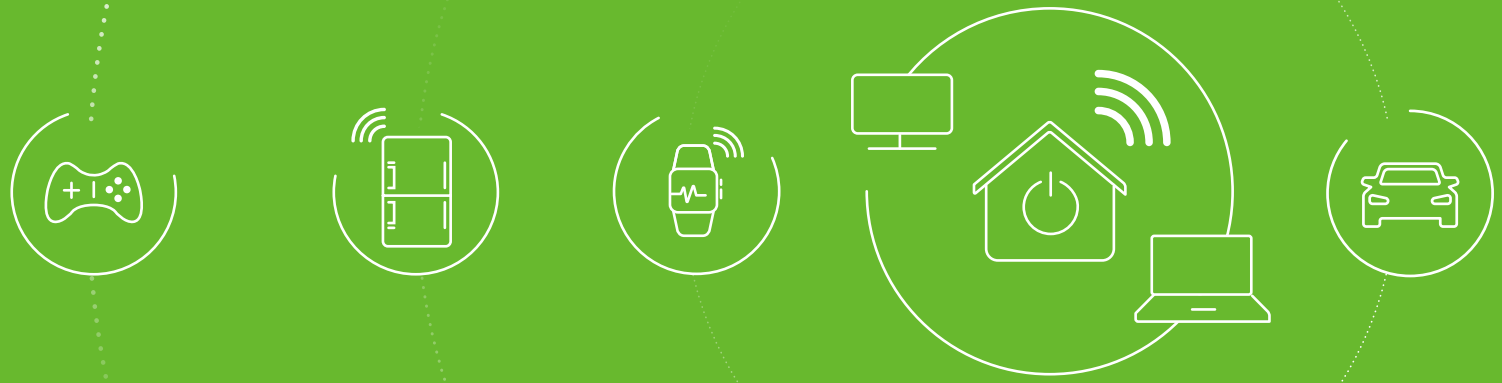
TRUSTED CONNECTIVITY ALLIANCE

Enabling trust in a connected future

A Trusted Connected Future:

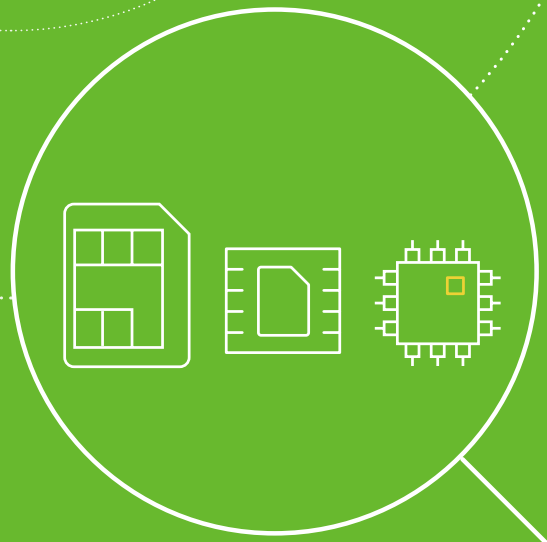
How Tamper-Resistant Elements (TREs) Can Secure the IoT



Aim

Addressing security and privacy vulnerabilities in the Internet of Things (IoT) landscape is an urgent priority. This is reflected by growing intervention from regulators, standards bodies and government authorities, many of whom emphasise similar security principles and best-practices which only hardware technology can provide.

This ebook explores IoT security challenges and outlines how they can be overcome by Tamper Resistant Elements (TREs). In addition to offering stringent, end-to-end security capabilities, TREs are already deployed in billions of devices globally. Many audiences are unaware that SIM products in all form factors – the removeable SIM eSIM and Integrated SIM – are built on TREs. While the SIM application on the TRE provides trusted connectivity between the device and cellular network, there is vast and untapped potential for the TRE to be used far more widely in connected devices for unsurpassed security features and services.



Contents

A world with limitless connection opportunities

Today, nearly everything can be connected. Wearables, tablets, PCs, cars and ordinary household appliances such as baby monitors, kettles and fridges, are all part of the growing IoT ecosystem.

In parallel, the Industrial Internet of Things (IIoT) is revolutionising the manufacturing, energy, and agriculture sectors, among others. Smart factories alone are projected to unlock nearly two trillion USD through productivity gains by 2023.[2]

Public sector services and critical infrastructure such as city-wide traffic lighting systems, hospitals, and power networks are also increasingly connected.

Yet potential brings challenge. Connection on this scale exposes homes, hospitals, power plants and other critical infrastructure to a new class of security threat: cyberattacks.

By 2025, the estimated revenue of the global IoT market will be over

900 billion USD[1]

[1]GSMA, 'IoT Revenue: State of the Market 2020', Aug 2020.
[2]Capgemini, 'Smart Factories at Scale', Nov 2019.

The IoT landscape is notoriously under-secured. In the rush to meet demand, many manufacturers have adopted a 'connect first, think later' strategy, where security has been an afterthought.

But once connected to the internet, traditionally offline systems and devices become vulnerable to cybercrime. Attacks can take different forms:

Understanding security:
Think first, connect later

Attacking a single device

Proximity hacks can steal passwords and valuable personal data, or install spyware or ransomware. While hacks limited to one device may initially seem to only impact a small number of stakeholders, the consequences can be significant.
Real-life scenarios include:

A connected car being hacked as it travels along a busy highway.

Baby monitors and childrens toys being hacked to enable criminals to watch, and even directly communicate, with children.

A smart meter being illegally monitored so a criminal knows whether a house is occupied.

Attacking at scale

An attack on critical infrastructure could bring society to a standstill, devastating the supply of food and utilities, transportation networks, healthcare and other key services. This is no longer a sci-fi scenario; in recent years several such attacks have occurred.

A German steelworks partially exploded following a hack in late 2014.

A similar attack in 2015 shut down a major Ukrainian electricity plant for several hours.

IIoT infrastructure is particularly vulnerable to DDoS (Distributed Denial of Service) attacks. These weaponize a critical mass of insecure IoT devices which are used to attack networks and web-based infrastructure. A notorious example is 2016's Mirai botnet attack, which brought down European and US websites including Twitter, the Guardian, Netflix, Reddit, and CNN.

Insecure-by-design?

A key part of the security challenge is that innovation has outpaced security and privacy across the IoT landscape. Manufacturers of traditionally offline products have not previously had to consider the digital security and privacy implications of their products. This has resulted in a significant knowledge and capability gap. Device vulnerability is not always prioritised in the design process.

When security and privacy 'by-design' is neglected, end-users and actors in the connected value chain are left vulnerable.

Limited end user awareness adds to the problem of device security, with many users neglecting to take simple precautions such as changing default passwords – a seemingly minor issue, yet one which provided a platform for the Mirai botnet attack to be successful.

Securing connectivity:
Increasing IoT regulation

Growing consensus on the urgency of the IoT security challenge, is driving new legislation, regulations and baseline security recommendations from authorities worldwide. Interventions from regulators tend to focus on recommendations across several key areas:

Secure storage of credentials

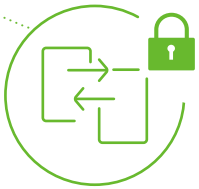
A central recommendation in much emerging legislation and policy is for trusted and secure storage of security-sensitive data, such as cryptographic keys, device identifiers and initialisation vectors.

Secure communication of credentials

Security-sensitive data should be encrypted in transit and mutually authenticated to ensure that device-to-device and device-to-cloud communications can be trusted.

Protection of personal data

Influenced by the EU's General Data Protection Regulation (GDPR), IoT codes of practice increasingly recommend as a minimum robust storage of personal data; full transparency about how data is processed; and that consumers are able to delete their data from a device as required.



Ensuring software/ firmware integrity

It is imperative that the authenticity and integrity of the software / firmware within a device is not compromised by malicious actors.

Towards a secure, interoperable IoT ecosystem

A common global standard for IoT security has not yet been realised and there is still a long way to go, but strong progress is being made. Similar principles and best practices are being emphasized by regulatory and certification frameworks, which can only be delivered by hardware technology.

The remainder of this ebook will examine the unique security benefits that hardware technology, specifically Tamper Resistant Elements (TREs), can deliver to the IoT ecosystem.

[3]Notable examples include ETSI's IoT Security Standard and ENISA's Baseline Security Recommendations for IoT. For a comprehensive overview of IoT security recommendations and best-practices, Trusted Connectivity Alliance encourages readers to review the various resources published by the IoT Security Foundation.

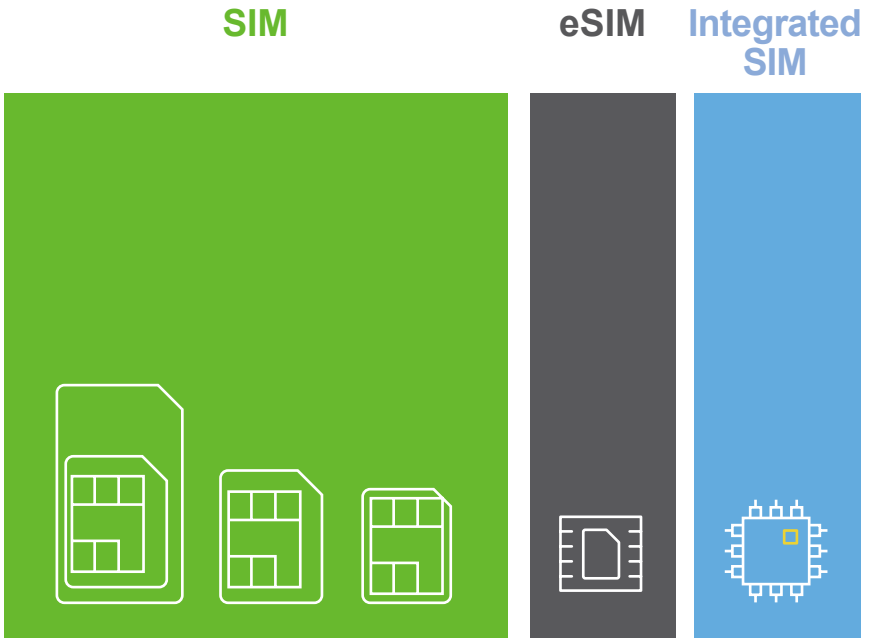
Tamper Resistant Elements:

Delivering advanced security to the IoT

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. TREs are available in removeable, embedded and more recently, integrated form factors (e.g. SIM, eSIM and integrated SIM).

These features give TREs a unique ability to offer the most stringent secure end-to-end connectivity solutions, in line with the recommendations and requirements of various regulatory initiatives and certification frameworks across multiple IoT and IIoT verticals.

And since all SIM form factors are built on TRE technology, there are numerous advantages to leveraging TRE-based SIM products to protect IoT devices.



An established (untapped) security platform already present in billions of devices

Tens of billions of devices which use cellular connectivity worldwide already contain TRE-based SIM products. The SIM application is required to authenticate a device's access to mobile networks and the SIM ecosystem is the most widely distributed, secure application delivery platform in the world. Yet it is often the case that the stringent security services and features offered by the TRE hosting the SIM application, are underestimated and therefore not fully utilised by device manufacturers.

Significant security efficiencies can be made by the makers of cellular devices, by leveraging the security capabilities of TREs already contained within their products. The TRE can be used to securely store and process critical device and application data, extending its value beyond trusted connectivity and removing a security pain point for device makers, leaving them free to focus on their core business.

TREs can also be easily leveraged to secure connectivity to a range of non-cellular networks, including LoRa. This means IoT devices which do not use cellular networks can also use TREs, benefiting from their immediate availability, established infrastructure which includes testing and certification processes, and unique ability to deliver stringent secure end-to-end connectivity.

[4] https://www.statista.com/statistics/245501/multiple-mobile-device-ownership-worldwide/

Form factor flexibility

SIM products are available in multiple form factors, which have emerged to support different applications and use cases. Form factor flexibility means that TRE-based SIMs are appropriate for all types of IoT devices and can provide a secure foundation for innovation across various IoT verticals, both now and in the future.

SIM
the hardware which enables connectivity to the cellular networks owned by mobile network operators (MNOs). The SIM applications contained within the hardware provides individual end users who subscribe to the mobile network (subscribers) with authenticated access and related value-added services.

eSIM
eSIM refers to a SIM which is capable of hosting multipleconnectivity profiles (as defined by GSMA). It supports secure remote SIM provisioning, as well as remote updates to the keys and applications post issuance. eSIMs can be either soldered to a device or removeable.

Integrated SIM
An Integrated SIM is a new form factor, where the silicon of the SIM is actually integrated as a secure enclave within a larger system-on-a-chip (SoC) alongside, for example, a modem and application processor.

Protecting data at rest and in transit

TRE-based SIM products support advanced functionality which enables the highest level of security when storing credentials and personal data. The security benefits of this go beyond a single device. Using the untapped potential of the SIM as a secure hardware Root of Trust (RoT) and the securely stored credentials, devices can securely connect or authenticate themselves to the cloud infrastructure and establish a secure communication channel for the transportation of data.

IoT SAFE, an industry partnership between GSMA and TCA, defines a standardised way to leverage the SIM and eSIM to securely perform mutual authentication between the IoT device applications and the cloud. The result is that IoT device manufacturers can easily execute security services and remotely manage credentials across billions of devices.

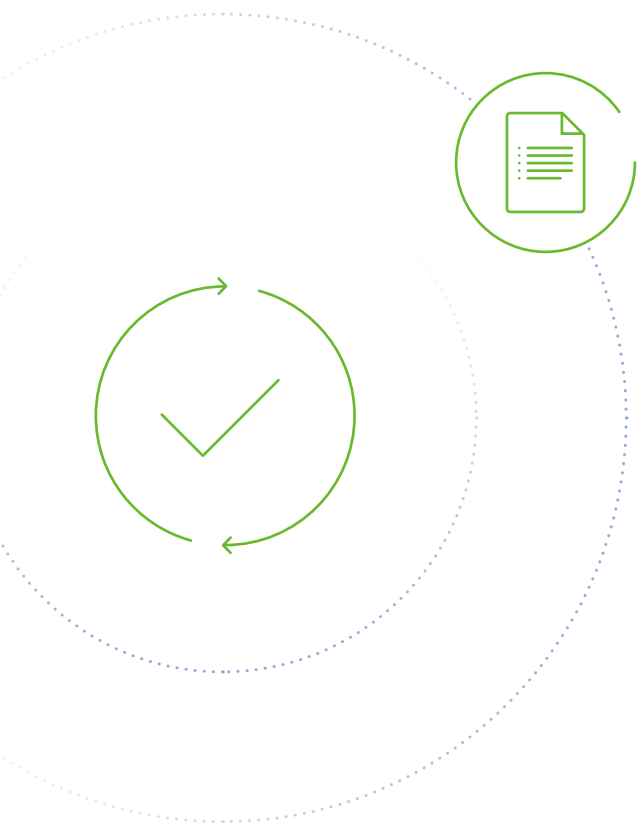
Future-proof security through remote management

SIM technology is supported by a long established, certified infrastructure which supports secure in-factory and in-field provisioning and personalisation, remote lifecycle management and security services. This allows security to be enhanced and updated throughout a device's lifetime.

For example, secure credentials can be provisioned remotely to a device on the factory production line to support a secure-by-design approach, without impacting manufacturing processes.

Since IoT security is not static and threats evolve over time, SIM technology enables credentials and security parameters to be updated, enhanced or revoked. Connected devices may have long lifespans and encounter new security threats and potentially multiple owners (e.g. cars). Remote management is therefore critical. SIM products can help strike a balance between robust security and simplicity of its deployment and future management.

Conclusions:



- As the IoT and IIoT expand and use-cases diversify, addressing the significant security and privacy vulnerabilities is an increasingly urgent priority.
- In recognition of this, governments, regulatory bodies, and industry groups are starting to move towards mandating considerably more stringent standards and baseline security requirements for IoT security, many of which require the robust protections only hardware technology can provide.
- TREs offer the most stringent secure end-to-end connectivity solutions for connected consumer and industrial devices, and have the potential to immediately address IoT security vulnerabilities.
- TRE form factors including the SIM, eSIM and, increasingly, Integrated SIM are already deployed across billions of devices and can deliver unsurpassed security features and services.
- Leveraging TRE-based SIM products reduces costs and shortens time to market, ultimately enabling players to focus on their own business with security taken care of.

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 CARD CENTRIC
东信和平 EASTCOMPEACE
kona i
Linxens crafting the future of connections
Qualcomm
Watchdata
WORKZ
TIANYU
COMPRION