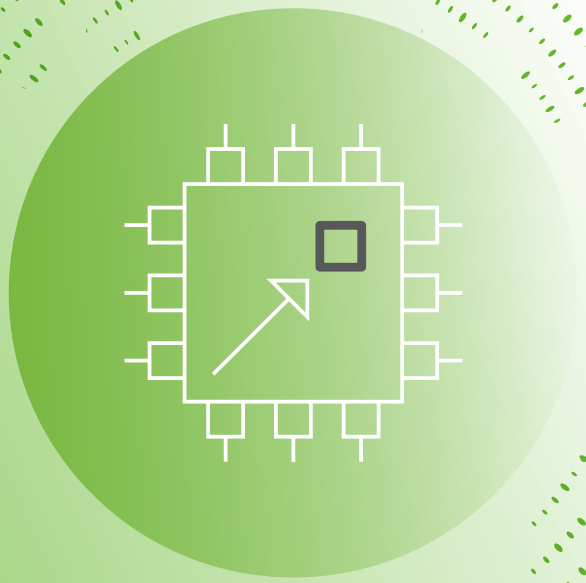
TRUSTED CONNECTIVITY ALLIANCE

Enabling trust in a connected future

Introduction to: integrated SIM

Understanding the drivers, concept and use-cases of integrated SIM technology



Contents

TRUSTED CONNECTIVITY ALLIANCE

1.
The drive for integration in a connected world

TRUSTED CONNECTIVITY ALLIANCE

Cellular networks are foundational to our globally connected world. As of Q4 2021, mobile connections for consumer and IoT devices reached nearly 10.5 billion (Source: GSMA).

The SIM applications that enable authenticated access to cellular networks are incorporated within connected devices via highly-secure Tamper Resistant Elements (TREs).

TREs are available in removeable and embedded form factors which are deployed across billions of devices globally.

As the vast mobile ecosystem continues to expand, the need for trusted connectivity and the highest-levels of device security remain paramount.

Importantly, TRE-based SIM form factors have a unique ability to offer the most stringent end-to-end security. This leads to trusted connectivity between the device and cellular network and supports the delivery of unsurpassed security features and services, which can be used by devices and / or the applications they run.

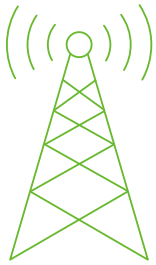
As of Q4 2021, nearly

10.5 billion

mobile connections

for consumer and IoT devices were powering the increasing digitalisation of lifestyles, commerce and industry

(Source: GSMA).



What is a TRE?

A TRE is a standalone secure element or secure enclave, consisting of hardware and low level software providing resistance against logical and physical attacks, capable of hosting secure applications and their confidential and cryptographic data.

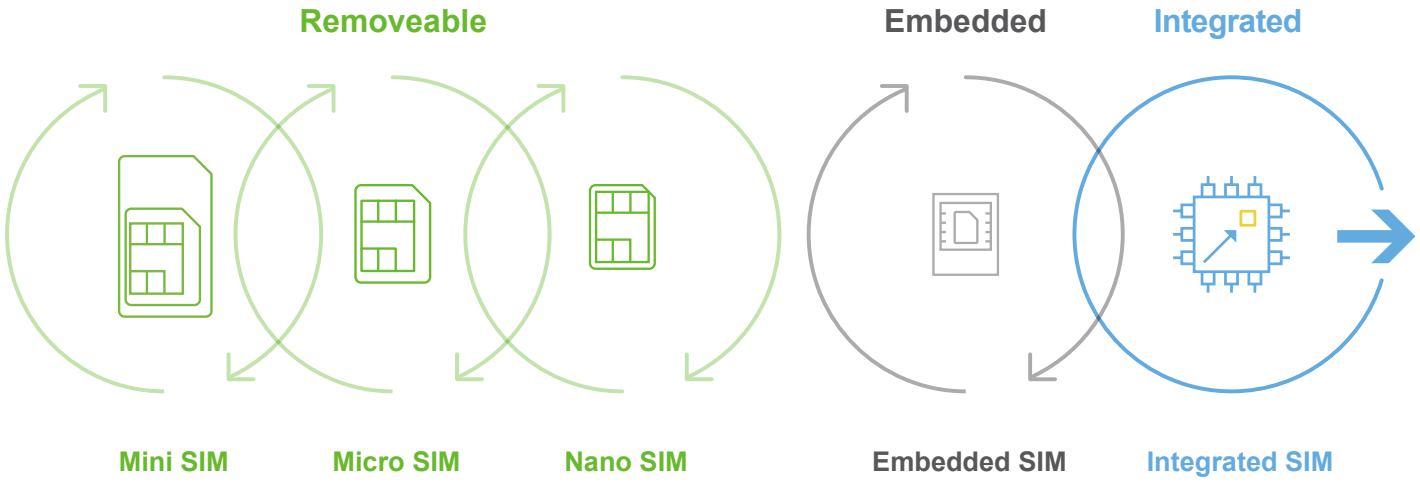
TRUSTED CONNECTIVITY ALLIANCE

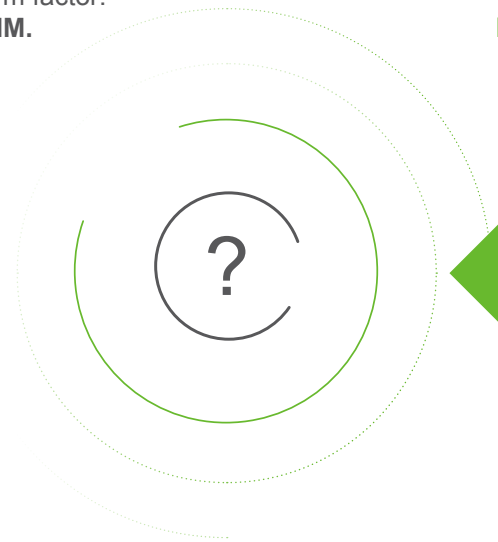
Integration: The next stage of SIM evolution

Innovation and evolution are at the heart of the SIM industry's relevance and longevity. SIM form factors have become progressively smaller and more advanced over time – while retaining the highest security levels - to support the emergence of different applications and use-cases.

And in recent years, various market forces have promoted the integration of SIM functionality on a System on Chip (SoC).

This has created increasing demand for a new TRE form factor: **the integrated SIM.**





What is a System on Chip?

A System on a Chip (SoC) is an integrated circuit – also known as a 'chip' – that integrates all or most components of a computer or other electronic system.

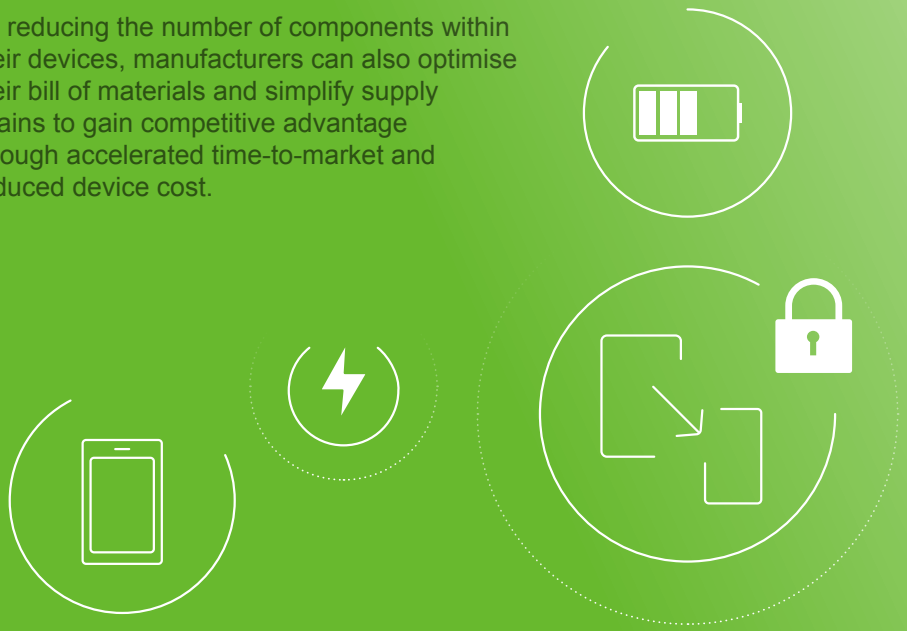
TRUSTED CONNECTIVITY ALLIANCE

Device miniaturisation: Smaller, better, faster, stronger

To meet consumer demand and counter increasing competition, manufacturers are developing cellular devices that are smaller, thinner and tougher – all while delivering more features, functionality and aesthetic appeal.

As a result, cellular devices are undergoing a sustained cycle of miniaturisation. This is the process of removing or integrating components to reduce device size or make room for more or expanded features, such as larger batteries and user interface displays. The reduction and / or removal of components can also reduce power consumption to increase battery life.

By reducing the number of components within their devices, manufacturers can also optimise their bill of materials and simplify supply chains to gain competitive advantage through accelerated time-to-market and reduced device cost.



The need to retain security in a digitalised and miniaturised world

The rapid growth of today's globally connected world has led to the need for trusted connectivity solutions that can be used by an increasing variety of devices in a digital context. This has led to further evolution within the SIM ecosystem. The eSIM has already driven the 'digitalisation' of SIM technology, enabling subscriber profiles to be delivered and managed remotely.

As digitalisation and miniaturisation continue, it is imperative that the security assurances provided by the SIM in its traditional hardware / software form factor are not compromised through software-only digital delivery. This need to retain SIM security levels is driving integration of the SIM functionality within a secure enclave on a SoC.

TRUSTED CONNECTIVITY ALLIANCE

5G: A tipping point?

The expansion of 5G networks is driving significant connectivity advances, including improved speed, latency, capacity and efficiency. This is a catalyst for further increases in connected device types and use cases.

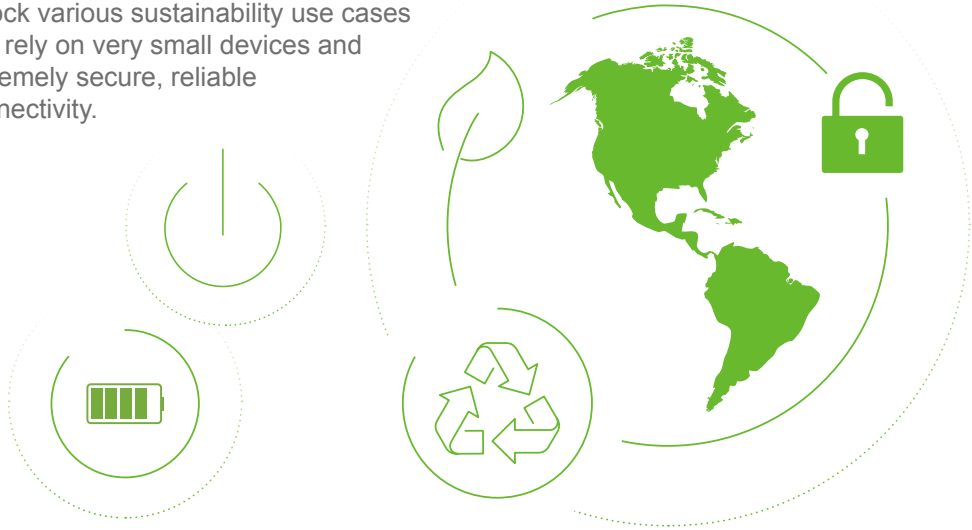
5G launches will likely drive device renewal, as consumers look to get their hands on the latest 5G-enabled tech. Mobile SoC manufacturers will also look to include new features and functionality to improve user experiences and maximise opportunities presented by new network technologies. This offers a natural juncture for the introduction of new technologies, such as the integrated SIM, to unlock performance and security benefits.

Integrate for the environment

With the climate crisis an increasingly urgent focus, developing sustainable technologies which run on low power, consume less resource and generate less waste has become a global priority.

Integration promises huge environmental benefits. For example, the integration of components within a device leads to reduced power consumption and smaller physical footprints thanks to fewer connectors and interfaces. And considering the massive and continued growth across connected devices, the collective annual efficiency gains enabled by integration could be significant.

Beyond making connected devices ‘greener’ themselves, integration also promises to unlock various sustainability use cases that rely on very small devices and extremely secure, reliable connectivity.

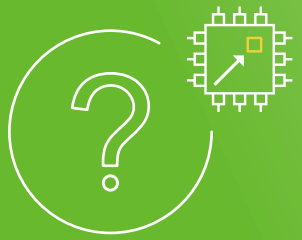


TRUSTED CONNECTIVITY ALLIANCE

2.
Integrated SIM: What, why and how?

Given these drivers, there have been various different industry initiatives over recent years to define and commercialise integrated SIM functionality for consumer and IoT devices.

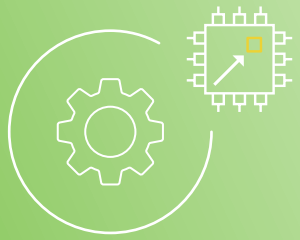
So, what exactly is an integrated SIM, when should it be considered, and how is the industry working to progress all-important standardisation initiatives?



What is an integrated SIM?

Integrated SIM solutions deliver the highest levels of security assurance already associated with other SIM form factors. To achieve this, SIM functionality is implemented on a hardware TRE integrated within a host SoC.

It has a well-defined physical boundary, as well as a set of interfaces to the host SoC, and is self-contained from a security perspective. As a result, it does not rely on any protection mechanisms of the host SoC. In fact, it can be thought of as a miniaturised smart card integrated within the SoC, which becomes its operational environment.



Why the integrated SIM?

Solutions like software-based SIM – where SIM functionality is implemented in pure software - and Trusted Execution Environment (TEE)-based SIM solutions – where SIM functionality is implemented within an isolated environment on the device's main processor – have been commercially deployed in limited markets for specific use-cases.

However, these solutions are strictly regional and lack global interoperability as well as security assurance levels that are required for most applications. This increases market fragmentation risk, product development costs and the potential for premature obsolescence.

In contrast, the trend towards integrated SIM is supported by significant industry-wide specification development and global, open standards.

How is the industry standardising the integrated SIM?

Internationally recognised industry associations and standard development organisations are already delivering specifications and definitions for the TREs enabling integrated SIM functionality.

The most notable are GSMA's integrated eUICC standards (which are now available and being deployed commercially) and ETSI's iSSP. In addition, Eurosmart is facilitating security certification efforts.

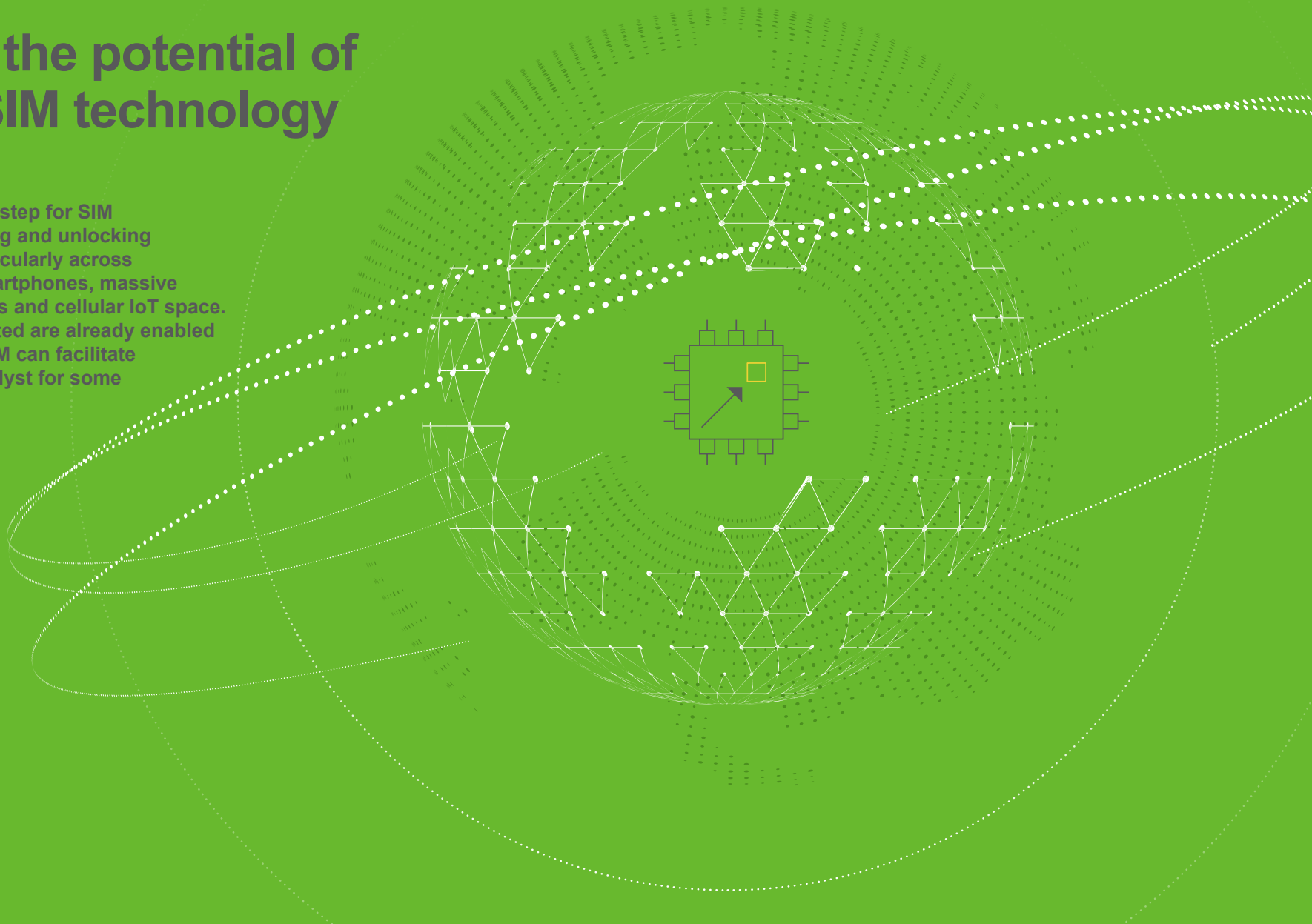
Already, it is clear that these global efforts to standardise nascent integrated SIM technology have been successful and that integrated SIM solutions which align with open standards can now be recognised for their high levels of security assurance and global interoperability.

Looking ahead, there are opportunities to drive further enhancements in the future through the reduction of the overall time and cost of certification for integrated SIM solutions, without compromising quality.

3.

Harnessing the potential of integrated SIM technology

Integration is an evolutionary step for SIM technology which is expediting and unlocking a host of new use-cases, particularly across cellular devices including smartphones, massive machine-type communications and cellular IoT space. Although all the use cases listed are already enabled by the eSIM, the integrated SIM can facilitate their adoption by being a catalyst for some new device categories.

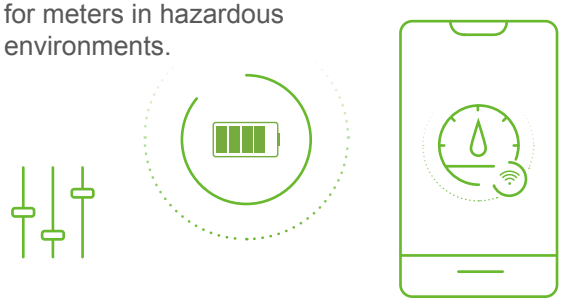


Integrated SIM for:

Utilities

Connectivity for smart meters requires reliable, robust security, as well as long battery life to support devices that can be in the field for several years.

An integrated SIM offers significant power-saving benefits and can remain operational for ten years with a life-time battery. The very nature of the integrated SIM form factor also provides further assurances to utility companies that it cannot be removed or swapped to falsify consumption data. It also offers improved robustness from its integrated design, ideal for meters in hazardous environments.



Logistics

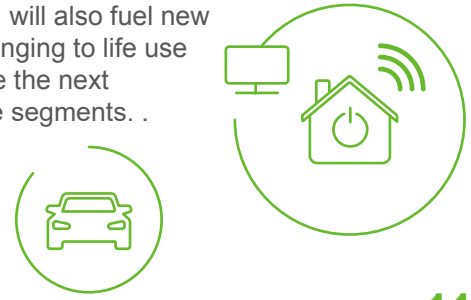
The COVID pandemic has exposed vulnerabilities in global supply chains, highlighting an increasing requirement for real-time information to support logistics at all levels.

Smart labels, which allow near real-time monitoring of supply chains, are one example of how devices enabled with integrated SIM functionality can be leveraged to meet that requirement, using Low Power Wide-Area Network (LPWAN) connectivity. For example, suppliers can track large quantities of goods on a global scale and take immediate corrective action if needed (e.g. an alert could be triggered if there is a sudden change in temperature or humidity that would damage the goods).

Consumer devices (health / lifestyle)

Fitness and health wearables have become hugely popular with hundreds of millions of units sold each year. However, limited battery life is the main pain point and many need to be charged daily. Maximising the power of the in-built battery with no compromise on features is a priority for manufacturers. As integrated SIM technology helps to optimise the device real estate and reduces the power budget significantly, it could usher in a new era of personal health sensors.

Of course, wearables go far beyond health and fitness. Smart watches and connected AR / VR glasses, for example, are poised for significant growth with the advent of 5G and will be among the first devices to benefit from the integrated SIM. Given the small size requirement and in-built battery, user comfort and aesthetic appeal relies on the power budget being maximised. The integrated SIM will also fuel new device features, bringing to life use cases that will drive the next generation of those segments. .



TRUSTED CONNECTIVITY ALLIANCE

4.

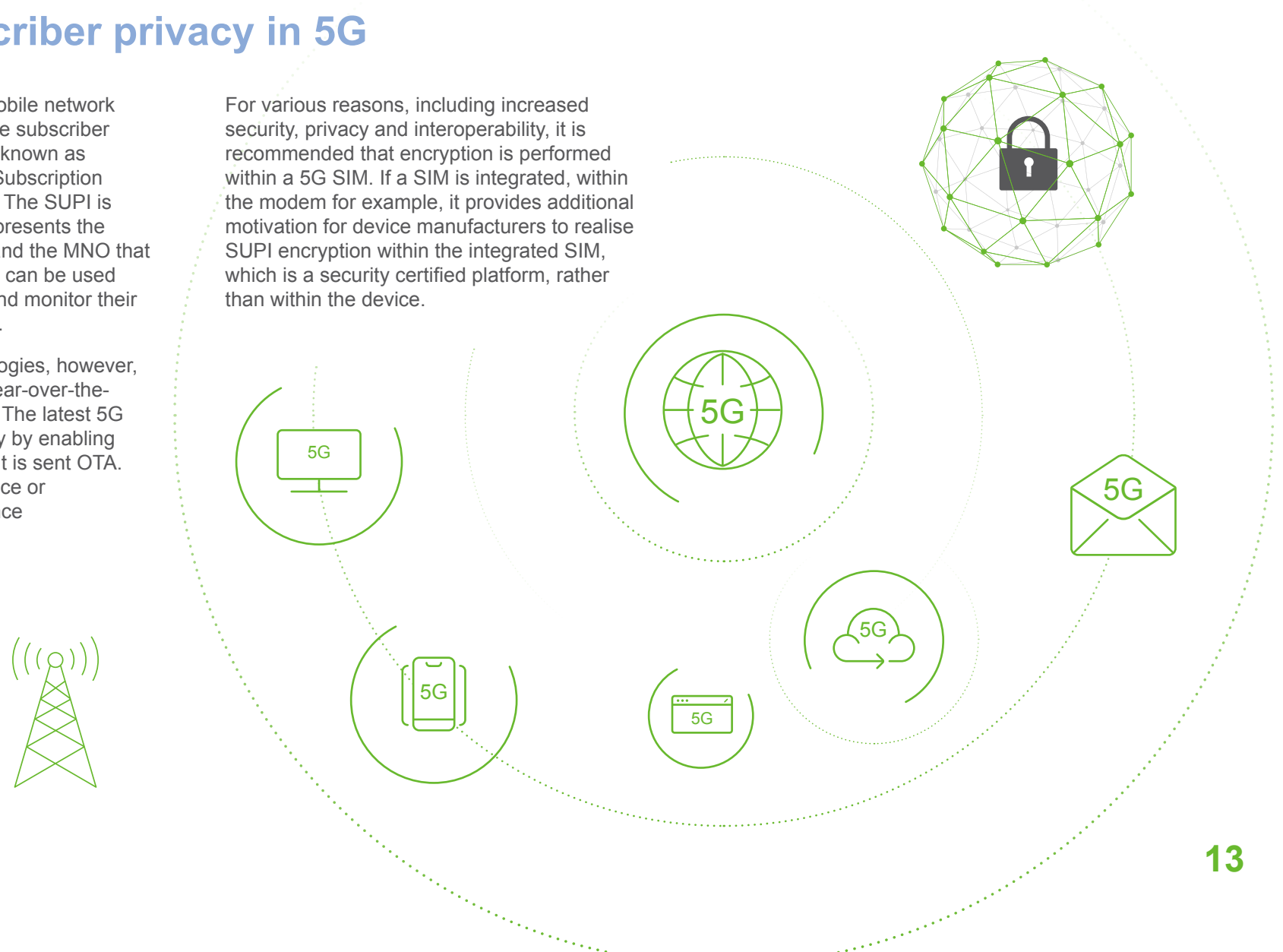
Leveraging the benefits of integration for device security features

Enhanced subscriber privacy in 5G

In mobile network technologies, mobile network operators (MNOs) allocate a unique subscriber identifier to each SIM card. This is known as an IMSI in 2G, 3G and 4G, and a Subscription Permanent Identifier (SUPI) in 5G. The SUPI is deeply private information, as it represents the relationship between subscribers and the MNO that issued the SIM card. This means it can be used to confirm a subscriber's identity and monitor their location, calls and SMS messages.

In 2G, 3G and 4G network technologies, however, the subscriber identity is sent in clear-over-the-air (OTA) without being encrypted. The latest 5G standards address this vulnerability by enabling MNOs to encrypt the SUPI before it is sent OTA. This can happen either on the device or within a Trusted Connectivity Alliance Recommended 5G SIM, eSIM or integrated SIM.

For various reasons, including increased security, privacy and interoperability, it is recommended that encryption is performed within a 5G SIM. If a SIM is integrated, within the modem for example, it provides additional motivation for device manufacturers to realise SUPI encryption within the integrated SIM, which is a security certified platform, rather than within the device.



TRUSTED CONNECTIVITY ALLIANCE

Protection for device and other digital identities

In the same way that it can protect subscriber privacy, the integrated SIM can offer secure storage capabilities for many types of security sensitive digital identities.

For example, if implemented within a modem processor, it can ensure secure storage of the device identity (also known as the IMEI). Device counterfeit detection schemes can rely on a pair of hardware tags (the device identity, embedded SIM identity and the integrated SIM identity) therefore improving existing counterfeit detection. The reliability of such counterfeit detection schemes benefits from a deeper integration of the integrated SIM.

User friendly biometric authentication

Since the integrated SIM uses the same hardware technology as the SoC, it is able to run at high frequency. The calculation speed and processing power of the integrated SIM enables it to handle highly sensitive and performance demanding applications. This means that user friendly, but privacy sensitive, operations such as biometric user authentication could, for example, be performed within the integrated SIM to replace a PIN code.

Summary:

- TRE form factors including the SIM and eSIM are already deployed across billions of devices, delivering connectivity and unsurpassed security features and services.
- The integrated SIM is a new, innovative TRE-based SIM form factor that sits alongside the established eSIM.
- It can bring numerous benefits to various secure connectivity use cases which require small SIM dimensions, low energy consumption, or high levels of accessible memory and/or advanced computing power.
- Global efforts from recognised industry bodies, including GSMA, to standardise nascent integrated SIM technology have been successful.
- This means integrated SIM technologies can provide the highest security and interoperability levels to match the SIM and eSIM, expediting and unlocking a host of secure connectivity use cases.

Download **'Integrated SIM Functionality: Drivers, Approaches to Standardisation and Use Cases'** for a deeper-dive into market forces driving the integration trend, the concept of the integrated SIM, current industry standardisation efforts, key emerging use cases, and the benefits of integration for device security.

About Trusted Connectivity Alliance

Trusted Connectivity Alliance (TCA) is a global, non-profit 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:

Giesecke+Devrient Creating Confidence
IDEMIA augmented identity
life.augmented
THALES
Valid
Kigen
NXP
CARD CENTRIC LIMITED
东信和平 EASTCOMPEACE
OASIS smart sim Embed. Connect. Activate
Linxens crafting the future of connections
Qualcomm
WORKZ
TIANYU
COMPRION