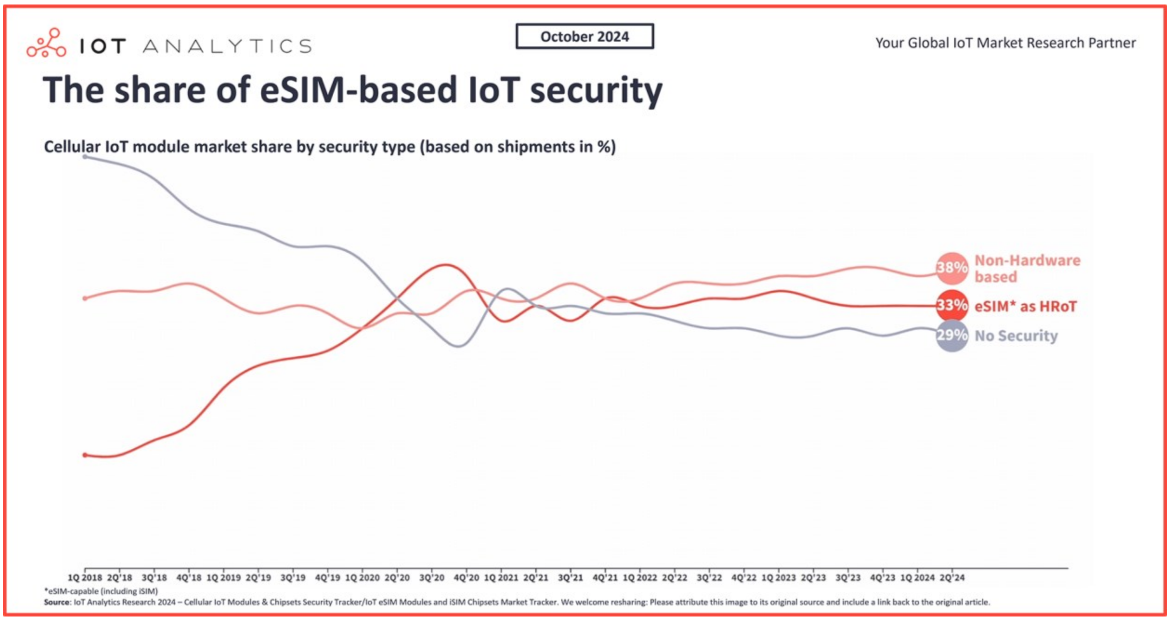
IoT Analytics GmbH
Zirkusweg 2
D-20359 Hamburg

T: +49 (0) 40- 63911891
M: press(at)iot-analytics.com
www.iot-analytics.com

FOR IMMEDIATE RELEASE

The role of eSIM for IoT: Better security, simplified roaming, and easier provisioning—but only 33% of cellular IoT devices use it



October 2024

Your Global IoT Market Research Partner

The share of eSIM-based IoT security

Cellular IoT module market share by security type (based on shipments in %)

*eSIM-capable (including iSIM)

Source: IoT Analytics Research 2024 – Cellular IoT Modules & Chipsets Security Tracker/IoT eSIM Modules and iSIM Chipsets Market Tracker. We welcome resharing: Please attribute this image to its original source and include a link back to the original article.

[Hamburg, Germany] – [October 15, 2024] – The adoption of eSIM and iSIM technology in cellular IoT connectivity is anticipated to see growth, according to new insights from IoT Analytics. Based on the latest *IoT eSIM Modules and iSIM Chipsets Market Tracker* and the *Cellular IoT Modules & Chipsets Security Tracker*, the installed base of eSIM-capable IoT connectivity modules reached 650 million in 2023. The recently published research article details that eSIM technology is widely recognized for its potential to revolutionize cellular IoT connectivity by facilitating remote SIM provisioning, global connectivity, and enhanced security through hardware-based solutions. Despite these advantages, adoption has been slower than anticipated due to challenges with remote SIM provisioning and fragmented standards. However, new specifications—SGP.31 and SGP.32 from the GSMA—are now easing these barriers, providing manufacturers and end-users with clearer frameworks to accelerate deployment.

KEY INSIGHTS

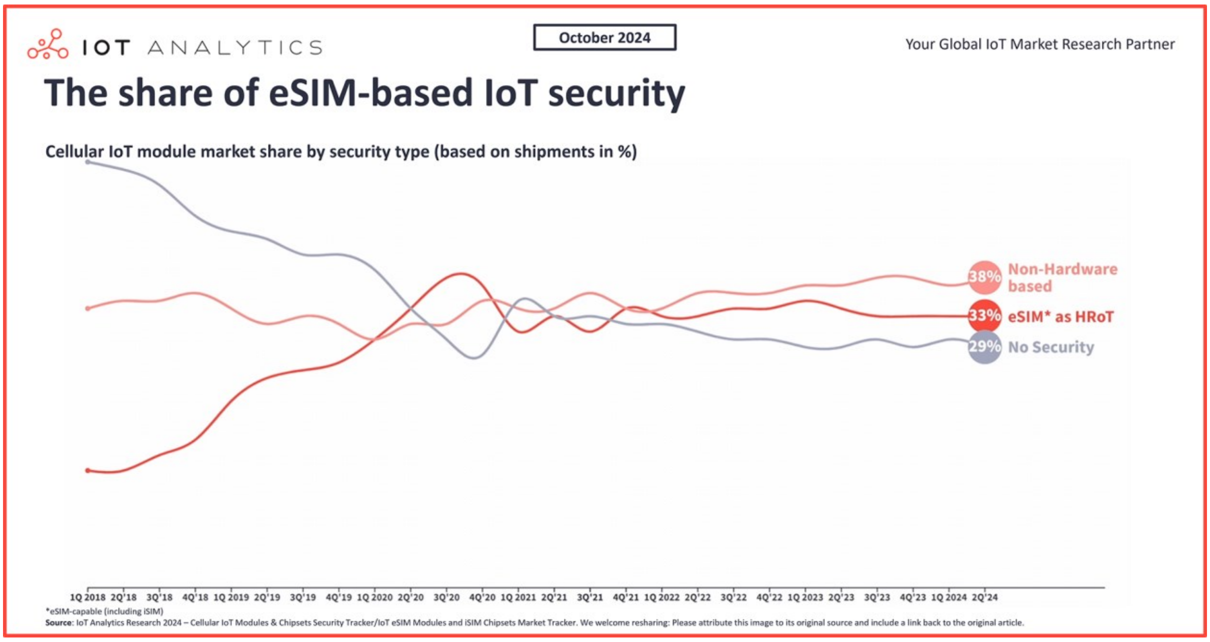
- The installed base of eSIM-capable (including iSIM) IoT connectivity modules reached 650 million in 2023, according to IoT Analytics' IoT eSIM Modules and iSIM Chipsets Market Tracker and Cellular IoT Modules & Chipsets Security Tracker (both updated September 2024).
- eSIM technology represents a paradigm shift in cellular IoT connectivity, enabling remote SIM provisioning, global connectivity, and enhanced security through a hardware-based approach.
- Despite the benefits, eSIM adoption has been slower than expected due to remote SIM provisioning complexities and divergent standards; recent eSIM IoT specifications—SGP.31 and SGP.32 from the GSMA—help manufacturers and end users overcome these challenges.
- IoT Analytics forecasts that cellular IoT modules with eSIM technology will experience accelerated growth starting in H2 2025.
-

SELECT QUOTES

Satyajit Sinha, Principal Analyst at IoT Analytics, comments that "In Q3 2024, we observed a notable shift in CEO discussions toward AI applications, renewable energy, IT resilience, and the upcoming U.S. elections. Despite this shift, economic concerns remained the most discussed theme overall. Historically, changes in CEO discussion themes have been indicators of shifts in sentiment and corporate investment behavior. I expect these emerging topics to play a more prominent role in corporate decision-making moving forward."

[The full research article is attached below]

The role of eSIM for IoT: Better security, simplified roaming, and easier provisioning—but only 33% of cellular IoT devices use it



The share of eSIM-based IoT security

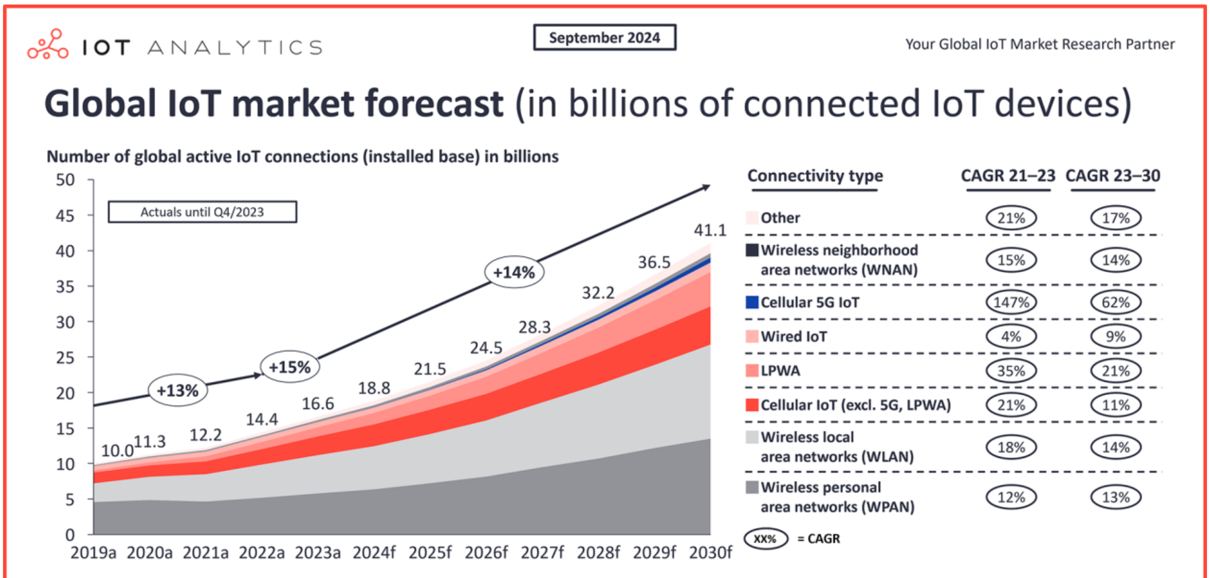
Cellular IoT module market share by security type (based on shipments in %)

*eSIM-capable (including iSIM)

Source: IoT Analytics Research 2024 – Cellular IoT Modules & Chipsets Security Tracker/IoT eSIM Modules and iSIM Chipsets Market Tracker. We welcome resharing: Please attribute this image to its original source and include a link back to the original article.

IoT connectivity and the rise of eSIM for IoT

Double-digit growth expected in connected IoT devices. By the end of 2023, there were 16.6 billion connected IoT devices, according to recent IoT Analytics reporting. This number is expected to surpass 40 billion in 2030 (growing at 14% CAGR), driven by the need for data collection and process and mechanical automation in key industries such as manufacturing, healthcare, transportation, and smart cities.



Connectivity type	CAGR 21–23	CAGR 23–30
Other	21%	17%
Wireless neighborhood area networks (WNAN)	15%	14%
Cellular 5G IoT	147%	62%
Wired IoT	4%	9%
LPWA	35%	21%
Cellular IoT (excl. 5G, LPWA)	21%	11%
Wireless local area networks (WLAN)	18%	14%
Wireless personal area networks (WPAN)	12%	13%

Note: IoT connections do not include any computers, laptops, fixed phones, cellphones, or consumers tablets. Counted are active nodes/devices or gateways that concentrate the end-sensors, not every sensor/actuator. Simple one-directional communications technology not considered (e.g., RFID, NFC). Wired includes ethernet and fieldbuses (e.g., connected industrial PLCs or I/O modules); Cellular includes 2G, 3G, 4G, 5G; LPWA includes unlicensed and licensed low-power networks; WPAN includes Bluetooth, Zigbee, Z-Wave or similar; WLAN includes Wi-Fi and related protocols; WNAN includes non-short-range mesh, such as Wi-SUN; Other includes satellite and unclassified proprietary networks with any range.
Source: IoT Analytics Research 2024-State of IoT Summer 2024. We welcome resharing: Please attribute this image to its original source and include a link back to the original article.

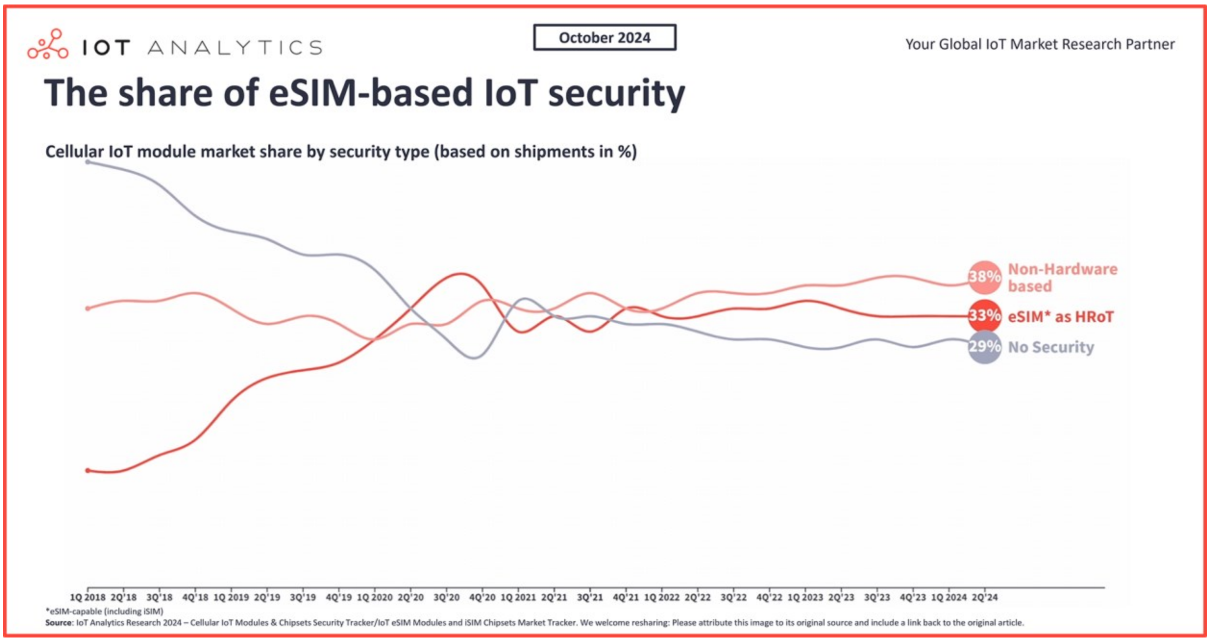
21% of connected IoT devices use cellular connectivity. Of the 16.6 billion connected IoT devices in 2023, 3.56 billion (or 21%) relied on cellular connectivity, according to IoT Analytics' Global Cellular IoT Connectivity Tracker and Forecast (published June 2024). This number—along with cellular connectivity's overall share of IoT connections—is expected to grow with the increasing adoption of 5G technologies. No doubt, cellular IoT has become critical for applications requiring mobility and reliable long-range coverage—the question becomes about cellular IoT scalability and security.

eSIM technology addresses limitations of traditional SIM cards in cellular IoT connectivity. Traditionally, cellular IoT connections relied on physical SIM cards, which were often locked into specific providers and required swapping when entering new regions, countries, or even coverage areas within countries, which is not feasible at scale and can be costly and labor-intensive. Additionally, cellular IoT devices leveraging traditional SIM cards often ship without dedicated hardware-based security, meaning they either rely on non-hardware-based security solutions or lack any security solutions. However, a modern SIM-type technology helps address these deployment and security limitations: embedded SIMs (eSIMs).

As the name suggests, eSIMs (including integrated SIMs, or iSIMs) are *part* of the cellular IoT module hardware. They are unique and programmable, allowing for remote, over-the-air network provisioning of network profiles. Further, eSIMs include embedded secure elements, and being rooted in the cellular IoT modules as unique elements, they enhance the integrity of the modules and the IoT devices into which they become integrated (more on these benefits below).

33% of shipped cellular IoT modules were eSIM-capable. According to IoT Analytics' Global IoT eSIM Modules & iSIM Chipsets Market Tracker (updated September

2024), a third of the total cellular IoT modules shipped in Q2 2024 were eSIM-capable—meaning they included an eSIM in the module—compared to 62.3% using physical SIM cards, with the remainder utilizing Soft SIM technology. Further, since eSIM technology incorporates embedded secure elements that protect the integrity of cellular IoT modules, this means that 33% of cellular IoT modules shipped included dedicated hardware-based security, according to IoT Analytics' Global Cellular IoT Modules & Chipsets Security Tracker (also updated September 2024).



IOT ANALYTICS

October 2024

Your Global IoT Market Research Partner

The share of eSIM-based IoT security

Cellular IoT module market share by security type (based on shipments in %)

*eSIM-capable (including iSIM)

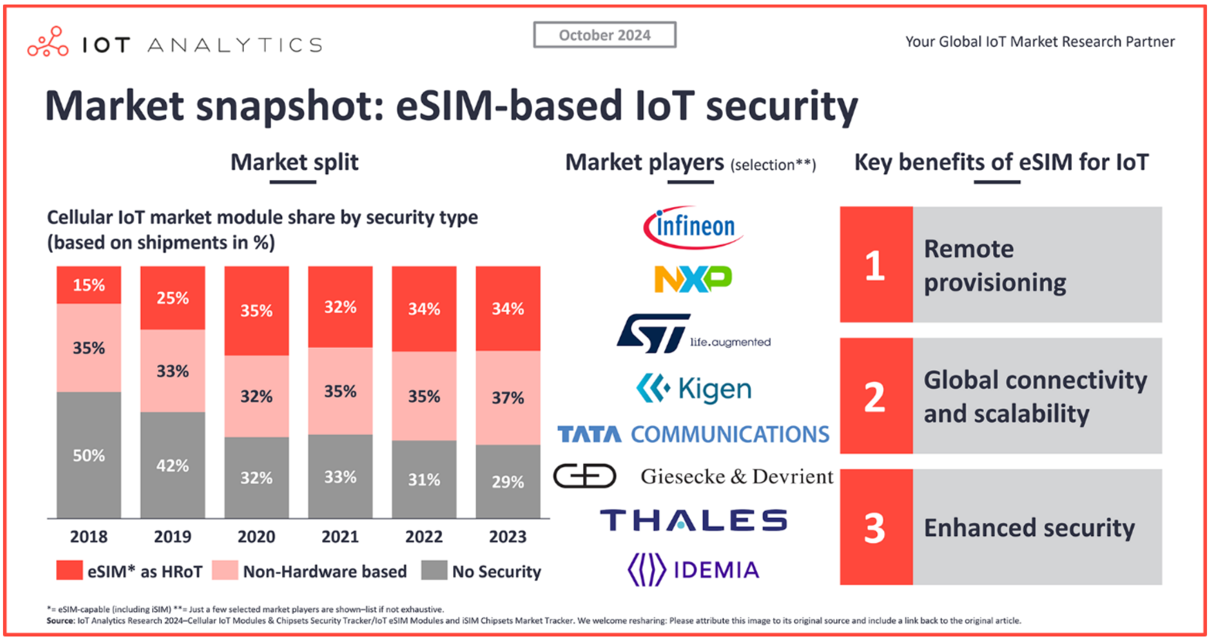
Source: IoT Analytics Research 2024 – Cellular IoT Modules & Chipsets Security Tracker/IoT eSIM Modules and iSIM Chipsets Market Tracker. We welcome resharing: Please attribute this image to its original source and include a link back to the original article.

How eSIM technology works in IoT

An **eSIM** is an integrated circuit that combines hardware, a secure element, and software called a universal integrated circuit card (UICC). eSIMs are typically available in various form factors, including machine-to-machine form factor (MFF2), wafer-level chip scale packaging (WLCSP), and miniaturized leadless packages. Specifically, eSIMs use an embedded UICC (eUICC) with a secure element for enhanced security in IoT devices.

An **iSIM** is a type of eSIM where an integrated UICC (iUICC) with a secure element is manufactured into a system-on-chip (SoC) or system-in-package (SiP), which then becomes integrated into a cellular IoT module.

Key benefits of eSIM for IoT



IOT ANALYTICS

October 2024

Your Global IoT Market Research Partner

Market snapshot: eSIM-based IoT security

Market split

Cellular IoT market module share by security type (based on shipments in %)

Market players (selection**)

Key benefits of eSIM for IoT

1 Remote provisioning

2 Global connectivity and scalability

3 Enhanced security

*= eSIM-capable (including iSIM) **= Just a few selected market players are shown–list if not exhaustive.
Source: IoT Analytics Research 2024–Cellular IoT Modules & Chipsets Security Tracker/IoT eSIM Modules and iSIM Chipsets Market Tracker. We welcome resharing: Please attribute this image to its original source and include a link back to the original article.

The rise of eSIM technology represents more than just a mere technological advancement—it is a paradigm shift. The technology is about the seamless integration and simplification of cellular connectivity in IoT devices and enhancing user experiences. As discussed below, eSIMs are central to transforming the dynamics of the cellular IoT market based mainly on 3 key aspects of the technology: 1) remote provisioning, 2) global connectivity and scalability, and 3) enhanced security.

1. Remote SIM provisioning in eSIM management

Remote SIM provisioning (RSP), a feature standardized by the GSM Association (GSMA), enables the remote management of SIM profiles over the air, eliminating the need for physical SIM card replacements. It provides a more efficient means to manage devices and has 2 primary benefits:

1. **Enhanced flexibility –** With RSP, organizations can provision IoT devices with different carrier profiles remotely, enabling seamless network switching. This is particularly beneficial for businesses operating across multiple countries or regions—or even within countries where areas lack coverage from one carrier but have coverage from another. For example, a logistics company can remotely provision its tracking devices to local carriers as shipments cross borders, ensuring consistent connectivity without manual intervention—i.e., swapping physical SIM cards.

2. **Reduced provisioning time –** RSP significantly reduces the time required to deploy IoT devices. Businesses can remotely activate and manage SIM profiles to expedite their go-to-market strategies (more go-to-market time below). Large-

scale IoT deployments become more manageable, as devices can be set up and updated in bulk without the logistical challenges of handling physical SIM cards.

2. Global connectivity and scalability: Accelerated go-to-market

eSIM technology empowers IoT devices with global connectivity, which is crucial for businesses aiming to operate internationally. The technology offers several **distinct advantages**:

1. **Seamless global operations –** Devices equipped with an eSIM can connect to local networks worldwide without requiring manual reconfiguration, simplifying cross-border operations. This is especially important for asset tracking and logistics use cases, where devices must remain connected across various regions. eSIM technology eliminates the need for traditional roaming agreements, ensuring consistent performance and compliance with local regulations.
2. **Physical SIM roaming vs. eSIM roaming –** Roaming with physical SIM cards typically involves dependency on local carriers' roaming agreements, leading to inconsistent performance, higher costs, and more complexity in managing connectivity across multiple regions. In contrast, eSIM technology, combined with RSP and eSIM management, enables seamless, cost-effective roaming by dynamically selecting and switching between local carriers as needed. This flexibility allows businesses to streamline their operations, avoid traditional roaming charges, and reduce the risk of service disruptions.
3. **Scalability –** The ability to manage connectivity remotely is a game-changer for companies scaling their IoT deployments. With eSIM, businesses can remotely provision new devices instantly, adding them to the network without needing physical intervention. This reduces the time to market for new products or services, enabling companies to expand quickly and efficiently. By allowing for the instant addition of devices to a network, eSIMs offer significant operational agility, helping businesses stay competitive and respond faster to shifting market demands.

Case study: Global logistics company switches to eSIM for IoT-based asset tracking

Situation: A global logistics company ran a large-scale IoT-based asset-tracking devices across Europe, North America, Latin America, and the Asia-Pacific region using physical SIM cards.

Challenge: Often, a physical SIM swap was necessary to access local MNO networks, which was labor-intensive.

Solution: The logistics company partnered with **Infineon**, a Germany-based semiconductor manufacturer and **Tata Communications**, an India-based telecommunications company to use eSIMs instead of physical SIMs (Using OPTIGA Connect eSIM and Tata Communication's MOVE platform).

Outcomes: The solution replaced the traditional SIM card with a soldered eSIM, removing the need to replace SIM cards. This solution eliminated the need to download credentials when crossing borders, enabled seamless connectivity, and provided access to Tata Communication's pre-negotiated rates with approximately 600 MNOs in over 200 countries and territories. Further, by replacing the multiple SIM batches of the previous solution with Infineon's eSIM, the company only had to manage a single SKU.

3. Enhanced security with embedded secure elements in eSIM

Software and network security solutions have historically overshadowed hardware security in IoT due to their visibility and simpler implementation, while hardware security is often more complex and costly. However, a hardware-based root of trust (HRoT) allows manufacturers and consumers to ensure module authenticity, addressing cloning, counterfeiting, and key protection. Once key security is guaranteed, additional components, like secure boot or TrustZone, from UK-based semiconductor manufacturer **Arm**, can be added. For IoT, eSIM technology is emerging as an HRoT, supported by initiatives like IoT SAFE.

eSIMs incorporate embedded secure elements, offering advanced security features surpassing traditional SIM cards. These secure elements act as an HRoT, enabling stronger protection through asymmetric encryption and ensuring secure, end-to-end communication.

1. **HRoT for enhanced encryption –** The embedded secure element is the foundation for secure operations by ensuring that cryptographic keys and sensitive data are securely stored and processed within the device. This makes eSIMs particularly well-suited for industries requiring high levels of data protection, such as financial services, healthcare, and critical infrastructure. The secure element ensures that communication channels between IoT devices and networks remain protected from interception or tampering, reducing the risk of cyberattacks.
2. **GSMA IoT SAFE specifications –** The GSMA's IoT Security Architecture for End-to-End Security (IoT SAFE) specifications further enhance the security provided by eSIM technology. IoT SAFE uses eSIM as an HRoT, enabling secure device authentication and encryption services for IoT applications. By leveraging the secure element within the eSIM/iSIM, businesses can ensure that their IoT devices meet stringent security standards and are protected from emerging cybersecurity threats.

"For manufacturers, establishing these roots of trust will be the first step in ensuring a new device is built to include trustable security. Kigen has been driving standardizing the RoT within a device's SIM, eSIM or iSIM: an approach that ensures a common mechanism for secure data communications using a highly trusted and time-tested module. It offers a cost-effective mechanism for cloud authentication and end-to-end security, since SIMs are already used for authentication on mobile networks. This is especially important for IP and data trust in the era of AI for realizing the vision of a truly secure IoT, from chip to cloud."

– Loic Bonvarlet, SVP, **Kigen**

Overcoming hindrances to widespread eSIM for IoT adoption

eSIM adoption has stagnated in recent years. Even with these benefits of eSIM over other SIM-type technologies, widespread eSIM adoption has been slower than expected, which has led to a plateau in the share of shipments of cellular IoT modules with eSIM technology compared to the shipment of such modules with other SIM-type technology—holding around 30% since late 2019. In turn, this has also plateaued the shipment share of cellular IoT modules with hardware-based security compared to modules with other or no dedicated security overall.

Interoperability issues and complex RSP standards are reasons for slow adoption. The delay in widespread adoption of eSIM for IoT (and in general) stems from challenges associated with RSP and divergent standards for consumer IoT devices versus machine-to-machine (M2M) technologies in enterprises, which have led to interoperability challenges and device management complications. For example, SGP.02, the GSMA's specification for RSP in M2M devices, has limitations that have hindered eSIM technology adoption in the overall IoT market (consumer and enterprise). Its architecture requires multiple functional entities, such as the Subscription Manager Data Preparation (SM-DP) and Subscription Manager Secure Routing (SM-SR). These functional entities increase deployment complexity and operational overhead, limiting scalability for large-scale IoT deployments and flexibility in operator switching due to static profile management.

SGP.31 and SGP.32 aim to simplify eSIM IoT architectures. To address these challenges, the GSMA has introduced two eSIM IoT specifications—SGP.31 and SGP.32—designed to complement M2M specification SGP.02 and consumer IoT specification SGP.22. The releases of SGP.31 and SGP.32 brought forth 3 significant changes to address the challenges that have so far hindered widespread adoption:

1. **Introducing the eSIM IoT Remote Manager (eIM) –** This component streamlines remote profile management and provisioning processes, reducing complexity.
2. **Transforming the Local Profile Assistant (LPA) into the IoT Profile Assistant (IPA) –** This change eliminates the need for user interaction during provisioning, simplifying IoT connectivity and reducing time to market for IoT deployments.
3. **Replacing SM-SR with Subscription Manager Discovery Server (SM-DS) and IPA in the architecture –** This eliminates the need for SM-SR in eSIM IoT deployments and reduces reliance on carrier integration.

In all, SGP.31 and SGP.32 aim to simplify the architecture, enhance scalability with efficient provisioning protocols suitable for large-scale IoT deployments, and improve flexibility in operator selection with on-demand profile switching.

Analyst opinion and market outlook

eSIM is a winner for IoT: Better security while improving cost efficiency. Currently, two-thirds of all cellular IoT module shipments lack support for HRoT—the foundation of IoT security. eSIM technology facilitates asymmetric encryption for secure chip-to-cloud communication by injecting the security key into the HRoT. Thus, implementing eSIMs into cellular IoT modules allows OEMs and end users to address two major challenges: global connectivity and security. Further, since IoT security has traditionally been viewed as an added cost, adopting eSIM technology allows OEMs to distribute the return on investment more efficiently.

All cellular IoT use cases benefit from eSIM. While the roaming benefit of eSIMs favors asset tracking type of use cases, the enhanced security features and easy remote provisioning (i.e., switching between different mobile operators) benefit all major IoT initiatives that make use of cellular connectivity. IoT Analytics, therefore, expects adoption across most, if not all, IoT use cases (smart meters, cars, health devices, etc.).

Adoption expected to accelerate by late 2025. Given the release of SGP.31 and SGP.32, there is reason to expect accelerating growth in the eSIM market. However, the full commercialization of SGP.32 will only begin in 2025 due to the need for widespread industry adoption and infrastructure upgrades. While SGP.31 is already facilitating growth, SGP.32 introduces more advanced features that require significant testing, integration, and compliance across various stakeholders before it can be fully deployed. This gradual roll-out ensures that the necessary ecosystem adjustments are made, minimizing potential disruptions and allowing for smoother transitions. With this, the IoT eSIM Modules and iSIM Chipsets Market Tracker projects accelerated growth in the shipments of cellular IoT modules with eSIM technology by Q3 and Q4 2025. This acceleration in shipment growth supports analysis in the Cellular IoT Modules & Chipsets Security Tracker that shipments of cellular IoT modules with hardware-based security will see accelerated growth in 2025 and onward as well.

Disclosure

Companies mentioned in this article—along with their products—are used as examples to showcase a vibrant IoT startup landscape. No company paid or received preferential treatment in this article, and it is at the discretion of the analyst to select which examples are used. IoT Analytics makes efforts to vary the companies and products mentioned to help shine attention to the numerous IoT and related technology market players.

It is worth noting that IoT Analytics may have commercial relationships with some companies mentioned in its articles, as some companies license IoT Analytics market research. However, for confidentiality, IoT Analytics cannot disclose individual relationships. Please contact compliance@iot-analytics.com for any questions or concerns on this front.

For more information or media inquiries, please contact:

Hoang Pham Van
IoT Analytics
+49 (0) 40 6391 1891
press(at)iot-analytics.com

For further reading please visit:

www.iot-analytics.com/research-blog

About IoT Analytics

IoT Analytics, founded and operating out of Germany, is a leading global provider of market insights and strategic business intelligence for the IoT, AI, Cloud, Edge, and Industry 4.0.
Our key workstreams across the tech stack include IoT applications, IoT platforms and software, IoT connectivity and hardware, and industrial IoT.
We are trusted by 1000+ leading companies around the world for our market insights, including globally leading software, telecommunications, consulting, semiconductor, and industrial players.

###