Can GSMA's new framework secure cellular IoT?

beecham research

SPONSORED BY

THALES

Building a future we can all trust

The likelihood of an IoT security breach is increasing and so is the cost

This report, by Robin Duke-Woolley, the chief executive of Beecham Research, outlines the IoT security framework for cellular devices being established by GSMA, working with key industry stakeholders

As IoT solutions become increasingly important to business operations, the cybersecurity threat level is also increasing. Compared with a few years ago, IoT solutions are becoming:

- **Larger** Deployments of 10,000+ connected devices are becoming more common as IoT moves towards massive IoT
- **Critical** Immediate, low latency trustful data for automation and control is required
- **Extended** Coverage over large geographic distances, including worldwide is needed
- **Interoperable** The ability to work with a wide range of other systems has become essential
- **Complex** More is being done remotely, and all of this must be maintained – remotely

Each of these increases the impact of cybersecurity issues, and the threat level is therefore increasing over time. It is now a question of when there will be a security breach for an IoT business user, not if, and minimising the severity of that.

The cost of a security breach comes primarily in three parts – operational, reputational and repair. The operational cost is usually measured in terms of the cost of downtime, which for a factory or other automated plant could be substantial. The reputational cost is potentially much higher, particularly for a well-known brand. To these must be added the cost of repair – it may be necessary to replace everything that has been deployed because the breach cannot be repaired remotely. As a total cost of ownership, these could represent a huge cost when combined together. ▶

Robin Duke-Woolley
Beecham Research

With the increasing likelihood of a security breach in mind, and the potential cost of that, how can enterprises ensure the effectiveness of their IoT security solution remains at the highest level over time?

Related to this, IoT security is a complex topic. Suppliers may claim their IoT security solution is secure and meets all these threats now and in the future. But can they prove it?

Establishing the proof

Such proof can be provided by a certification process, where the process is operated by a recognised independent third party using a scheme endorsed by the industry at large. Recognised in this case must mean recognised by the industry as an expert in security, with no vested interest in supply. Such a scheme is measurable, repeatable and objective, and as a result creates trust.

What should be certified? The secure hardware and secure software components that form the basis of the security solution.

Is it necessary to have both secure hardware and secure software components? Yes. Secure software on its own can always be hacked. If that structure can be changed, it can be cloned, impersonated or interfered with in many different ways. Secure hardware, on the other hand, is much more difficult. This is because hardware security means burning secure identifiers/secure credentials into the hardware, which cannot then be physically tampered with nor extracted. That is how the highest level of security can be created. It is called a secure Root of Trust and considerably more secure than anything else.
It is then a question of the level of security needed. If a low level of security is acceptable – for example, perhaps for a headset – then a pure software solution may be sufficient. How important is it not to be exposed to attack, even remotely? If there is less security, the risks are higher, which means that a balance must be struck – with full knowledge of the risks.

Does that add unnecessary extra cost? It need not be expensive, but compared with the cost of a breach as outlined earlier it is likely to be tiny anyway.

A mobile framework

The mobile industry has a particular interest in ensuring the highest levels of security because so much of our world is going mobile. According to **GSMA**, there are around 5.5 billion mobile device users around the world, plus nearly three billion cellular IoT connections, and the way consumers use their devices is evolving. With consumers increasingly relying on digital services across all aspects of their lives, the telecoms industry is facing rising demand for applications running on mobile devices like payments, transport ticketing, identity management and secure IoT services:

As the Trusted Connectivity Alliance (TCA) makes clear "Given the sensitivity of these applications, their critical role and the data they contain and share, it is crucial that the mobile telecoms industry has the appropriate security mechanisms to protect users and enable the market to reach its full potential. In response, the industry is leveraging the advanced capabilities of proven technologies already available in mobile devices that enable trusted cellular connectivity – such as eSIM – to provide the requisite security for these applications. This approach reflects the growing momentum for eSIM technology." ▶

1. Payment

The COVID-19 pandemic has accelerated the adoption of digital payments, with mobile devices enabling touchless methods such as EMV® contactless and QR codes. These are set to be 4.4 billion mobile wallet users by 2024 and the global mobile payment market is predicted to grow annually by 23.7% between 2021-26. (Source Juniper Research) This will see the value of digital wallet transactions reach $12 trillion - up from £$7.5 trillion in 2022. (source: iMARC)

4. Transport Ticketing

The days of relying on paper tickets are over as many public transit authorities are now offering passengers increased convenience, flexibility and security through mobile ticketing, where travellers can order, buy and validate tickets with their smartphone or wearable device

3. Mobile Identity

As mobile devices become the primary point through which consumers interact with service providers, the ability to securely identify and authenticate end-users is increasingly critical. Consequently, enabling users to authenticate themselves through their device for a varity of use cases - including banking, payments, government services and healthcare - promises significant benefits. In addition, mobile devices are increasingly used in place of physical identity documents, such as e-passports and mobile licenses (mDLs).

4. Secure IoT Services

The increasing number of high-end connected consumer IoT devices is driving demand for various secure services that can protect IoT data communications from the IoT device to the cloud.

Figure 1: Secured applications offer great potential

Source: Trusted Connectivity Alliance Ltd (TCA) – Realising the Potential of Secured Applications for Mobile (SAM), February 2023

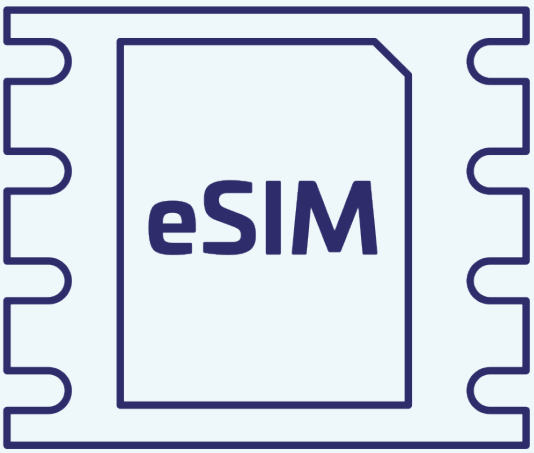
In response to these trends, it makes sense to have one overall framework to cater for all of these digital services – one that all suppliers in each of these areas can work with and inter-operate in. A standard approach for the whole mobile industry, which in turn reduces unit costs.

It is with this in mind that the GSMA together with mobile network operators (MNOs) and the supply industry including Thales has created a framework, comprising the following parts. Note that eSIM in this report means standalone or integrated eSIM (often referred to as iSIM):

1. eSIM architecture and technical specifications, including remote SIM provisioning (RSP)
2. An update on the RSP specification for provisioning constrained devices (low power, low data rate) to enable massive IoT – SGP .31/32
3. embedded universal integrated circuit card (eUICC) secure assurance (eSA) – the certification process for secure eSIM devices
4. IoT SIM Applet For Secure End-2-End Communication (IoT SAFE) – secure IoT services based on the eSIM
5. Secured applications for mobile (SAM) – extending the eSIM/iSIM to cover other digital services for mobiles where high-level security is essential

These all relate to the eSIM as a basis for IoT security for connected devices. In addition, but not directly part of the security solution for the devices, is the security accreditation scheme (SAS) for suppliers.

Thales occupies a unique position in the field of eSIM solutions. The company's solutions have been adopted by large numbers of original equipment manufacturers ▶



(OEMs), telecoms operators and key industry players worldwide. It has ongoing business relationships with 450 MNOs and over 100 OEMs in the IoT/M2M and consumer markets. Responsible for more than 360 projects, Thales is the world leader for RSP platforms, employed in both consumer and IoT/M2M environments.

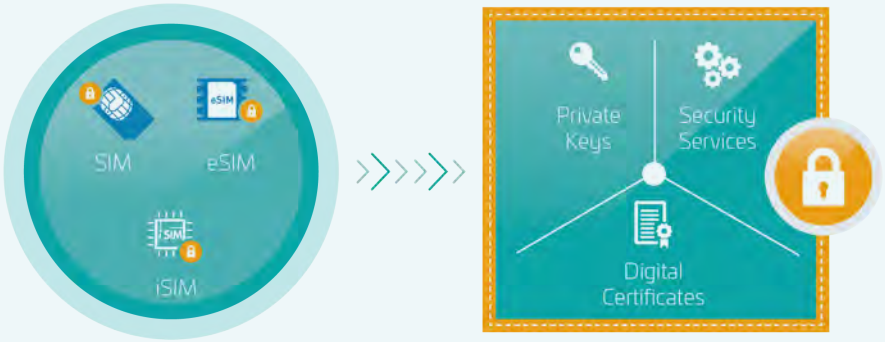
As part of that, Thales is actively and directly involved in the creation of these and new specifications, collaborating with the GSMA and other key stakeholders to establish an interoperable security framework.

Building the IoT Root of Trust

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.

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 exposed, 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 tamper resistant element (TRE). A TRE is a microprocessor chip that safeguards and manages digital keys, performs encryption and decryption functions for digital signatures, strong authentication and other cryptographic functions. Essentially, the security framework must fulfil three key requirements: ▶



Hardware cryptographic toolbox

Inside a hardware cryptographic toolbox

1. *Mutual trust between IoT device and cloud*
- Authentication - Device applications and IoT cloud applications need to exchange security-sensitive data. Trust must be established between the two applications before any such exchange takes place.

2. *Protection of security-sensitive data: at rest and in motion, in the device and in the cloud*
Two factors must be addressed here:
- Integrity - ensuring that the data has not been modified
- Confidentiality - ensuring that data is never disclosed to an unauthorised party

3. *Scalability*
With an exponential increase in the number of connected devices already underway, any security framework for the IoT must be scalable.

Why is the eSIM ideally suited to the demands of IoT security?

eSIMs can deliver scalable 'security by design' for IoT.

Thales' approach meets the scalability requirements of an IoT security framework by utilising standardised and field proven eSIM technology, irrespective of form factor, and building on experience from the billions of devices already deployed in the field. These tamper resistant elements are a standard technology that can integrate with the new GSMA specifications. Within this standardised framework, irrespective of their form factor, eSIM provides the same level of protection.

How does the eSIM-based approach work?

The foundation of any secure process is the handshake protocol between the IoT device and the cloud; mutual authentication must be enabled before any data exchange can occur. Specifically, this is achieved through hardware tamper resistant element-based security and cryptography, and GSMA specifications regarding:

- *The means by which the IoT device requests authentication from the cloud:*
device applications need to communicate in a language understood by the IoT security applications stored in eSIM to request authentication of the cloud. This language (which is the application programme interface (API) between the device middleware and the applet in the eSIM) is common to both device and hardware tamper resistant element, so therefore becomes scalable.

- *The means by which the cloud requests authentication from the IoT device:*
cloud applications need to communicate in a language understood by the IoT security applications (also in the cloud) to request authentication of the IoT device.

Once this handshake protocol is completed, the secure transport layer (TLS) is established, and can protect the data exchanged between the device and the cloud.

Within this framework, eSIMs are tamper resistant elements which can be regarded as cryptographic toolboxes serving two main purposes:

- Secure storage of security credentials
- Secure execution of security-sensitive services via IoT security applications

As a result, they address the three key IoT security requirements:

1. *Mutual trust between the IoT device and cloud*
- The device's private key, stored in the hardware tamper resistant element, is used to sign authentication data to the cloud
- The cloud digital certificate in the hardware tamper resistant element is used to authenticate the cloud
- This end-to-end mutual authentication enables a TLS connection

2. *Protection of data at rest and in motion*
- The device's key is stored safely in the hardware tamper resistant element ▶

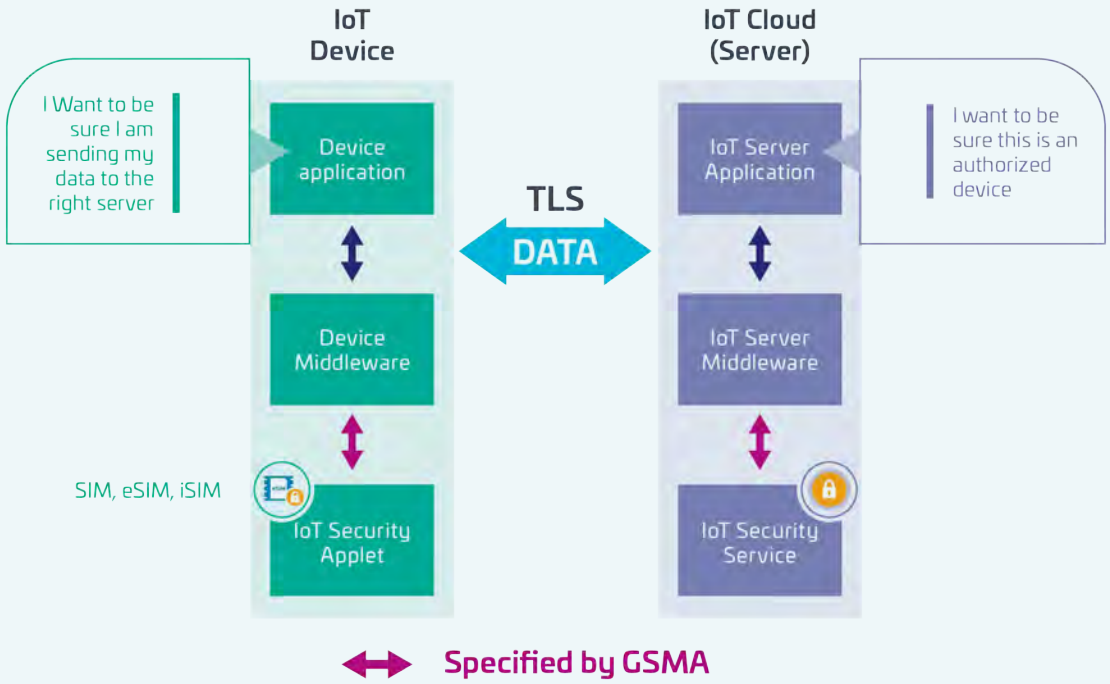


Figure 2: Handshake protocol: Transport Layer Security

- Onboard key generation capabilities
- Data is digitally signed by session keys calculated during the TLS handshake; the cloud can verify the integrity of the exchanged data
- The TLS ensures confidentiality between the device and the cloud

3. *Scalability*
- There are already billions of hardware tamper resistant elements in the field

Furthermore, all these security services pave the way for further services, including verification of IoT device firmware and remote lifecycle management of IoT security devices in the field, such as renewal and revocation of keys.

Keys are in the hardware tamper resistant element (device keys and cloud certificate) and the IoT Server Middleware (cloud keys and device certificate).
The IoT Security Server's role here is to provision the hardware tamper resistant element and the cloud and to manage the life cycle of the credentials.

eUICC Secure Assurance (eSA)

The purpose of GSMA eUICC Security Assurance (eSA) scheme is to provide a certification process for eUICC manufacturers of their secure hardware and software associated with eSIM/iSIM technology, for the purpose of demonstrating resilience against a range of high-level attack threats.

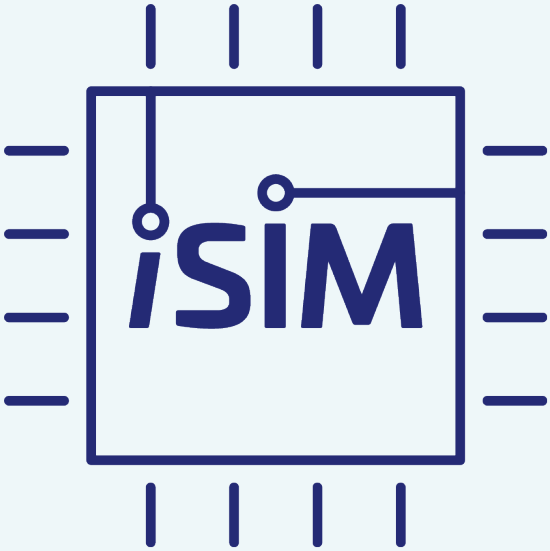
This certification is conducted by an independent third party, typically a laboratory recognised by the industry as an expert in cybersecurity and endorsed by the GSMA. It is not sufficient for a supplier to self-certify. With the best will in the world, that way leads to mistakes being made. There must be an external examiner for something so critical. Such a scheme is then measurable, repeatable and objective, and as a result can create trust. The methodology used is itself endorsed by industry, using criteria that are common not proprietary.

The scheme is designed to expedite the eUICC security certification process, overcome complexities, and reduce time to market for eSIM products. The scheme requires manufacturers to prove a benchmark level of security resilience across product processes. It does this by combining high-security quality with a pragmatic evaluation implementation approach adapted for the mobile market. The processes are in line with industry and ISO requirements and reflect the highest common criteria security standards recognised in Europe. While based on the common criteria approach to security assurance, it is more condensed, making the process fast and efficient. As a result, it represents a faster way to market than the alternative routes.

This demonstrates a very secure platform that can then be used to build secure services on top, such as IoT SAFE.

GSMA IoT SAFE

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. This recommends that the industry should use the SIM as a hardware TRE 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 standardised, 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. eSIM/iSIM are particularly suitable for IoT SAFE since they are certified as per eSA
- 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

The IoT SAFE applet runs on Java virtual machine, 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 utilising standardised and field proven eSIM/iSIM 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, tamper resistant elements are a standard technology that can integrate with the new GSMA specifications.

Thales has not only implemented the new GSMA IoT SAFE specifications. IoT SAFE is standard but there is additional value that can be provided to customers. The company works with providers of security stacks, TLS structures for example, to make sure the integration is easy. Touchless provisioning is also provided – a way to totally remove the cost impact of adding security into a device when the device is manufactured. When using Thales' IoT SAFE in the device, there is no change to the manufacturing process because the device credentials will be generated on board the device when it is deployed. There is no additional activity and no additional charge in the process because the touchless provisioning system works together with the security that Thales provides.

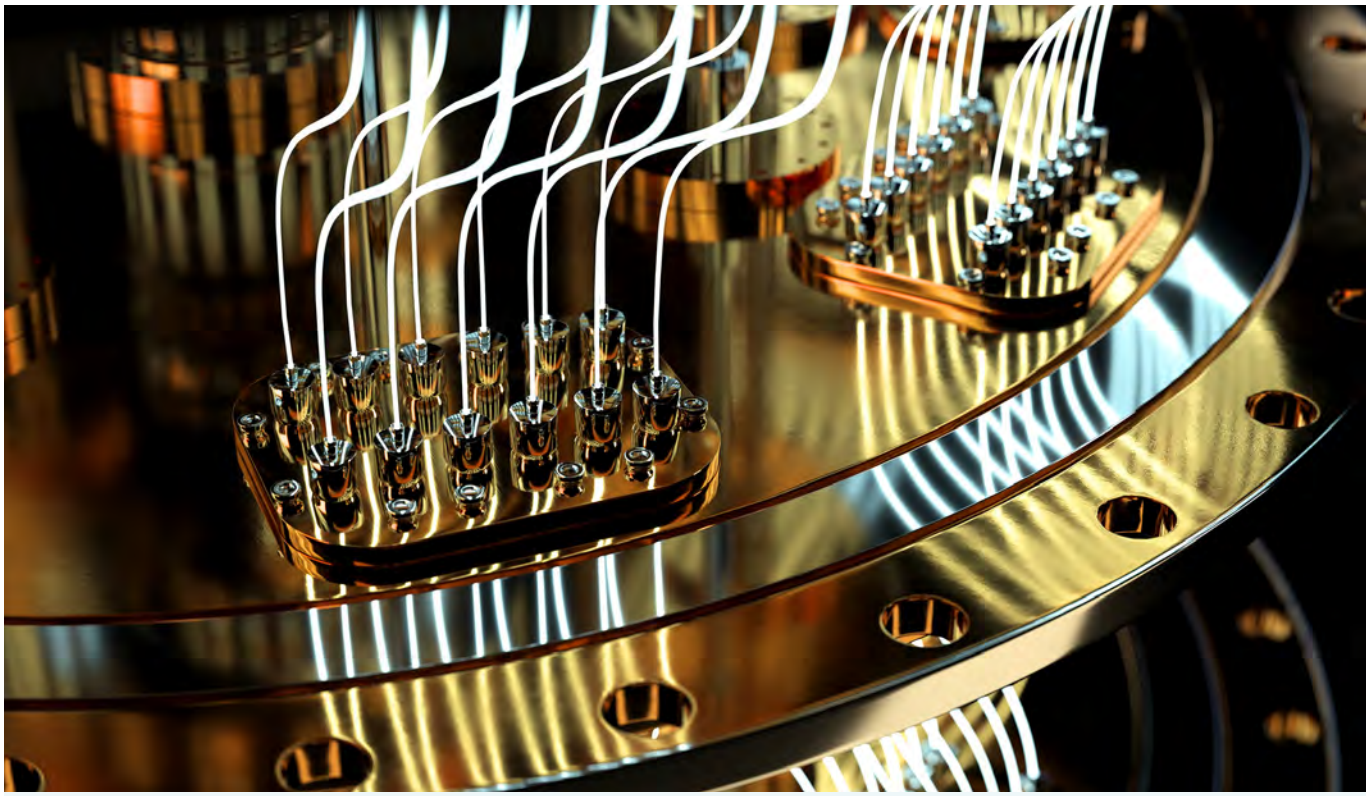
Secured applications for mobile (SAM)

As noted earlier in this paper, with consumers increasingly relying on digital services across all aspects of their lives, the telecoms industry is facing rising demand for applications running on devices like payments, transport ticketing, identity management and secure IoT services.

In response, the industry is leveraging the advanced capabilities of proven technologies already available in mobile devices that enable trusted cellular connectivity – such as eSIM – to provide the requisite security for these applications. This approach reflects the growing momentum for eSIM technology.

With these trends in mind, it makes sense to have one overall framework to cater for all of these digital services – one that all suppliers in each of these areas can work with and interoperate in. A standard approach for the whole mobile industry, which in turn reduces unit costs.

To support this trend for utilising the eSIM to host secure applets, GSMA published Secured Applications for Mobile – Requirements Version 1.0 [SAM.01] in June 2021. By providing a secure domain within the eSIM that enables access to applications regardless of the operator profile used, it is considered that this initiative presents significant opportunities to support new use-cases through proven, secure and reliable hardware technology. This goes beyond SIM functionality and provides a way to decouple the application layer security from the connection to the mobile network itself. Such functionality can then become 'transversal', where secure services like IoT SAFE can sit and be executed in a secure manner but independent from the connectivity providers. ▶



EU Cybersecurity Act

A further consideration is the EU Cybersecurity Act, which was passed in June 2019.

The EU Cybersecurity Act is a law that gives more authority and resources to the EU Agency for Cybersecurity, formerly known as ENISA. It also creates an EU-wide cybersecurity certification framework for ICT products, services, and processes. The framework will consist of common cybersecurity requirements and evaluation criteria across national markets and sectors. The certification will be recognised in all EU Member States and will be voluntary at first, but may become mandatory for critical products or activities. The EU Cybersecurity Act is part of the Digital Single Market initiative, which aims to increase data security and harmonize the rules for the digital economy in the EU. The EU Cybersecurity Act is still in the early stages of development and will affect the international standards community.

Security accreditation scheme (SAS)

Although beyond the scope of this paper to include in any depth, it is worth noting that the GSMA's security accreditation scheme (SAS) is a further part of the overall eSIM framework. This enables mobile operators, regardless of their resources or experience, to assess the security of their eSIM suppliers, and of their eSIM subscription management service providers.

Looking to the future

New cybersecurity threats are constantly emerging and new ways of dealing with them will be required. One such is post quantum cryptography (PQC), cryptographic algorithms that are thought to be secure against a cryptanalytic attack by a quantum computer. Thales is working on these new algorithms to combat such threats as they relate to SIM products. The company is investing heavily in security technologies – spending money researching new threats to make sure that future technologies are sufficiently secure for businesses to use effectively.

There is no doubt that IoT security is complex, and this will become more so over time. IoT users have a choice. They can have their own expert security team, maintain these skills, keep up to date with new threats arising and invest accordingly. Alternatively, they can work together with a security expert like Thales to assist in minimising both the cost and time to market. ■

About Thales

Thales (Euronext Paris: HO) is a global leader in advanced technologies within three domains: Defence & Security, Aeronautics & Space, and Digital Identity & Security. It develops products and solutions that help make the world safer, greener and more inclusive.

The Group invests close to €4 billion a year in Research & Development, particularly in key areas such as quantum technologies, Far Edge computing, 6G and cybersecurity.

Thales has 77,000 employees in 68 countries. In 2022, the Group generated sales of €17.6 billion.

THALES
Building a future we can all trust

Further reading:

GSMA IoT SAFE

Thales Adaptive Connect

Massive IoT: Tech overview, business opportunities and examples