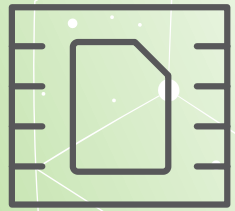
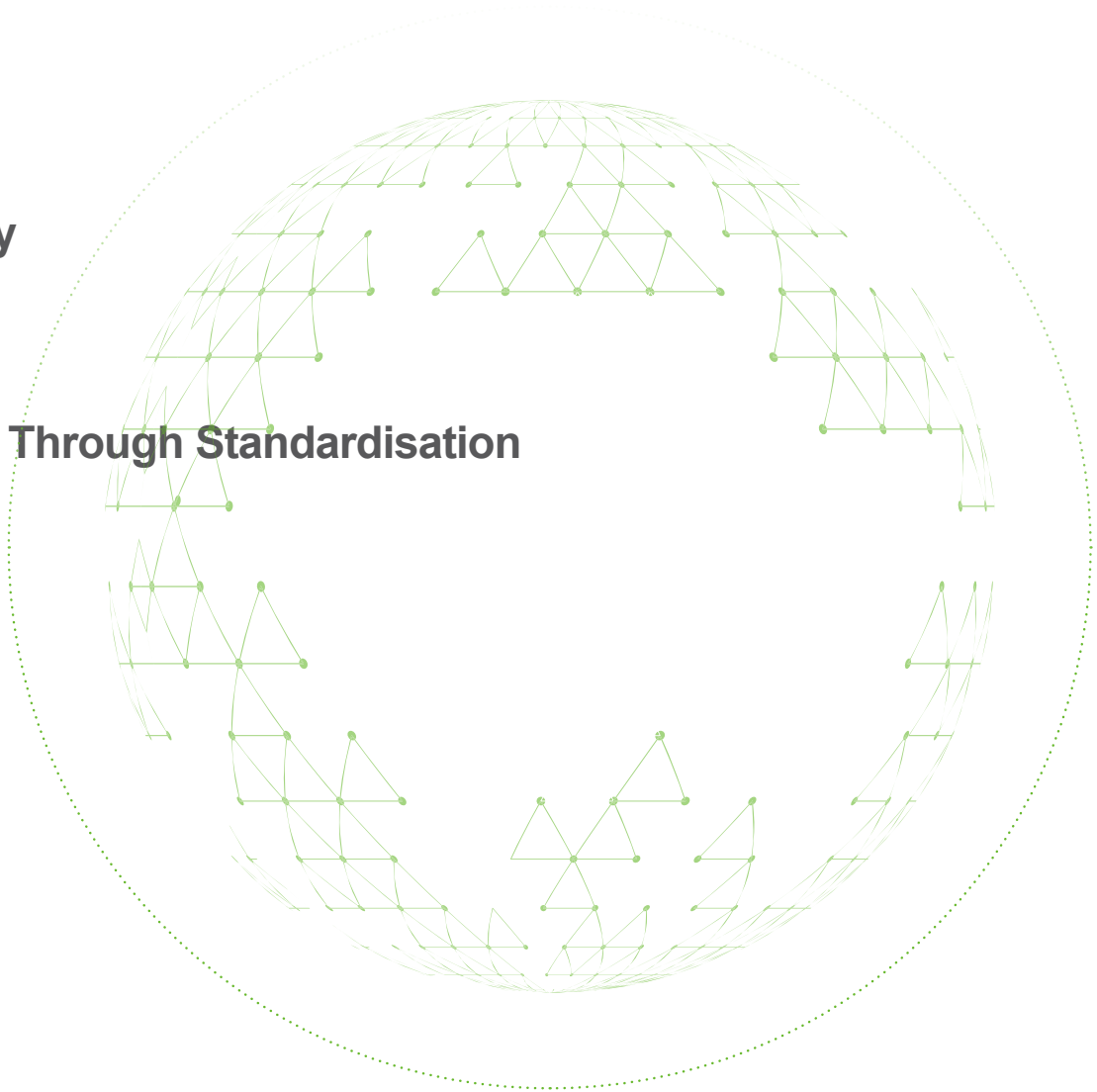
TRUSTED CONNECTIVITY ALLIANCE

Enabling trust in a connected future

Introduction to:
eSIM for IoT



Contents

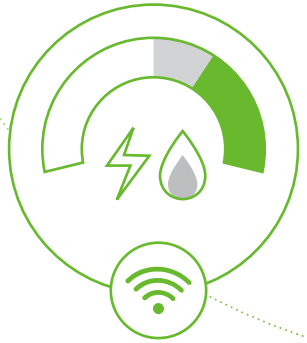


Introduction:
The Emerging IoT Opportunity

The emergence of the Internet of Things (IoT) is one of the defining technological trends of the 21st century, ushering in a new era of connectivity.

By 2027, there are expected to be over 29 billion IoT connections across the globe. *(Source: IoT Analytics)*
A key factor propelling the ongoing expansion of the IoT ecosystem is the growing deployment of low-cost, low-power devices at massive scale (known as massive IoT). These devices, which include smart meters, sensors, asset trackers and smart labels, are transforming industries and verticals such as smart cities, utilities, logistics and manufacturing to enable new use-cases, reveal insights and realise efficiencies.

29bn
IoT connections across the globe.

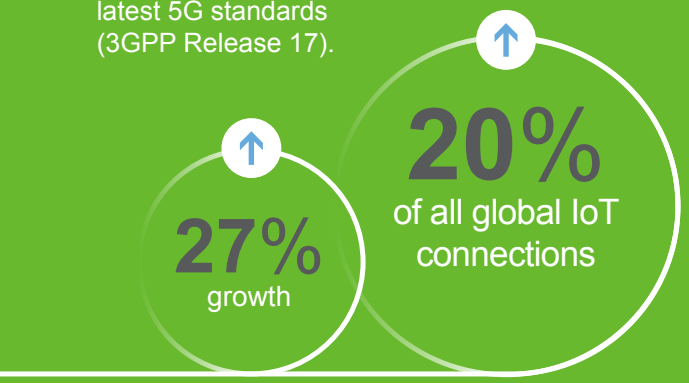


Introduction: The Emerging IoT Opportunity

Given the need for truly trusted, reliable and secure mobile connectivity across many of these industries and use-cases, cellular technologies (2G, 3G, 4G, 5G, LTE-M and NarrowBand-IoT) are increasingly being leveraged to connect IoT devices.

Global cellular IoT connections grew by **27% year-on-year in 2022** – significantly outstripping the overall growth rate – to account for nearly **20% of all global IoT connections.** *(Source: IoT Analytics)*

Looking ahead, the number of deployed cellular IoT devices is set to continue to increase with the new features, enhancements and value-added services introduced in the latest 5G standards (3GPP Release 17).

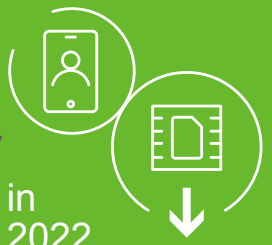


And as deployments increase, so too is the demand for eSIM technology to cut through complexity and promote simplified global connectivity and advanced security for the IoT.

This is demonstrated in the latest market figures reported by Trusted Connectivity Alliance members, which showed significant growth in the global adoption of eSIM technology in 2022. Consumer and M2M eSIM profile downloads collectively increased by 135%. Increased adoption also coincided with the growing deployment of eSIM-enabled devices, as eSIM shipment volumes increased 13% year-on-year to reach 382 million units.

Consumer and M2M eSIM profile downloads collectively increased by

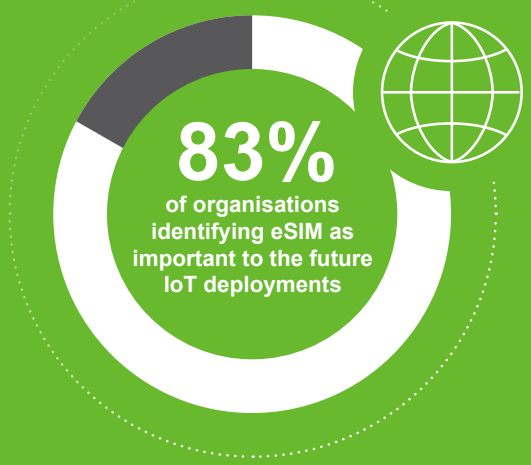
135% in 2022



eSIM shipments reported by TCA members increased by

13% year-on-year

to reach **382 million** units



Growth is set to continue, with **83%** of organisations identifying eSIM as important to the success of future IoT deployments. *(Source: GSMA Intelligence).*

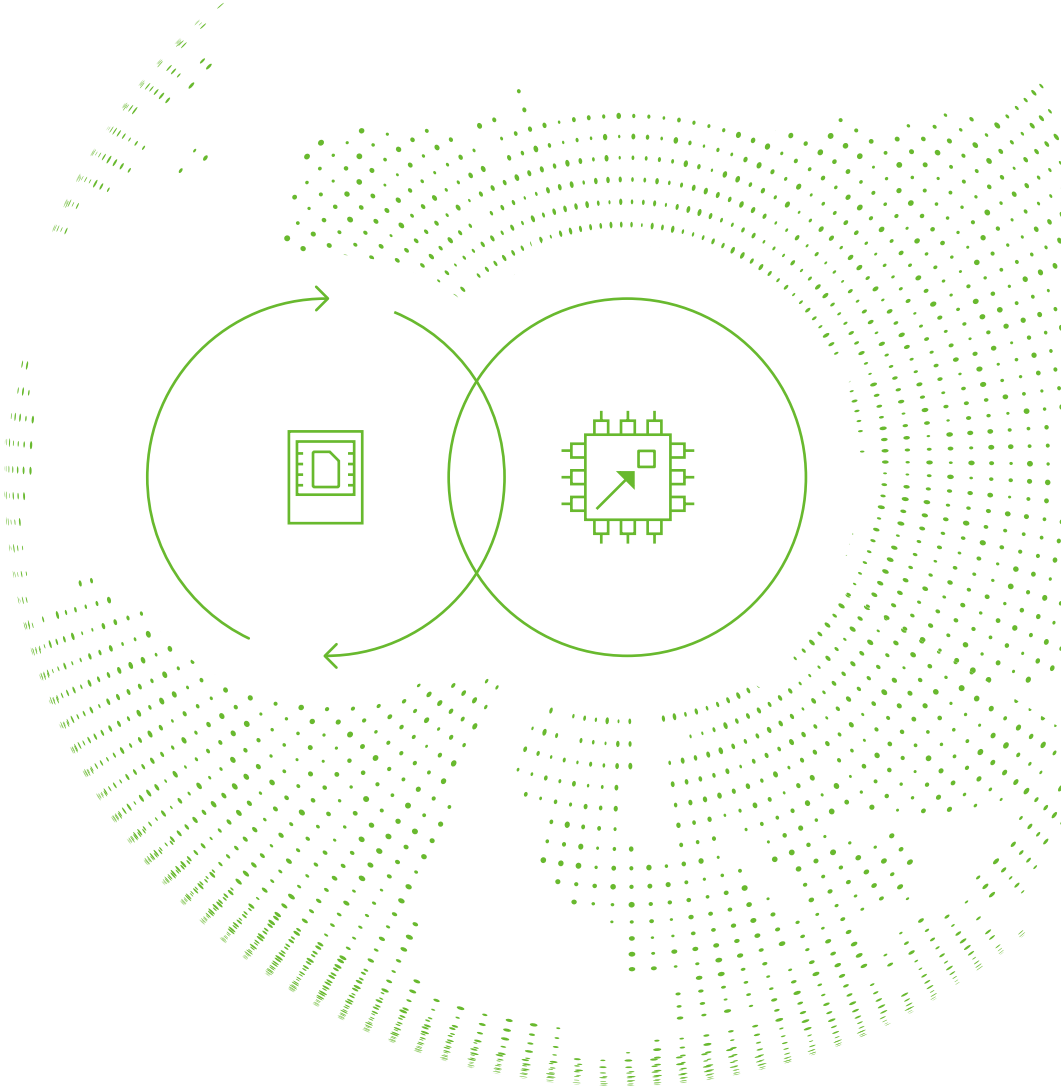
This marks a significant opportunity for stakeholders across the secure connectivity ecosystem to leverage eSIM technology to unlock the full, transformative potential of the IoT.

eSIM:
Unlocking the Potential of the IoT

An eSIM is a 'digital SIM' that can store multiple operator profiles (the combination of subscriber data and applications that provide secure connectivity to cellular networks) and be remotely managed in accordance with GSMA's Remote SIM Provisioning Specifications.

Remote SIM Provisioning refers to the process of downloading, installing, enabling, disabling, and deleting a profile on an eSIM. Remote SIM Provisioning is enabled by specialised secure servers called eSIM Subscription Manager (SM) platforms.

While 'eSIM' originates from the term 'embedded SIM' and can be soldered directly into the device, it is available in various form factors. This includes integration within a secure enclave on a System-on-Chip (SoC) – known as an integrated SIM.



The unique capabilities of eSIM technology deliver various benefits to support scalable and secure IoT deployments.

Globally reliable, flexible connectivity

Enabled by GSMA's Remote SIM Provisioning specifications, eSIM technology removes the need to physically change out a SIM card when switching to a different mobile operator. This addresses the prohibitive costs and logistical challenges associated with deploying and managing devices globally, delivering the flexibility and scalability required to unlock emerging cellular use-cases spanning the IoT ecosystem, anywhere in the world and across borders.

Advanced, dynamic security

An eSIM shares the advanced cryptographic features of the SIM, including a securely designed central processing unit and dedicated secure memory to store operating system programmes, keys, and certificate data, protect devices from various hacking scenarios, such as cloning, physical attacks to a single device, and remote attacks to many devices. eSIM functionality also enables remote upgrades to sensitive data, apps and subscriptions according to GSMA and GlobalPlatform specifications so that a device can immediately respond to emerging threats and attacks once it is live in the field.

End-to-end digitalisation

eSIM technology supports full end-to-end digitalisation, which enables operators and device manufacturers to simplify supply chains and production flows, significantly reducing manufacturing, distribution and transportation costs.

While eSIM technology is already widely utilised across IoT deployments, industry standardisation efforts now promise to address long-standing challenges.

Enabling device evolution

The eSIM is significantly smaller than the nano-SIM and can be soldered to the device, which enables manufacturers to develop more streamlined, powerful devices with longer battery life. Waterproofing, ruggedization and the ability to withstand hazardous environments also supports increasing demand for emerging industrial use-cases. In addition, the integrated SIM form factor reduces the number of components to support the development of smaller, thinner devices, while optimising power consumption to increase battery life.

Accelerating eSIM Adoption Across the IoT Through Standardisation

Industry standards offer significant benefits to technology ecosystems. A key benefit of eSIM technology is that it is supported by an advanced, mature infrastructure that promotes interoperability and security.

Standardisation activity for eSIM has been led by GSMA, the global industry association. Namely, GSMA created the Remote SIM Provisioning Specifications for M2M and Consumer Devices:

GSMA eSIM Solution for M2M – addresses devices where the profiles are managed remotely by the operator, and not the end-user.

GSMA eSIM Solution for Consumer Devices – addresses smartphones and other consumer devices where the end-user activates the profile or switches operator.

Accelerating eSIM Adoption
Across the IoT Through Standardisation

Yet the growth of the IoT ecosystem presents unique and challenges. Two primary challenges are:

1 Constrained IoT Devices

As the IoT ecosystem grows to encompass new verticals and use-cases, there are an increasing number of IoT devices deployed that have limited bandwidth (network constrained), limited or no user interface (UI constrained), and limited power (power constrained).

In particular, network constrained and UI constrained devices across the IoT ecosystem present significant challenges as they cannot be optimally managed using the existing GSMA Consumer and M2M Specifications.

For example, the M2M Specification requires an SMS or HTTPS connection for profile downloads and management, which network constrained devices cannot support. Similarly, many IoT devices lack a UI to enable an end-user to trigger or approve a profile download.

2 Integration Complexity

A challenge associated with the M2M Specification is that it requires complex integration processes between different operators, which makes it difficult to switch profiles between providers. While this model works for verticals such as automotive, its inflexibility is unsuited for IoT use-cases.

For example, an asset tracker in a shipping container needs to be able to connect to different providers across jurisdictions. Device manufacturers may also not know where their products will be deployed so, as they have to select an operator during production, multiple production lines must be established to address different geographies.

The Consumer Specification offers a more streamlined approach, but the limitations of UI constrained devices (as outlined above) reflect a need for a simpler model dedicated to the IoT.

The industry has recognised that enhancing the eSIM infrastructure to meet these specific IoT requirements is crucial. In response, GSMA has worked with industry stakeholders to develop and publish the eSIM for IoT Specifications (SGP.31 and 32).

GSMA™

Introducing eSIM for IoT

The new specification builds upon proven elements of the existing Consumer Specifications, while introducing new, dedicated features to address specific IoT considerations.

This includes:

• eSIM IoT Remote Manager (eIM)

The eIM is a standardised, remote provisioning tool that enables profiles to be downloaded and managed on a single IoT device or a fleet of devices. This removes the requirement for direct consumer interaction or complex, inflexible integrations, simplifying IoT deployments at scale. The eIM also supports lightweight communication protocols to address network constrained devices.

• IoT Profile Assistant (IPA)

Within the Consumer Specification, a feature called the Local Profile Assistant (LPA) enables users to download a profile from the operator's eSIM Subscription Manager platform (known as the SM-DP+). The IoT Profile Assistant (IPA) replaces the LPA used within the Consumer Specification and provides the functions that enable the eSIM to be remotely managed using the existing SM-DP+ platform infrastructure. It can either reside on the device (IPA.d) or on the eSIM (IPA.e).

• Lightweight IoT Minimal Profile

TCA's Interoperable Profile Package Specification – which is used in every eSIM deployed in the field – standardises the format used for the remote loading of subscriptions onto eSIMs across deployed devices. This enables mobile operators to load interoperable connectivity profiles in an eSIM, regardless of the SIM vendor.

A key update in Version 3.3 of TCA's Interoperable Profile Package Specification is the definition of a 'lightweight' IoT minimal profile to address the growing challenge of remotely managing network constrained IoT devices.

This makes it possible to provision a profile even when bandwidth is very limited, which is crucial to supporting the growing use of eSIM technology to support constrained devices and enable various IoT use-cases and connectivity services. Given these benefits, Version 3.3 is referenced in SGP.32.

Testing and Compliance

Work is now progressing on the associated test specifications and compliance programme, with TCA playing a key role shaping the development within GSMA. The aim is for this activity to be finalised by end-2024.

What's Next:
Advancing eSIM for IoT

The publication of a dedicated standard for remotely provisioning and managing IoT devices is a game-changing development that promises to accelerate the adoption of eSIM technology and unlock the full, transformative potential of the IoT across established and emerging use-cases.

While it will take some time for the first fully compliant solutions to be launched, it is anticipated that over half of active eSIMs across IoT deployments will be compliant with the new specification by 2028. *(Source: Kaleido Intelligence)*

But the work does not stop there. The growth of the IoT ecosystem will continue to present new challenges spanning connectivity, interoperability, security and privacy.

For this reason, TCA is committed to bringing together leading industry stakeholders to shape the ongoing standardisation and enhancement of eSIM technology and the supporting infrastructure. This includes continuing to be a key contributor to GSMA to further guide and support the development of its eSIM-related specifications and testing processes.

About Trusted Connectivity Alliance

Trusted Connectivity Alliance (TCA) is a global, industry association working to enable trust in a connected future. The organisation's vision is to drive the sustained growth of a connected society through trusted connectivity which protects assets, end user privacy and networks.

TCA members are leaders within the global Tamper Resistant Element (TRE) ecosystem and work collectively to define requirements and provide deliverables of a strategic, technical and marketing nature. This enables all stakeholders in our connected society to benefit from the most stringent secure connectivity solutions that leverage TCA members' expertise in tamper proof end-to-end-security.

TCA members:

COMPRION
card centric
东信和平 EASTCOMPEACE
Giesecke+Devrient
IDEMIA
Kigen
Linxens
NXP
OASIS smart sim
Qualcomm
life.augmented
THALES
Valid
WORKZ
Watchdata
TIANYU
XH Smart