IoT Everywhere
Succeed with IoT

Addressing IoT Cyber Security
through eSIM-based Scalable Trust

THALES

beecham research
Shaping the IoT future

Within the IoT market, huge numbers of devices collect, process and send data to the cloud, where a range of different IoT services are executed. To ensure security, the IoT cloud service must have absolute trust in the data that is received from connected devices. Equally, devices need to trust the cloud.

This is only possible if the device and server are mutually authenticated: the device knows it is sending its data to the right server and the server knows it is a genuine device that requests the data to be sent. However, IoT devices are not standardised, with a patchwork of different OS and chips being utilized. This prevents proprietary security solutions from being scaled or duplicated.

The ruggedized SIM, embedded SIM (eSIM), and more recently integrated SIM (iSIM) are increasingly used in IoT devices that are embracing cellular connectivity. These are standardized, regardless of their form factor. Associated with these SIM developments, a further GSMA initiative in addition to its work on SIM specifications is IoT SAFE (IoT SIM Applet for Secure End-to-End Communication). With this Applet, the SIM becomes a standardised hardware 'Root of Trust' that removes the fragmentation linked with proprietary solutions. The purpose of GSMA IoT SAFE is then to allow scalable end-to-end, chip-to-cloud security for IoT products and services. This security is also not OS dependant.

Thales has ongoing business relationships with 450 MNOs and over 100 OEMs and service providers across the M2M, IoT and consumer markets. The company is a world leader for Remote SIM Provisioning platforms employed in both consumer and IoT/M2M environments and lead the creation of new specifications, collaborating closely with the GSMA and other relevant industries.

The market view

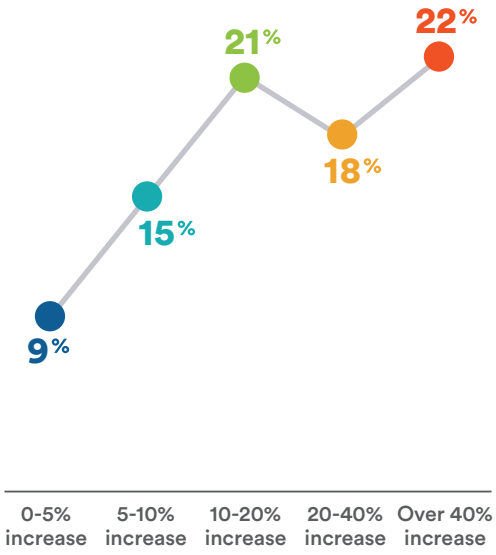
That the eSIM is seen in the IoT market as particularly well-suited for security of IoT data in addition to its established role of providing secure network access is confirmed in a recent survey by Beecham Research. This survey, drawn from 412 IoT users, confirmed that the IoT market is now moving quickly from the early adopter phase to early majority. **Figure 1** shows the findings from two questions. 33% of respondents already had over 5000 devices connected in their business. A massive 61% of respondents also expected growth of over 10% in the next 24 months, with 22% expecting over 40% growth. As this indicates, IoT growth is set to continue at a fast rate, with current deployments also increasing in size. This is a key consideration for management of IoT deployments – it is one thing to manage a deployment of 100 or so devices, quite another to manage one of 10,000 let alone 100,000 devices. IoT is now moving rapidly towards large deployments.

Figure 1: Use of IoT now and expected growth

How many IoT devices/terminals are connected in your business?

- 27% Less Than 100
- 13% 100 – 500
- 19% 500 – 5,000
- 7% 5,000 – 10,000
- 26% Over 10,000
- 8% Don't Know

How do you expect that to change in the next 24 months?



For those using cellular connectivity, eSIM was designed for IoT and, in the same Beecham survey, **Figure 2** illustrates how far this has now been accepted in the market. With 55% of respondents either already using or planning to implement eSIM and a further 37% researching its use, clear momentum is now taking place. More interestingly, the SIM itself was originally designed to provide security of access to cellular networks – not the security of the data. Nevertheless, in answer to the question: 'to what extent do you view the SIM as part of your IoT security?', Figure 2 also indicates that 64% see it as relevant for both a secure network connection and data security. It is evident from this that the SIM/eSIM is increasingly being seen in the market as a natural point for applying high levels of IoT solution security, covering both network access and the data itself.

Figure 2: Use of eSIM for IoT Security

Are you using eSIM in your IoT solution?

- **29%** Already using
- **26%** Planning to implement
- **37%** Researching
- **8%** Not relevant to requirements

To what extent is the SIM part of your IoT security?

- **9%** Not at all
- **27%** Only for secure network connection
- **64%** Secure network connection & data security

Use of SIM/eSIM for IoT

The traditional Subscriber Identity Module (SIM) card, used for cellular network authentication, was initially developed for consumer mobile phones. It has evolved over time, including with smaller form factors. Unlike mobile phones, most IoT solutions are installed on location. This creates significant logistical issues to ensure the right SIM card is matched with the right IoT device in the right place, particularly where international deployments are involved.

As noted earlier, the eSIM solution was developed in response to the limitations of traditional SIM cards for IoT. Initially deployed in the supply chain for connected cars, their use now extends to a majority of IoT applications. The eSIM solution specification enables remote over-the-air provisioning of network profiles and firmware updates, a great improvement for managing the connectivity of large IoT deployments. As part of the solution, the eSIM is typically soldered to a circuit board, is tamper-proof and better protected from extremes of vibration, temperature, dust, and other environmental challenges.

This creates the opportunity for a smaller form factor for the connected device, with no need for a SIM card slot or tray which then also reduces the unit cost. All of this means that a device with eSIM solution can be manufactured as a single stock keeping unit (SKU) for use in multiple geographies with the chosen network profile being downloaded at the point of use, once on the field. eSIM solutions are expected to represent over 70% of installed cellular IoT connections by 2025.

Establishing Trust

In addition to this, in order to ensure data security, the element of trust is paramount. Connected IoT devices are playing an increasingly significant role in every industry sector – from transport infrastructure and autonomous vehicles, through to greater automation in manufacturing operations, smart energy and faster diagnosis and treatment in healthcare. The core of all of these advances is the huge amounts of data they generate and, as greater reliance is put on that data for increasingly mission-critical activities, that data must be trusted. To be trusted, it must be recognised as coming from the right source, at the right time, in the right format and in no way corrupted.

Trust is essential to realise the full potential of the IoT. Digital security must be designed into IoT devices from the ground up and at all points in the solution to prevent vulnerabilities in one part from jeopardising the security of the whole. This is easy to say but IoT solutions can be complex and are becoming more so over time. Machines and objects in virtually any industry can be connected and configured to send data over cellular networks to cloud applications and backends. The digital security risk is present at every step along the IoT journey, and there are growing numbers of hackers at national and international levels that seek to take advantage of a system's vulnerability.

The first step for any IoT business is to undergo a thorough security risk assessment that examines vulnerabilities in devices and network systems and user and customer backend systems. Risk must be mitigated for the entire IoT lifecycle of the deployment, especially as it scales and expands geographically.

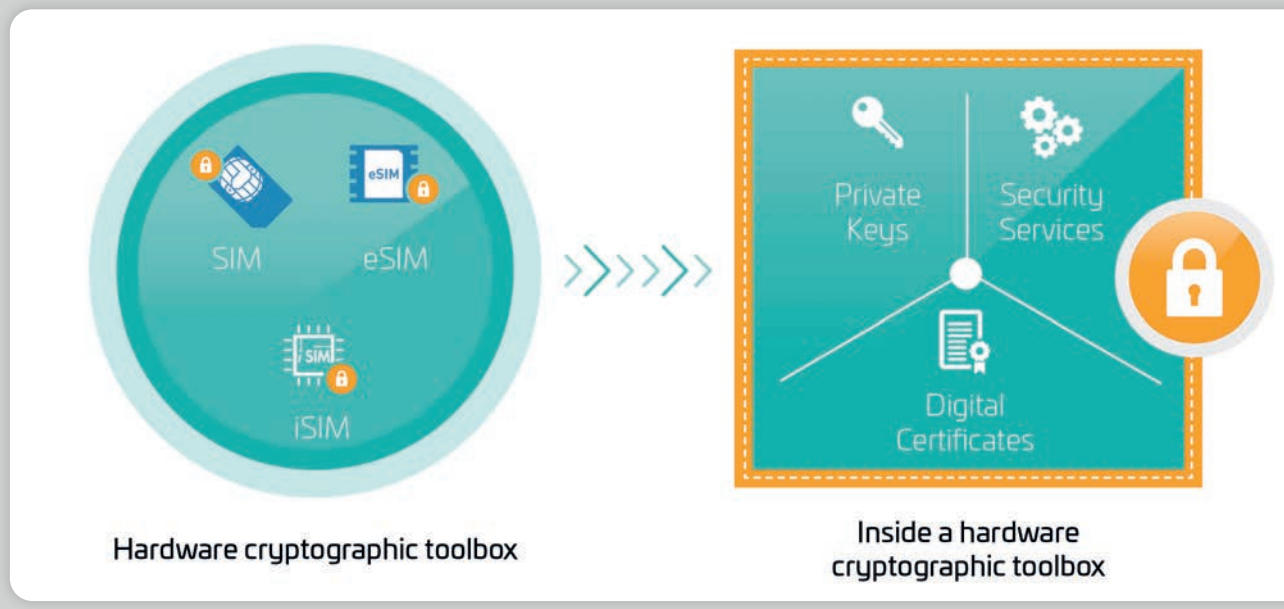
That requirement is provided by the Root of Trust (RoT), which is a set of implicitly trusted functions that the rest of the system or devices can use to ensure security. In IoT the RoT consists of identity and cryptographic keys built into the hardware of a device. It establishes a unique, immutable and unclonable identity to authorize a device in the IoT network. Since the root key is generated internally and never stored, no sensitive data is visible anywhere in the supply chain. It is a source that can always be trusted within a cryptographic system. Because cryptographic security is dependent on keys to encrypt and decrypt data and perform functions such as generating digital signatures and verifying signatures, solutions will normally include a hardened hardware module – a Secure Element. A Secure Element is a microprocessor chip that safeguards and manages digital keys, performs encryption and decryption functions for digital signatures, strong authentication and other cryptographic functions.

GSMA IoT SAFE by Thales

The standardised eSIM specification was developed by the GSMA as a response to the problems of using the traditional plastic SIM cards in IoT devices. A further GSMA initiative is IoT SAFE (IoT SIM Applet for Secure End-to-End Communication). This recommends that the industry should use the SIM as a hardware Secure Element or 'Root of Trust' to achieve end-to-end, chip-to-cloud security for IoT products and services. It is widely accepted technically that the SIM is particularly well-suited for this purpose: it is one of the hardest of all identifiers to spoof, with advanced security and cryptographic features, is fully standardized, and has been deployed in huge numbers of devices for the past 30 years.

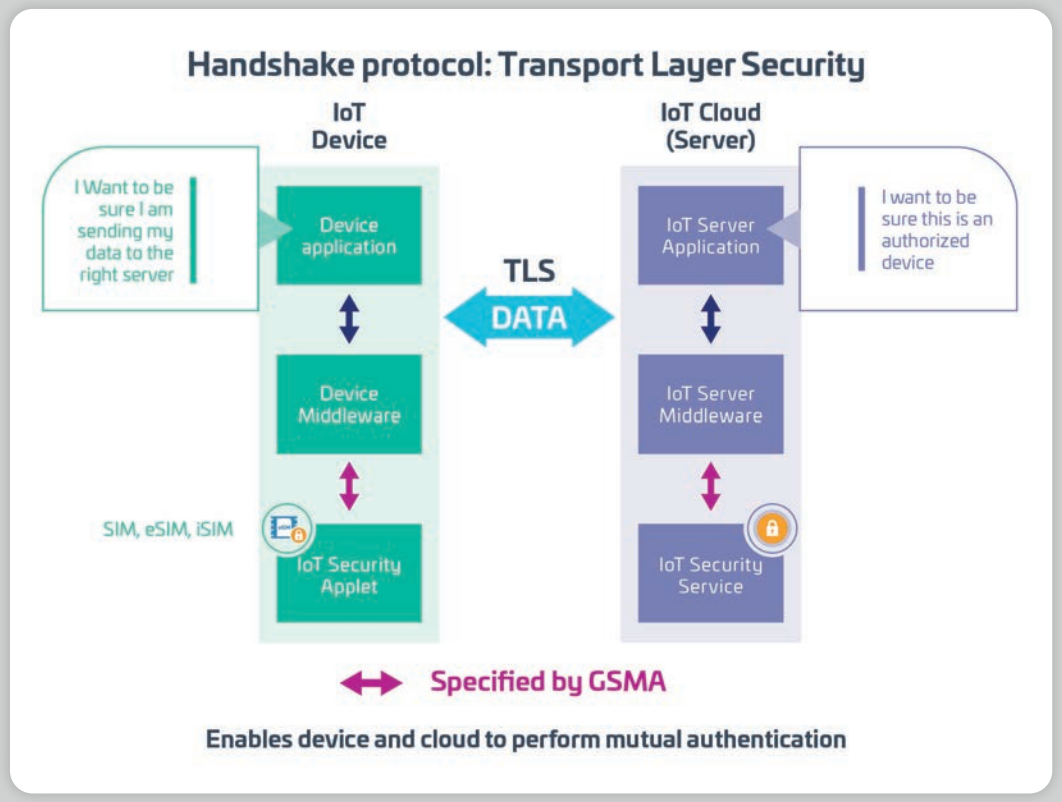
Key characteristics of IoT SAFE include:

- Use of the SIM/eSIM as a mini 'crypto-safe' inside the device to securely establish a TLS session with a corresponding application cloud/server
- Compatible with all SIM form factors such as eSIM and more recently iSIM
- Provides a common API for the highly secure SIM to be used as a hardware 'Root of Trust' by IoT devices
- Helps solve the challenge of provisioning millions of IoT devices



IoT SAFE

The IoT SAFE applet runs on Java OS, which in turn runs on the eSIM OS. In implementing this GSMA initiative, the Thales approach meets the scalability requirements of an IoT security framework by utilizing standardized and field proven SIM/eSIM/eSE technology, irrespective of form factor, and leveraging the billions of devices already deployed in the field. The company is actively and directly involved in the creation of new specifications, collaborating with the GSMA and other key stakeholders to establish an interoperable security framework. Indeed, Secure Elements are a standard technology that can integrate with the new GSMA specifications.



The benefits for stakeholders

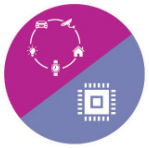
Secure Element-based security is field-proven, standardized, and enables the deployment of an IoTsecurity framework to be streamlined, within a fully interoperable environment. As a result, it delivers value for all the ecosystem's key stakeholders:

Mobile Network Operators (MNOs)

Alongside connectivity, MNOs can offer new secure IoT services, and utilize both their own and any other public cloud. They are ideally positioned to capitalize on their experience. MNOs already have billions of Secure Elements deployed in the field, remotely managed by OTA platforms. Moreover, they will deliver the next generation of 5G networks, enabling the extraordinary growth in connected objects.

Public Cloud Providers (such as Azure, AWS, Google)

In an interoperable framework, cloud providers can offer secure and seamless access, while minimizing the risk of attacks in their domain.



OEMs

OEMs and chipset makers can:

Protect the integrity of their devices against physical attacks, securing sensitive data leveraging hardware tamper resistant eSIM, iSIM or SIM

Deliver scalable security by design for the IoT, and avoid OS-dependent security implementations that, because of fragmentation, cannot be scaled up

Service Providers

Achieve seamless security with Thales touch-less provisioning concept: devices are automatically provisioned at first use with no impact on device design and production

THALES

Useful links

GSMA IoT SAFE | Thales Adaptive Connect | Thales Instant Connect

beecham research

Shaping the IoT future