

**THALES**

Building a future we can all trust

# Assessing 'Soft SIM' and 'Cloud SIM' as IoT Connectivity Choices

# Agenda

|  |    |
|--|----|
| Introduction .....   | 03 |
| Evolution of cellular connectivity .....   | 04 |
| New frontiers in cellular connectivity.....  | 05 |
| A comparison: eSIM, iSIM, Soft SIM, and<br>Cloud SIM in cellular IoT connectivity..... | 06 |
| Security and other concerns .....  | 07 |
| Usage applicability and case-dependence.....   | 09 |
| Comparative assessment .....   | 11 |
| More resources on eSIM and other technologies .....                                    | 13 |



# 1. Introduction

Navigating the intricate terrain of cellular connectivity for the Internet of Things (IoT) has become an increasingly challenging task in 2023.

As IoT Service Providers, Mobile Network Operators (MNOs), Mobile Virtual Network Operators (MVNOs), and Original Equipment Manufacturers (OEMs), your choices today can have far-reaching implications on your IoT solutions' viability, security, and resilience.

This guide is intended to provide a deep dive into the upcoming trends in cellular connectivity for IoT.

At the heart of this landscape, we find the concept of the **Subscriber Identity Module (SIM)** undergoing a transformative evolution.

From physical SIMs, we've moved to embedded SIM (**eSIM**), and now we're glimpsing the dawn of **integrated SIM (iSIM)**.

But just when you think you've got it all figured out, along come new contenders – the so-called **"Soft SIM"** and **"Cloud SIM."**

These alternatives are tempting in their novelty, suggesting an attractive world without physical SIM hardware.

While they can seem like promising solutions on the surface, diving deeper often reveals a different story.

So why read on?

Because making the right decision about cellular connectivity for your IoT devices isn't just about keeping up with the latest trends.

It's about understanding the entire picture – both the allure of the new and the tried-and-tested strength of the established.

By the end of this guide, you'll not only grasp the pros and cons of each technology but also understand how to gauge their suitability based on a set of comprehensive criteria, including:

- Security certifications
- Security scalability
- Simplicity
- Connectivity management
- Connectivity scalability
- Field-proven experience & future-proofing

Let's dig in and start with some definitions.

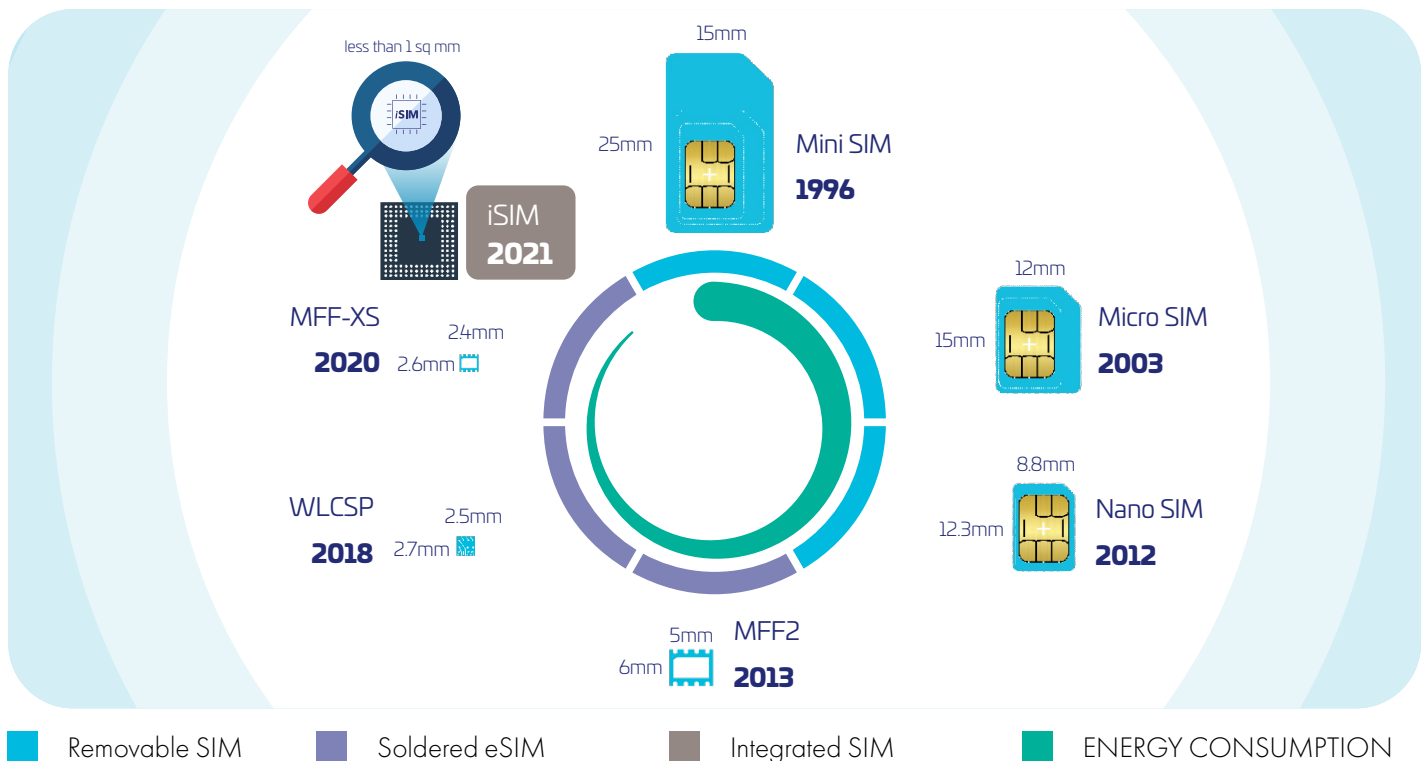
## 2. Evolution of cellular connectivity

Our journey starts with the humble beginnings of the cellular network and quickly transitions to the challenging IoT solutions of today.

Initially, the SIM was a physical card you inserted into your device to be authenticated and connected to your network.

It was the key to mobile communication, first appearing in 1991.

However, as the technology powering cellular devices evolved, the size of the physical SIM became a little outdated. This led to the development of the Mini-SIM in 1996, Micro-SIM in 2003, and the Nano-SIM in early 2012, each iteration becoming smaller and more suitable for the shrinking sizes of devices.



The introduction of the eSIM in [2016](#) marked a significant turning point.

No longer was the SIM a separate, physical component; instead, it was integrated directly into the device's hardware.

The result?

This shift streamlines device design and facilitates greater flexibility in selecting network carriers, a highly sought-after feature in IoT deployments, thanks to a reduced footprint and the ability to load the cellular subscription afterwards or change it remotely.

But the evolution didn't stop there.

The iSIM was the next leap forward in 2021. Incorporating SIM functionality directly into the device's main processor, the iSIM enhanced power efficiency, reduced device size, and increased cost-effectiveness, becoming an attractive option in the IoT landscape.

Some describe the iSIM, as a SIM integrated in a chipset.

Our view is that the iSIM is in fact an integrated eSIM with maximum security, and all the inherent benefits of an eSIM in terms of flexibility and remote connectivity management.

Despite its newer status and smaller size, whenever an iSIM is used as an eSIM it needs to follow the same certification processes as its eSIM predecessor. The critical data resides within the secure enclave of the chipset itself, providing a built-in and tamper-proof security measure.

In any case, whatever their form factor, SIM, eSIM and iSIM are all standardised and based on a secure tamper-proof physical component.

This aspect further strengthens its attractiveness for IoT applications, where data protection is paramount.

There is more.






Research suggests that by 2027, we could see as many as 300 million iSIM-compliant consumer and IoT devices in the field.

These developments will make it easier and more cost-effective for businesses to implement [private 5G networks](#), supporting the connectivity demands of large-scale Machine-Type Communications (mMTC).

# 3. New frontiers in cellular connectivity

Now, we're witnessing the emergence of Soft SIM and Cloud SIM technologies.

- The **Soft SIM** is a software-based SIM card. Also referred to as a virtual SIM, it features the functionality of a SIM but without a physical SIM card or embedded hardware.
- **Cloud SIM** follows a similar philosophy, but instead of residing on the device, the Cloud SIM lives in the cloud. The concept is that devices on the ground get temporary connectivity allocated by the cloud. In this framework, devices can share the same operational subscription.

| SIM Type  | Description   |
|---|---|
|  <b>SIM (Subscriber Identity Module)</b> | A physical tamper-proof secure chip that a mobile network operator provides to connect a phone or other device to a cellular network. It contains a unique identifier that allows the carrier to recognize the device and grant access to its services.   |
|  <b>eSIM (embedded SIM)</b>              | A smaller version of the traditional SIM card that's soldered directly onto the device's circuit board, with the same level of security as a SIM. It can be programmed and reprogrammed to different carriers remotely. eSIM is also known as eUICC.  |
|  <b>iSIM (integrated SIM)</b>            | A new version of eSIM with a smaller form factor than the eSIM where the SIM functionality is integrated directly into the secure enclave of the device's processor or System-on-Chip (SoC). iSIM has the same level of security as the eSIM. iSIM is also known as ieUICC.   |
|  <b>Soft SIM</b>                         | Also known as a virtual SIM, this is a software-based SIM. Instead of a physical card, the Soft SIM runs as any other software in the device to connect it to a mobile network. This concept is similar to virtual SIM and is often provided through a mobile application.  |
|  <b>Cloud SIM</b>                        | A technology that allows multiple numbers on a single device and a single cellular subscription to be shared across multiple devices without any physical SIM cards. The SIM profiles are stored and managed in the cloud, and users can switch between different profiles as needed. It utilizes a digital version that can be provisioned and activated over the air through a wireless connection. |

*SIM terminology and definitions.*

Let's dive deep into the advantages, potential limitations, and appropriateness of these new alternatives in the context of your specific IoT requirements.

# 4. A comparison: eSIM, iSIM, Soft SIM, and Cloud SIM in cellular IoT connectivity

## eSIM (embedded SIM)

eSIM is a global specification by the GSMA, enabling Remote SIM Provisioning of subscriptions in cellular devices.

eSIMs are a big step forward from traditional physical SIMs. They provide the ability to change carriers remotely and seamlessly. Like physical SIMs, they're secure, reliable, and widely supported by many network operators globally.

The new IoT eSIM specification released by the GSMA further simplifies the deployment and operations of eSIM in IoT devices.

## iSIM (integrated SIM)

iSIM takes eSIM a step further, integrating the SIM functionality directly into the secure enclave of the device's processor.

iSIMs provide all the benefits of eSIMs and more. They are more power-efficient and cost-effective and enable even smaller device form factors. As a newer alternative in the IoT connectivity space, iSIM may represent [19% of all eUICC shipments in 2027](#), according to Kaleido Intelligence.

## Soft SIM

Soft SIM is a technology where SIM card data is downloaded and stored on the device along with other types of data. The device's processor executes the SIM software to handle cellular connectivity. There is no difference with other software or applications running on the device in regard to data protection and resistance to attacks.

Soft SIMs are potentially simple to deploy as they have no specific hardware requirements. However, Soft SIMs face security, compatibility, and regulatory challenges as a newer alternative in the IoT connectivity realm.

## Cloud SIM

Cloud-based SIM is another type of virtual SIM technology. Here, the SIM card resides in the cloud, enabling the device to switch between different network providers over the air.

Note that, like the soft SIM there is specific software running on the device, with the same drawbacks in terms of data protection and resistance to attacks.

Cloud SIMs potentially provides better network coverage than Soft SIM by allowing carrier switching. However, like Soft SIMs, they are a newer alternative in the market and face security, compatibility, and regulatory acceptance issues.

# 5. Security and other concerns

## Security Risks for IoT Applications

In a recent study, "[Why IoT projects fail](#)", IOTNOW magazine revealed that security had been the biggest concern for IoT projects for the last five years.

### Why?

IoT solutions need end-to-end security, and that's easier said than done.

As IoT solutions develop, security needs to evolve right alongside them.

Soft SIMs and Cloud SIMs offer benefits like easy deployment, but their software nature heightens security risks, especially for IoT devices.

Compared to tamper-resistant hardware and field-proven options such as SIM, eSIM, and iSIM, software solutions are more vulnerable to cyber threats [\[ENISA\]](#).

Consequently, a compromise could lead to data breaches and disruption of entire IoT systems.

IoT devices, from smart home appliances to industrial sensors, already pose significant security challenges.

A [notable example](#) is the vulnerability uncovered in security cameras by cybersecurity company Mandiant and [CISA](#).

This vulnerability, identified in devices using the ThroughTek Kalay network, allowed cyber attackers to compromise the devices remotely.

The attackers could watch live feeds, listen in on audio, and potentially hijack the devices for further attacks. Such a breach threatens personal privacy and could lead to more significant security threats, such as snooping on sensitive enterprise meetings or devices being co-opted into botnets for Distributed Denial of Service (DDoS) attacks.

Adding a software-based SIM into the mix increases the [attack surface](#) for potential hackers. The attacks on IoT devices with

software-based connectivity options would resemble those on PCs.

Once the device is breached, viruses and worms can use the network to target all the devices from a distance. Potential threats include the ability to connect devices that were not initially authorised, thus enabling device impersonation and the use of unauthorized applications in the server. Potential threats also include corrupted data from infected objects that could lead to disastrous disruption of services in security-sensitive markets such as healthcare, automotive, energy...

Despite security measures like Trusted Execution Environment [\(TEE\)](#), software solutions are not able to match the resilience of secure hardware options.

Interestingly, the likely point of attack for a Cloud SIM wouldn't be the cloud, which is typically harder to breach, but the devices in the field.

Once infected, typical threats could evolve into distributed denial of service (DDoS) types of attacks.

On the other hand, certified technologies like eSIM and iSIM have demonstrated high security and resilience standards against cyber threats. This makes them a more secure choice for IoT cellular connectivity, reinforcing the idea that hardware-based solutions are typically more secure than their software counterparts.



## The importance of certification

The absence of universal standards for both Soft SIMs and Cloud SIMs could lead to compatibility and interoperability issues among different IoT devices, networks, and locations.

Furthermore, while we may have a cloud service protected against cyber attacks, obtaining strong security certification of software-based endpoints is not feasible. This presents a significant challenge because the overall security of a system depends on its weakest element.

So, even if a cloud system is secure, the software at the endpoint may still be vulnerable to attacks, leading to compromised security. Consequently, the lack of standardisation could complicate the management and deployment of IoT solutions and, more importantly, leave systems vulnerable to cyber threats.

Security certification performed by globally recognised independent bodies is the foundation of trust for the many industries and stakeholders of the IoT ecosystem that need to work within a common reliable framework. This can't be achieved by any self-declared security.

eSIM and iSIM technologies, backed by globally recognised standards, ensure seamless and interoperable deployment.

The GSMA imposes a high level of security. For instance, recently, the first-ever [eSA certification](#) of an iSIM by the GSMA highlights its security capabilities and flexible connectivity potential. The certification further confirms iSIM's position as the next-generation SIM, offering a future-ready solution in the evolving realm of IoT connectivity.

## Network availability and dependability

The reliability of Cloud SIMs, which depends significantly on network connectivity, might limit the deployment of IoT devices in challenging or remote environments.

These are common settings for IoT devices where network reliability can be a concern.

Inconsistent network connectivity could impair the functionality of Cloud SIMs, making eSIM and iSIM technologies more dependable solutions as they do not share this limitation.

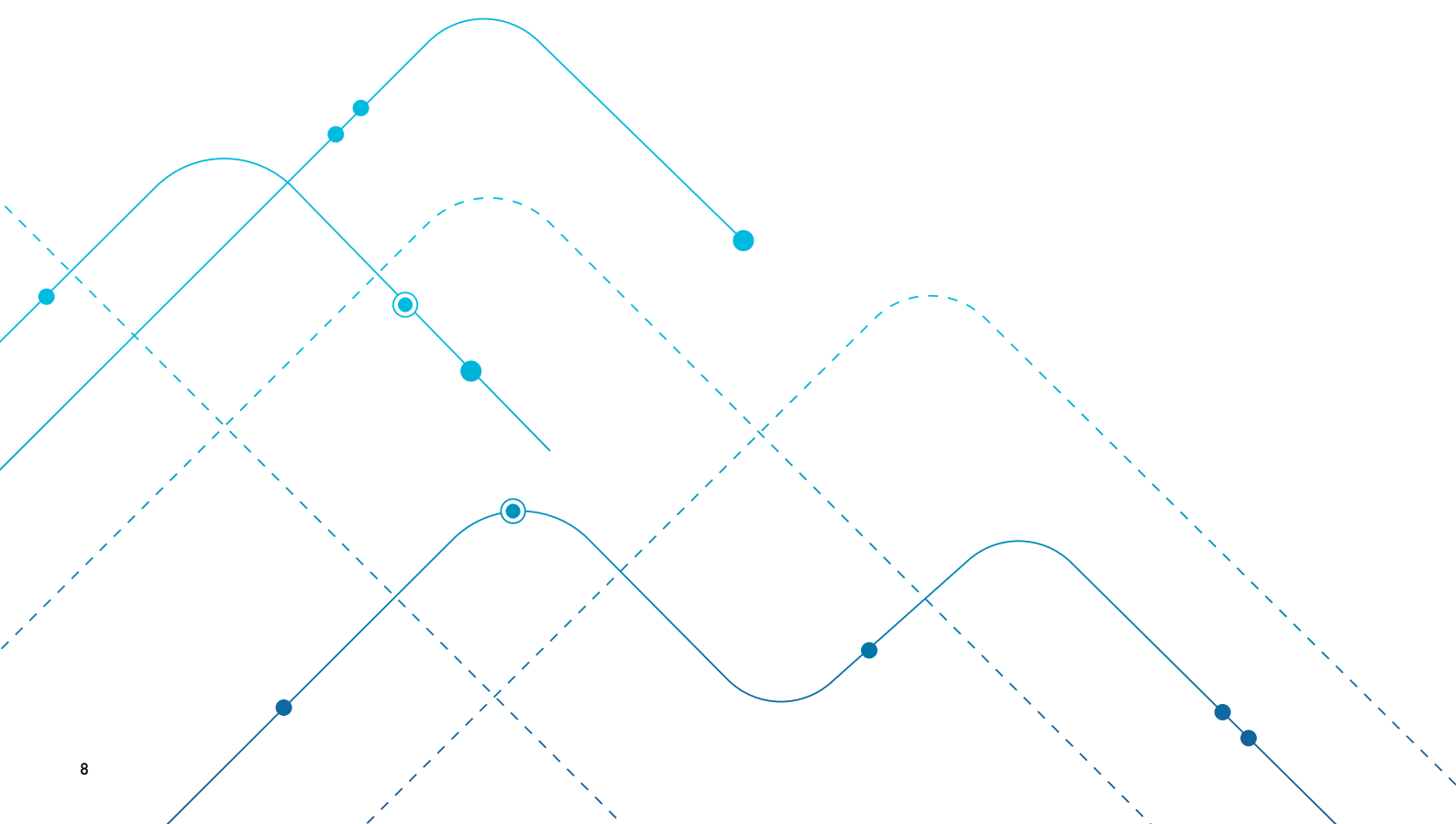
Therefore, the dependence on high-quality network connectivity for Cloud SIMs could potentially restrict IoT operations during network outages or in remote areas.

## Longevity and backward compatibility

Rapid evolution in the IoT domain might outpace software-based SIMs' potential to extend the lifespan of IoT equipment. eSIM and iSIM technologies, backed by global standards and widespread industry adoption, offer backward compatibility and a more future-proof solution.

## Vendor lock-in

The proprietary nature of Soft SIM and Cloud SIM might lead to vendor lock-in, restricting organisations in their choice of other components, devices, or services. This lack of standardisation might lead to increased costs and less flexibility in the future.







## 6. Usage applicability and case-dependence

Each SIM solution brings its unique features and advantages to the table, making them suitable for varying use cases in the expansive world of IoT applications.

However, some notable challenges, particularly related to security, arise with specific solutions, making eSIM/iSIM technology the safer and more reliable choice for sensitive applications.

Let's examine this in the context of various IoT applications.

- **Example IoT application - Connected Cars**

eSIMs, which are by their very nature embedded, are ideal for applications demanding longer device life cycles or those where physical access to the SIM card is challenging.

The realm of [connected cars](#), offering features such as real-time navigation, emergency services, and infotainment, finds eSIMs particularly suitable due to their ability to connect with the most favorable local network, essential for vehicles used internationally or by frequent travelers.

Even though Soft SIM and Cloud SIM technologies might be simple, they can't meet the security required for these types of security sensitive applications.

- **Example IoT application - Smart Grids**

Integrating iSIMs within the secure enclave of the device's System-on-Chip (SoC) saves space and cuts costs.

Moreover, they provide high security, making them appropriate for applications demanding robust trust mechanisms.

Smart grids, requiring secure and reliable data transmission, can benefit significantly from iSIM technology, securing remote connectivity to control the balance between the electrical power supply system's demand and supply.

Even though Soft SIM could also save space and reduce costs, together with Cloud SIM it can't meet the security requirements of such applications.

- **Example IoT application - International Shipping**

International shipping logistics companies can benefit hugely from eSIMs, providing uninterrupted data for tracking and monitoring due to their ability to connect with the most suitable local network in various countries.

Although Soft SIM and Cloud SIM technologies might offer flexibility and potential cost savings, they introduce significant security risks, especially in sensitive applications such as [smart cities](#), medical IoT, and maintenance scenarios.



### **Soft SIM in the context of the Smart City and Medical IoT**

Due to their software-based nature, Soft SIMs are susceptible to hacking, viruses, and malware. In the context of smart cities, a hacked Soft SIM-operated traffic control system could create widespread disorder.

Similarly, a compromised Soft SIM in a remote patient monitoring device in the medical IoT space could reveal or alter sensitive patient data, leading to severe implications for patient privacy and health.

### **Cloud SIM in Maintenance and Remote Connectivity Cases**

While Cloud SIM technology could offer simplicity, it simultaneously creates extra points of vulnerability because of

the continuous information exchange between the device and the cloud server.

For instance, a compromised Cloud SIM controlling an IoT-based predictive maintenance system could lead to incorrect data reporting, potentially causing expensive machinery failure.

Moreover, the reliance on a data connection to access the SIM profile makes Cloud SIMs vulnerable to service disruptions in cases of unreliable or compromised data connections.

In contrast, with the scalability needed in massive IoT applications and the low latency required in critical IoT scenarios, eSIM/iSIM technologies provide a more secure and reliable solution, overcoming the security concerns of Soft SIM and Cloud SIM technologies.

# 7. Comparative assessment

Here, we assess three significant players - eSIM, Soft SIM, and Cloud SIM and assign them scores on key criteria.

These include security certification, security scalability, simplicity, connectivity management, field-proven experience, and connectivity scalability. The ensuing discussion examines these technologies, shedding light on their potential advantages, limitations, and suitability for different IoT requirements.

## eSIM, Soft SIM and Cloud SIM



### Security certification:

This comprises global certifications such as the GSMA specifications, which consequently leads to different Security Assurance Levels.

Compared to other solutions which use self-declared security, eSIM relies on security certifications from external, globally recognised independent bodies and scores the highest because of its unique combination of secure software and hardware. It is built-in and tamper-proof and being adopted increasingly by Mobile Network Operators as well as device manufacturers.

Soft SIM's lack of standardisation could lead to compatibility and regulatory issues. Soft SIM is also software-based and vulnerable to cyber threats.

Cloud SIM similarly presents issues with standardisation for devices and depends on regulatory acceptance. However, the server can be in a secure zone. From the perspective of the devices, Cloud SIM is susceptible to risks similar to those of Soft SIMs.

### Security scalability:

- eSIM: presents scalable security by design and globally recognised certifications
- Soft SIM: device-dependent security, difficult to scale, and security risks due to being entirely software-based
- Cloud SIM: similar risks to Soft SIMs on the devices, reliance on the robustness of infrastructure hosting multiple networks

### Simplicity:

- eSIM: eliminates the need for physical SIMs but requires hardware changes
- Soft SIM: uses downloadable software, allowing easy updates and deployments
- Cloud SIM: ability to switch networks, but depends on internet quality

### Connectivity management:

- eSIM: allows for easier carrier switching
- Soft SIM: no hardware needed but could face regulatory and compatibility issues
- Cloud SIM: potential for better coverage than Soft SIM, but relies on the availability and quality of the internet

### Field-proven experience and future-proofing:

- eSIM: widely supported, standardised SIM technology that has been around for decades. eSIM technology is widely adopted in the automotive sector and growing rapidly in the smartphone industry.
- Soft SIM: security, compatibility and regulatory challenges
- Cloud SIM: about the same as Soft SIM in terms of security, compatibility and regulatory challenges. However, it can be hosted in a secure server.

### Connectivity scalability:

- eSIM: With GSMA SGP.32 standards, it provides scalable and unlimited connectivity by design, where and when it is needed whilst following global standards
- Both Soft SIM and Cloud SIM lack standardisation and are use case dependent; the connectivity cannot scale

These scores are based on our assessments as of July 2023. Also it should be noted that in China, Soft SIM and Cloud SIM are more deployed than all other regions.

## Conclusion: IoT connectivity and SIM technologies

Our exploration of IoT SIMs – from eSIMs and iSIMs to Soft SIMs and Cloud SIMs – highlights the unique benefits and challenges each brings to the IoT landscape.

- eSIMs emerge as a robust solution for most IoT use cases due to their embedded nature, secure global connectivity, and the ability to switch remotely between mobile network operators. Especially suited for applications demanding extended device life cycles or where physical access to the SIM card is impractical, eSIMs offer substantial advantages in areas such as utilities, healthcare, connected cars and similar applications.
- On the other hand, integrated SIMs (iSIMs), with their enhanced security features and chip integration, are primed for applications requiring a high degree of trust and energy efficiency, like smart utilities. They save space, reduce cost, and offer increased security by integrating SIM functionalities into the [SoC](#).
- Soft SIMs and Cloud SIMs, despite their apparent flexibility, introduce significant challenges, such as dependence on network quality, potential security vulnerabilities, and issues with standardisation and compatibility. This severely limits their potential, especially in high-stakes applications like smart cities and medical IoT, and when scalability is required.

As we plunge into an increasingly interconnected future, IoT Service Providers, MNOs, MVNOs and OEMs must make informed decisions.

Your choice of SIM technology goes beyond influencing operational efficiency, form factor, and cost; it also sets the standard for the level of security achievable in your IoT solutions.

Based on our experience, **eSIM technology is the first choice** for its superior flexibility, robust security, and compatibility with a wide range of devices. It is also standardised and enables the interoperability and trust required for the cellular IoT ecosystem.

This technology can serve IoT deployments effectively and efficiently, ensuring a secure and reliable connection while allowing for seamless network transitions.

For devices with lower power requirements or simpler functionality, **transitioning to iSIM technology** can bring further advantages in terms of cost and space savings.

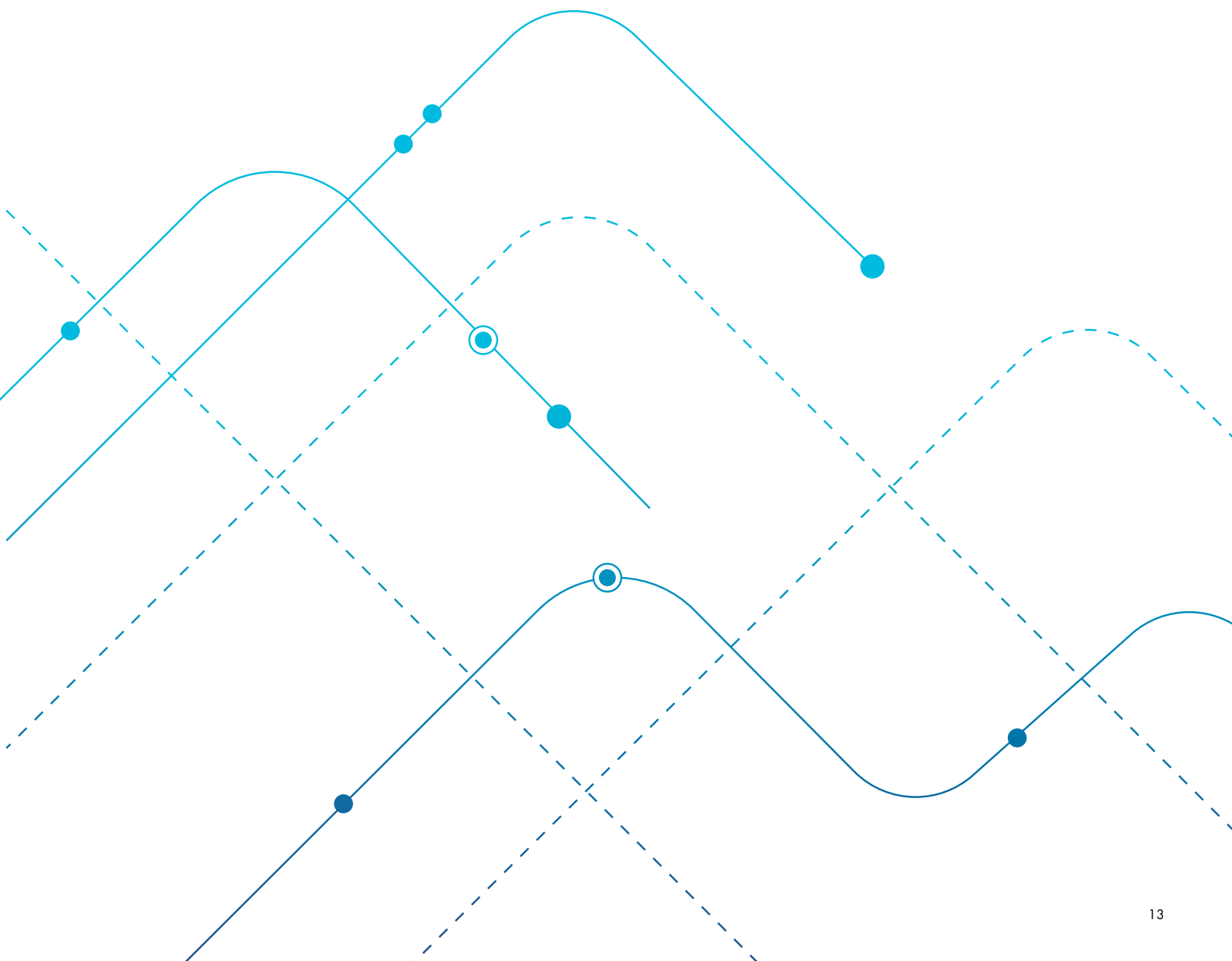
iSIMs' integration into the SoC of devices makes them particularly suitable for compact, low-power IoT devices, enhancing their efficiency and usability.

Remember, the most successful IoT deployments will be those that skillfully balance the need for flexibility, cost-effectiveness, operational efficiency, and, above all, security.

# More resources on **eSIM and other technologies**

---

1. [Global eSIM markets \(March 2023\)](#)
2. [iSIM opens a new world of opportunity for mobile and IoT innovation \(June 2023\)](#)
3. [Internet of Things \(IoT\): Cheat sheet \(August 2022\)](#)
4. [GSMA's eSIM IoT Architecture and Requirements SGP.31 specification \(May 2023\)](#)
5. [Massive IoT: Tech overview, business opportunities and examples \(January 2023\)](#)
6. [What is an eSIM](#)
7. [What is an iSIM](#)
8. [Ruggedized SIM and eSIM](#)



# THALES

Building a future we can all trust

[thalesgroup.com](https://thalesgroup.com)

