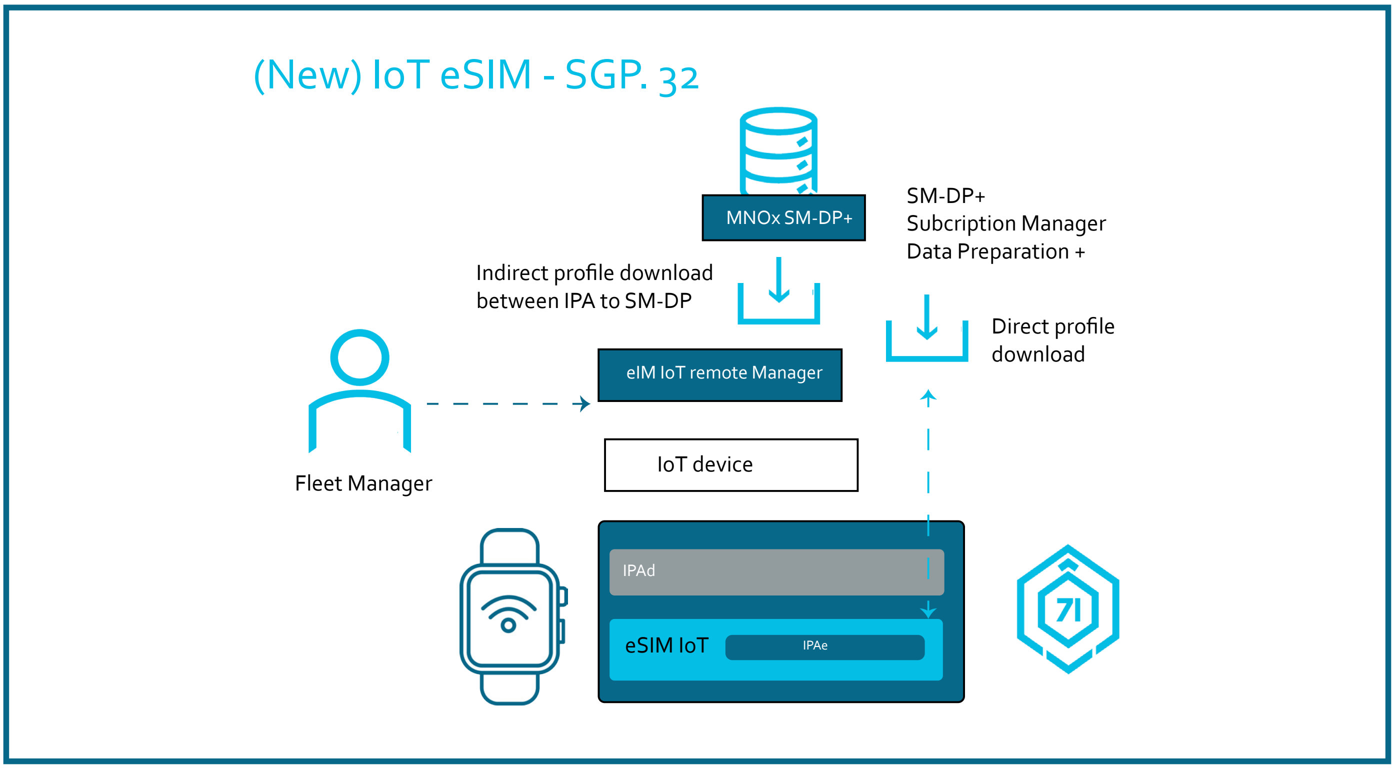


- Not suitable for IoT. Requires screen or camera type capabilities on devices, and triggered by user intervention.

eSIM for IoT based on the GSMA's SGP.31/.32 specification

A third RSP model is eSIM for IoT, which will be defined in GSMA's SGP.31 and SGP.32 specification families. The eSIM IoT remote provisioning solution complements the consumer RSP solution, which evolved from the original architecture for M2M. This option introduces a capability for device fleet owners to remotely manage and switch connectivity profiles without human on-device intervention.

The updated eSIM specifications are designed to future-proof IoT products and streamline connectivity for manufacturers and end-users. When procuring eSIM modules for newly developed products, verifying that they comply with SGP.32 specifications is essential. Of course, there are many IoT connectivity providers, but few offer full-spectrum RSP services, complete with GSMA-compliant profile management and hosting.



Given the constrained or unmanned nature of many IoT devices, the IoT RSP added the eSIM IoT Remote Manager (eIM) component to reintroduce a remote push capability for device owner profile management independent of the carrier / SM-DP+. Meanwhile, the eIM allows remote profile management and acts as a communication proxy to broker profile delivery from the SM-DP+, essential to network-constrained devices.

The benefit of using eSIM for IoT compared to the M2M model is that it avoids tying a device to one SM-SR, which can limit profile availability or require a costly integration. SGP.32 is an essential specification for OEMs, mobile network operators, and enterprises, as it aids interoperability across different devices and networks. To discover more on how to leverage SGP. 32, see our eSIM in transition article for OEMs.

C5 - eSIM Root of Trust for Data

Addressing end-to-end data security in a standardized manner

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

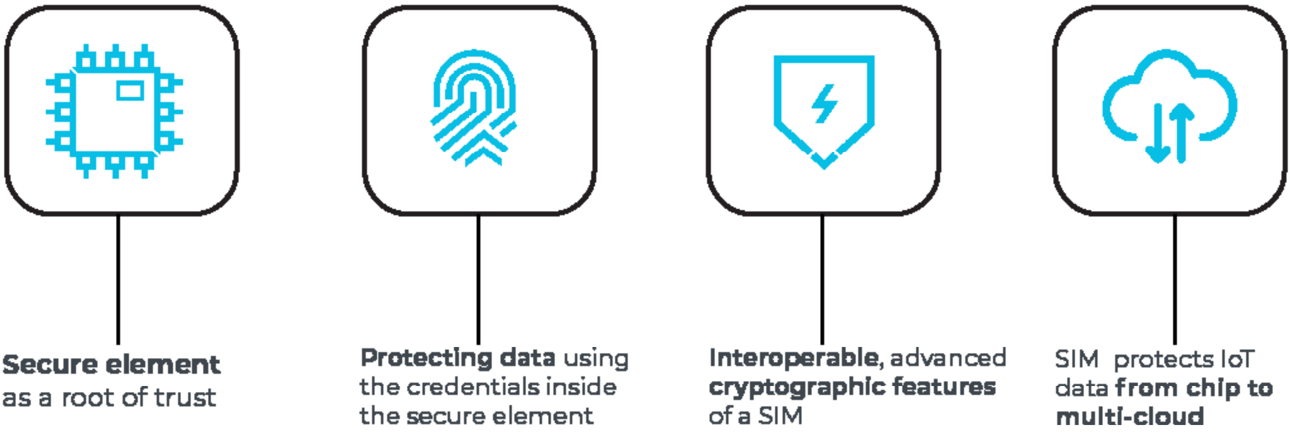
IoT devices typically employ several isolated and trusted components called Root of Trust (RoT) on their processers. Often proprietary, they’re spread across hardware, firmware, and software elements, performing specific critical functions. This creates inconsistency.

What is IoT SAFE Standard and why is it essential for devices?

As the name suggests, IoT SAFE is for the security of the data stream; it’s essential to have the assurance that the data is from the device it should be from, is secure when it was generated and stays 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 till 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 we’re looking to maximize IoT security, it makes the most sense to bake that Root of Trust (RoT) directly into the System on Chip (SoC), which integrates into the heart of a device’s capabilities.

98% Enterprises want end to end solutions that protect data from place of colleciton, to cloud. - *GSMA Intelligence, Dec 2020*



Secure element as a root of trust

Protecting data using the credentials inside the secure element

Interoperable, advanced **cryptographic features** of a SIM

SIM protects IoT data **from chip to multi-cloud**

Secure device identity with cryptography

IoT devices require verified identities to ensure they are genuine, trusted, and conform to a specific level of certification.

Secure identities typically depend on partially encrypted credentials. Different types of cryptographic schemes are employed depending on the security level needed and a lightweight symmetric scheme using a single shared key may be sufficient where less security is required.

A root of trust is often used for IoT devices where steps must be performed in a certain order. If any step fails to produce the expected result, the process fails, and the device's identity won't be verified. This failure prevents the device from continuing to function in a manner that could pose a security risk. Simple IoT devices with limited resources may use the LWM2M (Light Weight Machine to Machine) protocol to authenticate the device identity. This method uses small amounts of data to communicate the necessary information.

C6 - eSIM implementation for Enterprise Needs

What is a multi-profile SIM card?

The multi-profile SIM allows devices with a single eSIM chip to have multiple SIM profiles and connect to various carriers and locations. A traditional SIM usually contains only one profile, matching only one mobile network carrier. Device manufacturers must work with SoC vendors and eSIM chipset vendors to integrate this feature on their devices. Using multiple profile SIMs can be complex as the device user must negotiate with each mobile network operator. It is increasingly discouraged but popular for certain scenarios.

What is multi-IMSI?

This is when several IMSIs (subscriptions) from different mobile network operators are stored on one SIM card (or single eSIM profile). The user does not need to change SIM card (or eSIM profile) to switch from one IMSI to another. This technology is beneficial when the coverage of the primary network provider is inadequate, as it enables the device user to benefit from roaming services for optimum cellular connectivity. Unlike eSIM, it doesn't implement a complete network operator profile, can encounter connectivity issues, and is not future-proofed.

Criteria	eUICC	Multi-IMSI	eUICC with Multi-IMSI Profile (s)
Form factors (2/3/4 FF, MF22, integrated)	✓	✓	✓
Number of profiles	Multiple	Profile with pre-loaded IMSIs ONLY	Multiple with one being a Multi-IMSI profile
New MNO Profile Download	Via RSP	✕	✓
IMSI switch	✕ Profile change	✓	✓
New IMSI download	Via profile download using RSP	Via OTA if the SIM owner has IMSI loaded on their core network and network keys are already on the SIM	Via profile Download using RSP or if SIM owner adds new IMSI to their core network and IMSI/K is already included in profile
Costs	Profile generation and download fee	Cost of hosting IMSIs on core network. Recurring OTA subscription fees for multi-IMSI management	Recurring OTA subscription and/or profile generation with download fee
Flexibility	Medium	Medium/Low	High
Interoperability	GSMA standard based	Multi-IMSI application is interoperable for IMSIs hosted on SIM providers core network.	Combination of both
Coverage	Able to switch to any RSP supporting global network	Limited to regions for which IMSIs are pre-loaded	SImilar to eUICC

Roaming with eSIM

Unlike traditional SIM cards, eSIMs are embedded directly into the device during manufacturing, eliminating the need to swap cards physically. eSIM remotely manages carrier profiles and allows IoT devices to conform to local regulations without physically exchanging SIM cards.
This digital flexibility ensures devices can stay connected and adhere to legal compliance anywhere in the world.

Compliant solutions for evolving mobile data regulations

Turkey has specific requirements for local cellular connectivity. Permanent roaming is impossible, and IP data must be routed locally within the country. Businesses deploying IoT devices with eSIM in Turkey must engage with one or more local mobile network operators to ensure coverage and continuous connectivity.

In this case, multiple production lines are required, which increases manufacturing costs. For this reason, floLIVE, Kigen, and Protahub have partnered up to make local IoT cellular connectivity possible in Turkey by managing the local eSIM subscription profile. OEMs can use a single SKU, which eases the logistics and supply chain. Read the article for more on continuous IoT coverage for OEMs in Turkey.

Continuous connectivity with non-terrestrial networks (NTN)

Implementing satellite connectivity establishes a non-terrestrial network (NTN) ecosystem following the 3rd Generation Partnership Project (3GPP) specifications. This system facilitates the seamless integration of terrestrial and satellite systems on a single mobile platform. NTN facilitates a smooth transition between cellular and satellite connectivity for IoT devices, necessitating continual cellular access.

Combining cellular and non-terrestrial networks (NTN) or satellite connectivity is highly advantageous for devices used in remote and challenging environments where relying solely on terrestrial cellular networks can present significant challenges. Kigen's secure OS is being used to ensure connectivity to power rugged devices worldwide so users can use their smartphones in locations without cellular coverage. See our partnership with Ulefone and Skylo's NTN connectivity.

C7 - eSIM Provisioning in Factory

Embedded product connectivity in the factory

Product and device makers face challenges related to the growing emphasis on manufacturing process efficiency and increasing requirements for cellular connectivity within IoT devices. Specifically, it is a challenge to provide the correct SIM within the device based on the country in which it will be deployed.

Kigen’s in-factory profile provisioning (IFPP) is designed to meet OEM manufacturing needs by streamlining the process of loading cellular profiles into large batches of connected devices on the factory floor. IFPP reduces the number of SKUs required and simplifies the secure loading of MNO profiles to the embedded SIM (eSIM) based on the device’s geographic destination. It also saves power and cost compared to using a global bootstrap and localizing the device in the field.

Single SKU

In-factory connectivity enablement during order fulfilment means no need to maintain multiple SKUs for different versions of the same product

Reduce the cost of manufacturing, supply, and logistics of the eSIM.

Future Proof

Protection and compliance even when regulations evolve

Ability to change connectivity provider later in field using an eSIM (Remote SIM Provisioning) solution should it be required.

Latency

Can deliver profiles in batch mode, reducing dependence on connectivity

Resiliency against costly outages.

Simplified eSIM Management

Pre-standard but fully aligned to the needs of SGP.32 for remote provisioning and carrier profile swap

IoT devices that monitor moving objects, such as cargo or cold chain storage, require continuous coverage using local connectivity wherever they may be. This has significant benefits for many use cases where devices run on battery power, especially applications using Low-Power Wide-Area (LPWAN) technologies, including NB-IoT, which rely on power efficiency. The production lines of connected cellular devices can be dynamically updated with multiple profiles, streamlining fulfillment and enabling scalability.

In-Factory Profile Provisioning benefits include:

- **Remote UI:** The consumer Local Profile Assistant (LPA) role has been split. It is partially on the device or eSIM, implemented as the IoT Profile Assistant (IPA), and partially hosted by the device fleet owner's chosen eIM(s), allowing for the remote control of the device's connectivity options.

- **Flexible eIM association:** It can happen at eUICC Manufacturing, IoT Device Manufacturing, or in the field to suit the manufacturing process.

- **Support for lightweight protocols:** Raw CoAP normative, Lightweight M2M (LwM2M) informative is an option to manage profile downloads, -SGP.32 does not require support for TCP/IP, which is heavier than the UDP protocol used in CoAP. This helps overcome bandwidth issues familiar with constrained IoT technologies such as NB-IoT and LTE-M.

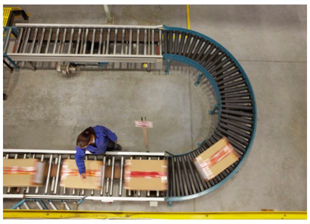
- **Small footprint:** Because some of the functionality of the LPA can be moved into the eIM, the memory and processing requirements on the device itself can be reduced. This aids device operational efficiency and reduces power consumption.

IFPP helps IoT device manufacturers boost efficiency in the production process and enhance the functionality of connected products. Find out more on in-factory profile provisioning.

C8 - Industry Applications for eSIM Devices

The emerging marketplace for cellular connectivity includes thousands of possibilities for organizations in many industries. Establishing trust and interoperability of eSIM-enabled devices will ensure broad and varied use cases. Here are examples of vertical sectors using eSIM devices to enhance operational efficiencies:

Smart Meters: With eSIM technology, cellular networks can transfer data over long distances, using minimal power at a low cost. Smart meter data feeds into the smart grid, allowing utility companies to aggregate and monitor the grid's health remotely and at scale. Smart grid technology uses analytic tools to automate and control utilities' availability across cities. Low Power Wide Area (LPWA) network technologies, such as NB-IoT and LTE-M, allow metering devices to establish cellular connectivity once or twice daily to report data when they don't need constant connectivity.



Shipping and logistics: eSIM technology allows tracked assets to be shipped to any part of the world, and knowing the exact location of goods in real-time during shipment is essential. Cellular M2M modules are desirable in logistics, especially for use on high-value, highly mobile assets. With eSIM technology, service providers can change network profiles from their management console using remote SIM provisioning (RSP). This simplifies logistics and lowers tracking costs.

Automotive: With eSIM technology, fleet operators benefit from fast, reliable, secure cellular connectivity, enabling real-time data. Organizations can use remote diagnostic monitoring services to track their vehicles in real time to monitor driver behavior, fuel consumption, and maintenance schedules. The data from the vehicle sensors enable predictive maintenance and improve how the fleet performs, leading to increased efficiency and cost savings.

Agriculture: eSIM technology has emerged as a crucial application for livestock management. eSIM combined with a non-terrestrial network (NTN) provides a reliable real-time data stream, enabling farmers to manage their livestock more efficiently with features like location tracking, health monitoring, and animal behavior analysis.

Vehicle and asset monitoring: IoT tracking devices use eSIM for cellular network connectivity to maintain perishable items, including sensitive medicines, food, and high-value goods that require specific temperature conditions during transportation. This is possible through networks comprising small, tiny sensors that can be deployed to monitor and regulate factors such as temperature, air quality, humidity, lighting, and pressure. eSIM-enabled chain management solutions provide trustworthy analytics.

Micro-mobility: For journeys less than 15 km, micro-mobility transport means such as e-bikes and e-scooters offer greener ways to travel and make our cities more sustainable. Due to their compact nature and need to maximize battery life between charges, these solutions greatly benefit from eSIM technology.

Smartwatches and Wearables: Consumers increasingly opt for smartwatches with eSIM, which allow users to use them autonomously. They can use their watch to do everything they usually do on the phone without carrying it. For example, users can go jogging and listen to music without needing their smartphone while exercising.

Smartphones : eSIM-enabled smartphones make switching mobile network carriers easier than with traditional SIM cards. Instead of making a trip to a local shop, consumers make the switch on their phones by entering information from their carrier, often by scanning a QR code using the smartphone's camera.

Laptops and tablets: Integrating eSIM technology in laptops and tablets provides seamless connectivity, allowing users to switch between networks and service providers seamlessly.

This flexibility is helpful in remote areas where coverage is unreliable, as the eSIM can be programmed remotely to connect to specific networks.

Conforming to Standards

Interoperability of devices from different manufacturers within an ecosystem of chip makers, module makers, OEMs and network operators is vital to the success of any new technology. It is ensured through the establishment of and conformity with industry-wide standards. Standards also build economies of scale, which drives down costs.

Because RSP-capable eSIMs must be interoperable and may store profiles from various operators, the GSMA has enforced a product certification program. All eSIM products issued on the market must be certified by the GSMA. This ensures both functional and security compliance for the eSIM. While the security level of traditional SIM cards may differ from operator to operator, the GSMA eSIM compliance program forces the adoption of the highest security 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 SIM alliance, and the GSMA have enabled innovative technology concepts, including those supporting remotely provisionable SIMs.

The GSMA has encouraged the industry to formulate 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 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 (SAS) to promote best operational practices:

- **SAS for UICC Production (SAS-UP):** The scheme through which UICC manufacturers subject their data generation and production sites and processes to a security audit.

- **SAS for Subscription Management (SAS-SM):** The scheme for security auditing and accreditation of eUICC subscription management services providers.

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

Kigen actively adheres to numerous industry standards and participates in several telecom industry-standard bodies. We are dedicated to playing a key role in the development and evolution of these architectures. Partner with Kigen for forward-thinking insights to help you enhance your portfolio while staying ahead of industry changes. Reach out to our Kigen experts today.

Dr Saïd Gharout
Head of Standards

Paul Bradley
Regional VP Solutions Sales

C8 - Kigen’s eSIM Solutions

GSMA eSIM discovery service

The GSMA eSIM discovery service is a cloud-based digital activation solution for remote provisioning specifications for the consumer market.

The Subscription Management-Discovery Service (SM-DS) service connects the eSIM to a purchased network operator profile using the eUICC identifier (EID). This allows for remote device provisioning with the relevant network operator’s SM-DP+. The entire process, including subscription discovery, profile preparation and delivery, happens seamlessly in the background. For end users, it offers a one-click digital eSIM activation, and for MNOs, it provides a trusted way to provision subscribers.

Kigen Pulse

Kigen Pulse is a single glass-of-pane platform for comprehensive eSIM and Profiles lifecycle management, built to support a range of customer orchestration scenarios. With a flexible deployment architecture, eSIM profiles for fleets of devices can be managed in a single platform.

Kigen Pulse offers a unified view of all eSIM and profiles, providing the same look and feel across M2M, consumer, and IoT RSP eSIM as a single access point for MNO/MVNOs and Enterprises. The platform intelligently takes care of the underlying communication to the eSIM irrespective of which standard it complies to. Therefore, this reduces the complexity of customers’ maintaining multiple platforms and separate user journeys.

How does eSIM provide secure connectivity from M2M?

Machine-to-machine (M2M) technology is meant explicitly for IoT sensors in smart meters, fleet trackers, and devices that typically operate with minimal human interaction on-site and may have limited power resources. These low-power devices receive the network operator profile, sent through a remote command from the subscription management platform.

eSIM technology allows users to manage multiple M2M connections remotely from one central location. This, in turn, ensures secure and reliable cellular connectivity, enabling efficient profile management in IoT deployments spread across different geographical locations. This means businesses can deploy their eSIM-enabled applications quickly in any region with minimal set-up time.

Contact Kigen

With Kigen's eSIM and flexible remote SIM provisioning solution, you can futureproof your deployments and accelerate your go-to-market timeline. Expand your customer base by capitalizing on eSIM interoperability with a broader OEM base to deliver trustworthy IoT information to third parties. For more information, please get in touch with us.

eSIM adoption is simpler than you think. Get in touch with our experts to see how we can help you: https://kigen.com/contact/

To keep up with the latest developments on eSIM, join our #FutureofSIM conversation on LinkedIn.

About Kigen

Kigen is the forerunner in eSIM and iSIM security-enabled IoT solutions built for scale. An Arm-founded company, Kigen flexibly empowers OEMs with security on leading IoT chipsets and modules and with the world's leading IoT and LPWAN connectivity providers in up to 200 countries. Our industry-leading SIM OS products enable over 2.5 billion SIMs and complement our GSMA-accredited Remote SIM provisioning secure service capabilities. Find out more at kigen.com or join our **#Futureof*SIM*** conversation on LinkedIn.

Kigen

All brand names or product names are the property of their respective holders. Neither the whole nor any part of the information contained in, or the product described in, this document may be adapted or reproduced in any material form except with the prior written permission of the copyright holder. The product described in this document is subject to continuous developments and improvements. All particulars of the product and its use contained in this document are given in good faith. All warranties implied or expressed, including but not limited to implied warranties of satisfactory quality or fitness for purpose are excluded. This document is intended only to provide information to the reader about the product. To the extent permitted by local laws Kigen shall not be liable for any loss or damage arising from the use of any information in this document or any error or omission in such information.