eSIM (eUICC) Growth

Recent Insights on eSIM (eUICC) Impact

Growing Trends in IoT

As more devices become interconnected, the demand for robust and versatile connectivity solutions has surged, driving innovation and investment in this space. By the close of 2023, the world counted approximately 16.1 billion active IoT devices, a figure anticipated to expand to nearly 40 billion by 2033. **Cellular IoT connections** will experience remarkable growth, rising from 1.9 billion in 2023 to 7.5 billion by 2033, with substantial contributions from 5G. This will include 5.5 billion devices connected via 5G—primarily using massive Machine-Type Communications (mMTC) solutions such as NB-IoT and LTE-M, while only 1.1 billion devices will connect via 'full' 5G New Radio (NR).

Active IoT devices in 2033	Cellular IoT connections in 2033	Customer sector within all connections in 2033	Lifetime connectivity savings
40 billion	7.5 billion	61%	8-13%

The LPWA Role

Alternative Low Power Wide Area (LPWA) technologies, such as **LoRaWAN**, are projected to scale significantly, with their collective footprint expanding from 360 million connections in 2023 to over 2 billion by 2033. Financially, the total IoT market—encompassing connectivity modules, value-added connectivity, and core applications—will see a dramatic increase in value from USD 335 billion in 2023 to USD 934 billion by 2033. Within this, value-added connectivity will account for 10% of the overall spending, with an additional 4% allocated to connectivity modules.

Verticals and Markets

The consumer sector will account for 61% of all connections, driven by the increasing demand for smart home devices, wearables, and other personal IoT solutions. In the enterprise space, connections will be diversified across industries. Approximately 35% of devices will be dedicated to cross-vertical applications like asset tracking, office automation, and fleet management. Utilities, particularly through smart metering, will make up 24% of enterprise connections, while retail and wholesale—largely driven by payment processing devices and electronic shelf labels—will represent 22%. Government use will comprise 7%, followed by transport and logistics at 4%, and agriculture at 3%. Regionally, China, North America, and Europe are set to maintain their strongholds, contributing 32%, 21%, and 19% respectively to the total market value by 2033.

eSIM Comes into Play

Simultaneously, **the adoption of eSIM and eUICC technologies** will provide enhanced flexibility and ease of remote provisioning for IoT devices. The market for eSIM and eUICC solutions is expected to grow in parallel with the overall increase in cellular IoT connections.

Connect with 1NCE:

1NCE.com sales@1nce.com

Connect with Kigen:

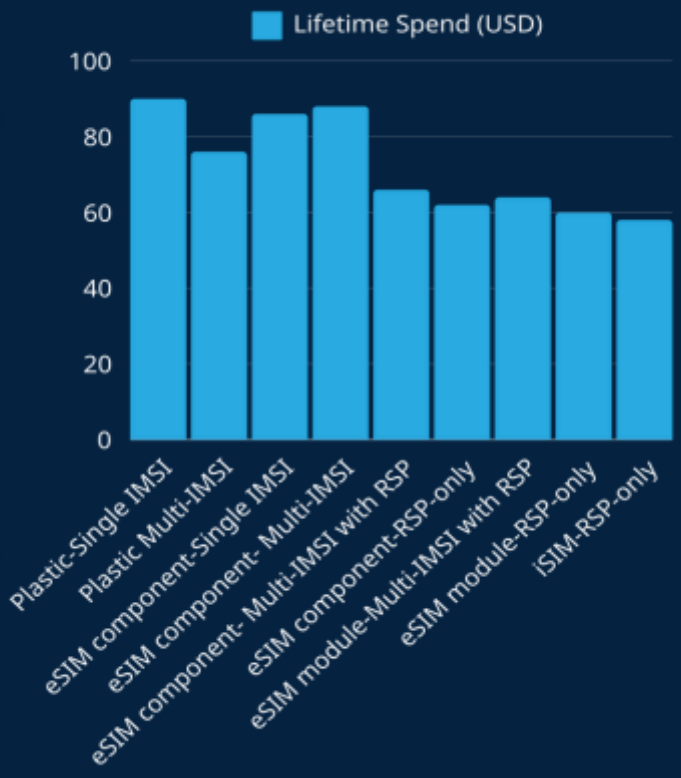
kigen.com contact@Kigen.com #FutureofSIM

eSIM(eUICC) Is Getting Traction

Remote SIM Provisioning

The introduction of **eSIM (eUICC)** technologies enables broader, scalable deployment of IoT devices by addressing limitations tied to traditional SIM cards. Unlike conventional SIMs, which are locked to a specific network operator and require physical replacement to switch carriers, eUICC allows network profiles to be managed remotely.

This remote capability, known as Remote SIM Provisioning (RSP), removes the need for manual SIM swaps, which can be a significant barrier to scaling IoT applications, especially when managing large fleets or devices in hard-to-reach areas. Consequently, manufacturers can upgrade network access on devices without physical intervention, which is essential for both global reach and operational efficiency in IoT deployments.



Average cellular IoT connectivity and SIM lifetime spend
[Source: Transforma Insights, 2022]

Impact on Costs

According to Transforma Insights, enterprises could achieve lifetime connectivity savings of 8-13% by selecting **eSIM and iSIM** technologies over traditional plastic SIM cards for IoT deployments. As embedded SIM (eSIM) technology matures, with iSIM as its natural successor, these options have become essential considerations for organizations planning cellular IoT solutions. Although eSIM and iSIM technologies are still developing, they are now largely standardized and are increasingly promoted by connectivity providers, particularly IoT-focused mobile virtual network operators (MVNOs).

A thorough cost evaluation of eSIM, iSIM, and RSP reveals both direct and indirect impacts on device lifetime costs, from component and subscription management expenses to security, compliance, and logistics. When accounting for factors like the complexity of component choices and SIM provisioning mechanisms, it's apparent that using eSIM lowers lifetime connectivity costs by 8% compared to plastic SIMs, reaching 11% savings with an integrated module.

iSIM further enhances cost savings, averaging a 13% reduction over plastic SIMs. However, the actual cost benefits vary across IoT applications. Certain use cases may not require multi-IMSI capabilities, and applications favoring NB-IoT—unsuited to RSP-based solutions—require a different approach. Additionally, use cases such as automotive IoT often demand ruggedized SIM cards, adding further costs.

Cost assessments for IoT connectivity across cellular generations indicate that 5G devices incur the highest lifetime spending, followed by 4G. Interestingly, NB-IoT, frequently used in long-lifespan applications like smart metering, incurs higher costs than LTE-M. Each vertical, therefore, has unique requirements that influence the selection and cost-efficiency of eSIM and iSIM options, underscoring the importance of tailored connectivity planning to maximize value for specific IoT applications.

Connect with 1NCE:

1NCE.com sales@1nce.com

Connect with Kigen:

kigen.com contact@Kigen.com #FutureofSIM

eSIM(eUICC) and Security in IoT

As the number of connected devices in IoT networks continues to grow, maintaining security is crucial. eSIMs enhance device safety by providing a secure environment for storing encryption keys and managing network credentials directly on the device. Unlike traditional SIM cards, eSIMs are embedded in the hardware, making them more resistant to tampering and removal. They also support remote management, allowing for over-the-air updates of network credentials and security protocols without requiring physical access to the devices.
The use of established security protocols—such as TLS (Transport Layer Security) and DTLS (Datagram Transport Layer Security)—in conjunction with eSIM technology helps ensure secure data transmission and device integrity. The combination of eSIMs and standardized protocols creates a comprehensive security architecture for IoT devices, enabling them to operate securely in diverse environments and adapt to emerging threats.

GSMA Specifications

Certification from the **GSMA** (Global System for Mobile Communications Association) is not mandatory for eUICC hardware and SIMs, but many providers adhere to GSMA standards and seek independent evaluations to validate product reliability.

GSMA certification initiatives, such as the **Security Accreditation Scheme (SAS)** and SGP.02 compliance, focus on the evaluation and certification of eUICC modules and devices. By following these specifications, manufacturers, mobile network operators, and service providers can ensure compatibility and maintain quality and security standards. Additionally, the IoT SAFE (IoT SIM Applet for Secure End-to-End Communication) framework standardizes security practices across IoT deployments.

a. eSIM for M2M

The GSMA's Embedded SIM Specification for M2M (eSIM for M2M) focuses on "business-to-business-to-consumer" channels, providing a framework for the architecture, implementation, testing, security, and compliance of eUICCs and eSIMs in M2M and IoT scenarios.

Key specifications include:

- **SGP.01:** Architecture for managing eUICC profiles in M2M devices.
- **SGP.02:** Technical requirements for implementing eUICC technology.
- **SGP.11:** Testing procedures for compliance and performance of M2M devices.

b. eSIM Consumer Specifications

The consumer solution allows end users to select their connectivity provider, requiring a high level of user interaction. Key specifications include:

- **SGP.21:** Architecture guidelines for eUICC.
- **SGP.22:** Technical details on eUICC functionality.

c. eSIM IoT Specifications

The new GSMA eUICC IoT Specification, published in Q2 2023, simplifies profile provisioning for constrained devices, such as those operating on LPWAN technologies. Key specifications include:

- **SGP.31:** eSIM IoT Architecture and Requirements Specification
- **SGP.32**: eSIM IoT Technical Specification

Other eUICC Standards

Various organizations, including the European Telecommunications Standards Institute (ETSI) and the Trusted Connectivity Alliance, contribute to eUICC standardization. ETSI focuses on smart M2M communications, while the Trusted Connectivity Alliance defines interoperability formats for eUICC profile packages.

Adhering to these standards is essential for secure, scalable, and interoperable eUICC-enabled IoT deployments. Compliance with recognized security standards, such as Common Criteria (CC) certification, ensures that eUICCs meet stringent security requirements through thorough evaluation processes.

Learn more about eUICC (eSIM) standards:

- eUICC (eSIM) Standards and Specifications in IoT Explained
- GSMA - Remote SIM Provisioning for M2M
- Trusted Connectivity Alliance - SIM Specifications

Key Considerations for Companies

When adopting eSIM (eUICC) technology, companies must navigate several critical factors to ensure successful implementation and operation:

Hardware

Hardware and software integration is paramount; organizations need to seamlessly incorporate eSIM capabilities into their devices, addressing both the physical components and the associated software frameworks.

This integration process involves evaluating existing hardware architectures to determine compatibility with eSIM modules, as well as implementing necessary firmware updates and developing robust application programming interfaces (APIs) that facilitate communication between the eSIM and device management systems.

RSP Capabilities

Additionally, **remote provisioning capabilities** are essential. This functionality enables businesses to manage and update devices over the air (OTA), allowing for the dynamic activation of mobile network operator profiles without the need for physical access to devices in the field. Companies should implement a secure remote provisioning server that adheres to GSMA standards, ensuring reliable profile management and seamless transitions between operators.

Security

Security is another key consideration; robust measures must be established to protect devices and sensitive data from potential threats. This includes employing advanced encryption protocols, such **as TLS (Transport Layer Security) and DTLS (Datagram Transport Layer Security),** to secure communication channels and safeguard data exchanges between devices and network operators.

Additionally, companies should conduct thorough security assessments and ensure compliance with industry standards and regulations, such as GDPR for data privacy and Common Criteria for security evaluation. Implementing a comprehensive security architecture that includes identity management, secure boot processes, and regular firmware updates is crucial for mitigating vulnerabilities.

Global Connectivity

Furthermore, companies should explore **global connectivity solutions** that facilitate seamless operation across diverse geographical regions. This involves selecting eSIM solutions that support multiple mobile network operators (MNOs) and are compliant with various regulatory frameworks worldwide. By utilizing standardized protocols, such as the GSMA's Remote SIM Provisioning (RSP), organizations can ensure that devices maintain reliable connections regardless of their location, enabling effective international deployments. Companies may also consider partnerships with local MNOs to enhance coverage and reduce latency in specific markets.

Instant Analytics

Finally, companies should establish a **monitoring and analytics framework** to track device performance, connectivity status, and security events. Utilizing IoT platforms equipped with real-time analytics capabilities can provide insights into device behavior, allowing for proactive management and quick responses to potential issues. By addressing these technical considerations, organizations can effectively leverage eSIM technology to enhance their IoT strategies, improve operational efficiency, and ensure robust security measures are in place.

Connect with 1NCE:

1NCE.com sales@1nce.com

Connect with Kigen:

kigen.com contact@Kigen.com #FutureofSIM

Kigen & 1NCE Partnership

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 https://kigen.com/

Kigen's approach focused on manufacturers and enterprises offers the most compact eSIM OS supporting all 5G and Low-Power Wide Area Networks, such as NB-IoT and Cat-M1 technologies, enhances flexibility and scalability, particularly for Massive IoT deployments. Kigen's platform supports remote provisioning, which allows eSIM profiles to be activated and configured remotely in the field or in factory. This capability is critical for large-scale IoT deployments, as it simplifies device management and reduces the need for physical access to devices in various locations.

About 1NCE

1NCE provides global connectivity solutions tailored for IoT applications. Their platform enables devices to connect to mobile networks across different regions, facilitating seamless communication. 1NCE focuses on IoT connectivity with flexible, cost-effective pricing models designed for various device types. The company's API-based integration allows developers to incorporate cellular connectivity into their applications easily, enhancing interoperability with existing systems.

The Partnership

Together with Kigen, 1NCE **developed eUICC-capable SIM cards** with RSP functionality that leverage **Kigen's world-class GMSA SAS**-accredited technology to enable seamless switching between profiles, allowing enhanced flexibility and adapta-bility in IoT applications. This feature is included at no additional cost with **1NCE's Lifetime Flat license**, designed specifically for industrial-grade IoT SIMs. Freedom to Switch ensures that customers are prepared for any eventuality throughout the lifecycle of their devices. It promotes vendor neutrality, enabling users to avoid vendor lock-in and maintain modern, flexible IoT solutions. In collaboration with Kigen, 1NCE enhances its offering with Kigen's secure and energy-efficient **eSIM OS and RSP solutions**. This partnership strengthens the security and efficiency of device management. Together, 1NCE and Kigen empower manufacturers to effectively innovate with their IoT technology throughout product development while addressing the challenges related to eSIM roaming, ensuring compliant and cost-effective eSIM management at scale, from production to deployment.

Additional Benefits

Here are additional benefits of choosing eUICC-enabled SIMs with 1NCE's Freedom to Switch:

- **Defy Vendor Lock-in:** Customers can switch between operators as needed, breaking free from reliance on a single provider.
- **Reduce Truck Rolls:** The ability to remotely manage and switch operator profiles eliminates the need for manual SIM swaps or physical interventions, significantly reducing operational costs.
- **Stay Flexible:** With eUICC technology, operations can be future-proofed, allowing businesses to adapt to changes in their device fleets without significant disruption.
- **Enhance Quality Assurance:** eUICC-enabled SIMs allow for immediate testing of network functionality during the assembly process, ensuring higher quality and reliability of IoT devices.

Connect with 1NCE:

1NCE.com sales@1nce.com

Connect with Kigen:

kigen.com contact@Kigen.com #FutureofSIM

Get started **today**.

1NCE Shop

Introduction to eUICC

Contact

Knowledge Base

Connect with 1NCE:

1NCE.com sales@1nce.com

Connect with Kigen:

kigen.com contact@Kigen.com #FutureofSIM