TRUSTED
CONNECTIVITY
ALLIANCE

Integrated SIM Functionality: Drivers, Approaches to Standardisation and Use Cases

Version 1.0

May 2021

Table of Contents

1. Integration: Drivers of an evolution in SIM technology

SIM technology provides the foundation for the most widely distributed secure application delivery platform in the world. SIM / USIM applications enable access to mobile networks and have traditionally been incorporated within mobile devices via Tamper Resistant Element (TRE)[1] hardware, in standalone Secure Element (SE) form factors such as the removable or embedded SIM.

In recent years however, market forces have been driving demand for SIM functionality to be integrated within a secure enclave on a System on Chip (SoC)[2]. While expectations have changed regarding the performance and physical attributes of connected devices, the need to retain SIM security levels remains constant. The need for flexible, trusted connectivity has never been so great and the integration of SIM functionality on a SoC offers a unique approach which brings exclusive benefits to a host of use cases.

The forces driving the demand for integrated SIM functionality include:

- **Miniaturisation:**

To satisfy consumer demand for continual device enhancements, the quest of many manufacturers is to develop cellular devices that are increasingly smaller, thinner, more portable, aesthetically superior, perhaps even water resistant – all while delivering the same, if not more, features and functionality. 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 to 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, through removal or integration, manufacturers can also optimise their bill of materials and reduce their supply chain. These are significant drivers when time-to-market considerations and device cost can contribute to competitive advantage.

Following this trend towards miniaturisation, it is clear to see the benefits of a SIM form factor that evolves to work with smaller devices that contain fewer components and connectors. Integrated SIM functionality addresses demands from device manufacturers over recent years for SIMs to become smaller and require less device space.

- **Need to evolve SIM while retaining security levels:**

The revolutionary impact of digitalisation is not a new concept; aligned with it enabling an ever-increasing number of connected objects, it has driven a transformation of the SIM ecosystem in recent years. Embedded solutions have already resulted in the SIM become increasingly 'digitalised', in terms of how subscriber profiles and subscriptions are delivered and managed remotely. Yet as the quest for miniaturisation continues, and integrated SIM functionality drives further digitalisation of the SIM, there is a need to ensure that the security assurances provided by the SIM in its traditional hardware / software form factor are not compromised through software-only digital delivery. Integrating the SIM functionality within a secure enclave on a SoC addresses this concern.

[1] A Tamper Resistant Element (TRE) is a standalone secure element or a 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 removable, embedded and more recently, integrated form factors (e.g. SIM, eSIM and integrated SIM).

[2] 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. (Source: Wikipedia)

- **Device evolution in line with 5G launches:**

The expansion of 5G networks and the significant connectivity advances that 5G brings – including improved speed, latency, capacity and efficiency – are factors expected to act as a catalyst for further increases in connected device types and associated use cases. 5G launches are also likely to drive device renewal as well as advances in modem processors. Mobile SoC manufacturers will seek to incorporate new features and functionality that can maximise opportunities presented by new network technologies. This point of device renewal and enhancement is a natural juncture for new technologies such as the integrated SIM to be considered, due to the miniaturisation and performance benefits described above.

- **The preference for sustainable technology:**

Sustainable technologies – those which run on low power, use less resource and generate less waste than traditional solutions - are high on the global agenda. The integration of components within a device leads to reduced power consumption, and smaller physical footprints thanks to fewer connectors and interfaces. The annual efficiency gains brought about by integration could be significant considering the exponential growth in connected devices globally.

Beyond the physical attributes of connected devices themselves favouring integration in some cases to support their own sustainability, such devices are being harnessed to tackle wider societal sustainability challenges, such as reducing energy consumption and supporting resource optimisation as well as just-in-time production. Many sustainability use cases today, which have connected devices at their heart, rely on very small devices and extremely secure, reliable connectivity. Integrated SIM functionality is uniquely positioned to support these.

2. How has the industry responded?

In the face of these market trends driving smaller yet highly secure connected devices, there have been multiple industry initiatives in recent years to define and commercialise integrated SIM functionality for consumer and IoT devices.

Broadly, these initiatives can be classified according to the level of security assurance they provide and the corresponding complexity, flexibility and interoperability level of the resulting solution.

Below is a non-exhaustive overview of solutions that have been created. They vary in terms of their reach and relevance: some have been deployed on a regional basis for niche time-limited markets while others are global standardised solutions poised for imminent adoption:

- **Software-based SIM**

The proprietary software-based SIM is considered the least secure means of storing mobile network authentication credentials. There is no effective interoperability between software-based SIM solutions. It offers SIM functionality implemented in pure software (which may be reinforced by white-box, software-based cryptography techniques), running on a regular processor / microcontroller that does not offer dedicated hardware protection capability. Due to the lack of dedicated hardware mechanisms, software-based SIMs are not certifiable under major industry schemes like common criteria, used by industry bodies such as the GSMA. Credentials could potentially be retrieved from a software-based SIM through sophisticated attacks due to the lack of side-channel protection mechanisms.

Such solutions have been commercially deployed on a very limited basis and for niche time-limited use cases, like secondary SIMs for short term cellular-data roaming services, in certain regions of the world.

- **Trusted Execution Environment-based SIM**

In the case of Trusted Execution Environment (TEE)-based SIM solutions, the SIM functionality is implemented within an isolated execution environment on the device's main processor. The TEE employs a hybrid approach that utilises both hardware and software to provide increased security with minimal impact on flexibility, as it gives the trusted applications full access to the resources of the main processor. Certain operators have been commercially deploying TEE-based SIM solutions, mainly targeting the IoT market.

An overall architecture, including functional and security requirements together with evaluation mechanisms, has been developed by Chinese standards organisations. Yet it is important to note that these developments are strictly regional and lack global interoperability as well as security assurance levels that are required for most applications. Globally recognised standards development organisations (SDOs) and industry associations such as GSMA and ETSI have not defined technical specifications for TEE-based SIM.

- **Integrated SIM**

Integrated SIM solutions have been introduced to deliver the highest levels of security assurance. In these solutions, SIM functionality is implemented on a hardware TRE integrated within a host SoC.

An integrated TRE (iTRE) 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. This means that it does not rely on any protection mechanisms of the host SoC. It can be thought of as a miniaturised smart card integrated within the SoC, which becomes its operational environment.

Significant standardisation and specification development activity related to the integrated SIM is advancing within widely recognised international SDOs and industry associations to promote global interoperability and consistency. Of particular note is the publication of the GSMA's Integrated eUICC standard for M2M and the advanced status of its consumer standardisation efforts. More information follows in Section 5.

***

Given the high-security and potential for global interoperability through industry-wide standardisation initiatives, the focus of the remainder of this paper is on integrated SIM solutions.

3. Understanding hardware SIM form factors

The concept of an integrated SIM is easier to understand with some background knowledge of how hardware SIM form factors have evolved. Driven by market trends, SIM form factors have become progressively smaller over time.

Today, there are three main hardware solutions which provide the basis for the different form factors:

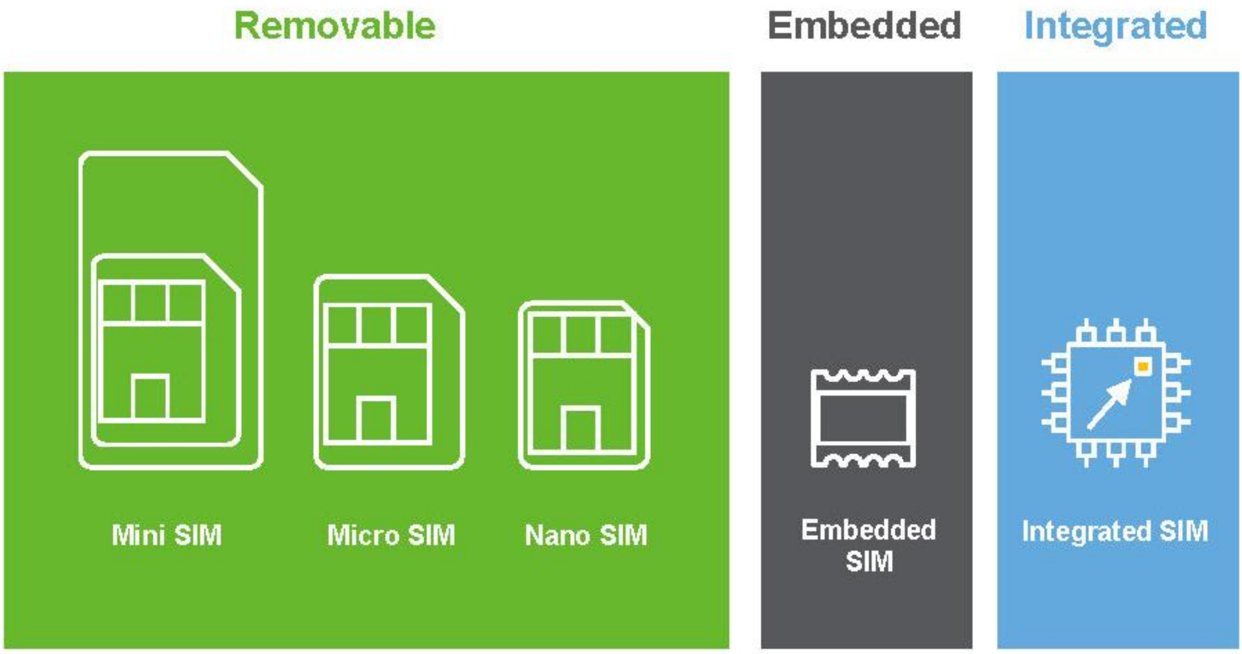

Figure 1: Form factor evolution

- **Removable –** *where the TRE is a standalone Secure Element (SE) which can be physically removed from the device by the user.* SIM form factors related to the removable TRE architecture have been used since the mid-1990s and are out of the scope of this document.

- **Embedded –** *where there is no requirement for the TRE, which is a standalone SE, to be physically removed and it is typically soldered*. Embedded or soldered SIM form factors are out of the scope of this document.

- **Integrated –** *where the TRE is a secure enclave that is integrated within a SoC.* The SoC comprises additional functionalities alongside the TRE, such as a modem and/or an application processor.

4. Integrated SIM: A definition

The term integrated SIM refers to an implementation in which the functionalities of a SIM or eSIM are realised on an iTRE, which provides physical isolation from all other silicon cores (such as a modem, application processor or any other functional block) within a purpose-built SoC.

While the architecture of the iTRE can vary, it commonly consists of its own central processing unit, random-access memory (RAM), one-time programmable memory, hardware cryptographic accelerator, true random-number generator and perturbation and environmental sensors.

Due to current technological limitations, non-volatile memory (NVM) - which is used for storage of data after power is removed - cannot be integrated with modern SoCs that utilise the most advanced technology nodes. Because of this, the iTRE has a different architectural approach to removable and embedded solutions, which contain their own NVM. Commonly, iTRE will utilise the external memory (e.g. flash and RAM), which is also shared by other SoC entities.

Since the external memory is outside of its physical boundary, the iTRE implements appropriate security measures and functionalities to protect its assets stored within this external resource. These measures and functionalities allow the iTRE to remain self-contained with respect to security and to provide security assurance levels at least equivalent to the removable and embedded solutions, while taking full advantage of other architectural benefits such as performance, capacity and increased flexibility.

5. Integrated SIM: Standardisation efforts

Industry standards offer significant benefits to technology ecosystems. They drive higher scrutiny, robustness and interoperability, encourage competition and reduce costs for both vendors and users. They also reduce the risk of premature product obsolescence and mitigate the risk of market fragmentation due to technological incompatibilities.

Internationally recognised industry associations and standard development organisations are already delivering specifications and definitions for iTREs enabling integrated SIM functionality. The most notable are GSMA's Integrated eUICC and ETSI's iSSP. In addition, Eurosmart is facilitating iTRE security certification efforts by developing a dedicated Protection Profile. These initiatives are explored below:

GSMA – Integrated eUICC

GSMA first launched its integrated SIM technology initiative in early 2015 to address emerging market expectations and demand for deeper integration of secure network access functionality. An initial Proof of Concept was demonstrated in 2017, promoting integration of UICC technology within SoCs.

The GSMA has finalised the standardisation of the Integrated eUICC, which is an eUICC implemented on a TRE that is integrated into a SoC, optionally making use of remote volatile / non-volatile memory. Security requirements to be fulfilled by an Integrated eUICC solution have been identified, agreed and added to both GSMA Remote SIM provisioning consumer and M2M specifications.

The Integrated eUICC security certification is defined by GSMA working groups. It covers evaluating and certifying the iTRE using the same methodology that is used for embedded and removable solutions, while extending it to cover all additional hardware security requirements related to integration into the SoC. This can be followed by a complete hardware and software integrated SIM (eUICC) certification.

Eurosmart

A dedicated Protection Profile covering security requirements for 'Secure Sub-Systems in SoCs' is being developed by Eurosmart with the aim of standardising and streamlining the security certification process for iTRE-based solutions such as Integrated eUICC.

ETSI – iSSP

In parallel to the standardisation work of GSMA, ETSI has specified the new Smart Secure Platform (SSP) which is one possible evolution of the UICC platform, with various physical interfaces and form factors, including an option for an integrated form factor called integrated SSP or iSSP.

SSP is a platform targeting applications from multiple market sectors. In addition to secure network access, the use cases for the SSP include banking and payments, ID management and transport. Sector independence and broader functionality of the SSP leads to increased complexity of the specification when compared to GSMA's Integrated eUICC.

While the commercial deployment of solutions adopting iSSP specifications are broadly expected to emerge after those based on the GSMA's Integrated eUICC, the timeframe for adoption is still unclear due to the broader functional scope of iSSP and the corresponding complexity. To date iSSP has not been considered within the certification frameworks and processes of the market sectors it can address.

Remote management approaches

Market regulation applicable to mobile phones typically demands that users are able to change their subscription / telecom operator during the lifetime of the device. The requirement for remote management capability, which also applies to the integrated SIM, has been addressed by GSMA.

In particular, the GSMA has specified Remote SIM Provisioning (RSP), or 'profile management', for the telecom market for both consumer and M2M segments. Both specifications were adapted to also cover RSP of the Integrated eUICC. A 'profile' is a set of personalisation data representing a mobile network operator's (MNO) subscription and is coded in an interoperable format.

For ETSI's iSSP, profile management is extended to 'bundle' management, where a high-level operating system is provisioned together with the profile.

Conformance and interoperability testing for integrated SIM

Conformance and interoperability testing are of critical importance for the success of new technologies such as the integrated SIM. For this reason, GSMA has introduced a dedicated Security Accreditation Scheme (SAS) process, which verifies the security of the integrated SIM production processes. Standardising MNO security needs and requirements will enhance their confidence in the handling of their data and result in increased adoption. This also improves flexibility to enable personalisation outside of a manufacturer's GSMA SAS-accredited secure facility.

For the Integrated eUICC, a test environment has been defined by GSMA. The infrastructure is already in place for platforms to be immediately tested, integrated and certified. Such an advanced testing and certification status ultimately supports and enables imminent deployment of Integrated eUICC solutions.

6. Integrated SIM: Use cases

Integration is an evolutionary step that enables significant improvements in SIM functionality, notably: the physical dimensions of the SIM form factor; energy consumption; amount of accessible memory; computing power; and performance. Additional benefits include simplified sourcing, integration and production. Cellular devices including smartphones which feature an integrated SIM can directly benefit from these improvements. Several themes which are emerging in the massive machine-type communications or cellular IoT space are explored below. Although all the use cases listed are already enabled by the embedded SIM, the integrated SIM can facilitate their adoption by being a catalyst for some new device categories.

- **Utilities:**

Connectivity for **smart meters**, especially for gas and water utilities that do not have access to any power grid, requires reliable, robust security as well as long battery life to support devices in the field for more than ten years. An integrated SIM offers significant power-saving benefits over its predecessors, allowing it to 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 misreport the amount of utility consumed; it offers improved robustness from its integrated design (removing soldered SIM complexity by leveraging a simpler chip design).

- **Logistics:**

Since the start of the COVID pandemic, there is an increasing requirement for real-time information related to **supply chain logistics** at all levels. Smart labels, which allow near real-time monitoring of supply chains, are one example of how connected devices that are enabled with integrated SIM functionality can be leveraged to meet that requirement, using Low Power Wide-Area Network (LPWAN) connectivity. 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 are becoming extremely important in the preliminary diagnosis of disease and to monitor lifestyle patterns of individuals. Battery life is a limitation of this type of feature-packed device; many modern devices need to be charged daily. Consumer brands promoting these devices recognise that there is significant value in maximising the power of the in-built battery with no compromise on features. Integrated SIM technology helps to optimise the device real estate and reduces the power budget significantly when compared to a discrete eUICC equivalent. Integrated SIM enables a new generation of personal health sensors.

Other fashion-oriented smart wearables are designed to serve trends, such as quantified self and augmented reality. **Smart watches**, which are increasingly becoming lifestyle devices, and **connected goggles with AR/VR applications**, which will see increased growth with 5G enablement, will both be among the first devices to benefit from the integrated SIM. Given the nature of these devices and their small size requirement and in-built battery, user comfort in their wearability relies on the power budget being maximised. An integrated SIM offers better prospects than an eUICC in meeting these goals. As detailed in section 7, the integrated SIM will also fuel new device features, bringing to life new use cases that will drive the next generation of those segments.

7. Leveraging the benefits of integration for device security features

Integration of both SIM functionality and the TRE hardware can result in streamlined internal device designs while providing an opportunity for new device features that are capable of securely supporting existing and emerging security-sensitive use cases. Deep integration into the device, together with its enhanced processing power and flexible memory configuration, allows the integrated TRE / integrated SIM to be leveraged for a variety of different security applications that could not be addressed with TRE technology until now. The integrated TRE can act as a secure processor for applications and use cases that previously had to be served by insecure technologies, due to limitations related to processing power, memory capacity or accessibility by device applications.

Below are some examples of security use cases that could be supported by the features of an integrated SIM or integrated TRE:

- **Protection of 5G subscriber privacy by leveraging deep device integration:**

The 5G standards developed by 3GPP introduced a mechanism to protect the privacy of subscribers to the mobile network. In 2G, 3G and 4G network technologies, as defined in 3GPP standards, the subscriber identity (also known as the IMSI) is sent in clear-over-the-air (OTA) without being encrypted. The latest 5G standards however introduce the possibility for MNOs to encrypt the IMSI before it is sent OTA. This can happen either on the device or within a Trusted Connectivity Alliance Recommended 5G SIM, embedded SIM or integrated SIM. If a SIM is integrated, within the modem for example, it provides additional motivation for device manufacturers to realise IMSI encryption within the integrated SIM, which is a security certified platform, rather than within the device.

- **Protection for device and other digital identities by leveraging flexible memory dimensions:**

In the same way that it can protect subscriber privacy (outlined above), the integrated TRE can offer secure storage capabilities for many types of security sensitive digital identities. Its deep integration into the device together with its flexible memory dimensions allow the storage of several identities for different types of use cases. If implemented within a modem processor it could also 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[3]. The reliability of such counterfeit detection schemes benefits from a deeper integration of the integrated SIM.

- **User friendly biometric authentication by leveraging increased processing power:**

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. 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.

8. Integrated SIM outlook: What’s next?

The advantages of integrating complex functionality into a single silicon substrate are numerous. Broadly speaking integration offers the potential for significant performance improvements and cost benefits within the semiconductor industry.

Trusted Connectivity Alliance (TCA) advocates that the trend towards integrated SIM functionality is supported by global, open standards which are developed by recognised industry organisations, for reasons explained earlier in this paper.

There is already strong market demand for integrated SIM solutions that provide secure network access capabilities for both IoT and consumer mobile products. As such, TCA welcomes the development of the Integrated eUICC by the GSMA as commercial deployments are expected soon, with the GSMA's standardisation work at an advanced stage. Adoption of the GSMA’s Integrated eUICC solution is anticipated to be within a short timeframe, thanks to its synergies and similarities with the embedded SIM solution (e.g. seamless compliance with the RSP mechanism). The result is that it could help to meet market demand relatively quickly.

ETSI's iSSP offers a potential integrated solution that extends beyond secure connectivity to bring benefits to other sectors including transport, payment and secure ID. Yet the broader application of ETSI's solution brings with it more complexity and currently, the timeframe for commercial iSSP deployments is not known.

[3] https://www.itu.int/rec/T-REC-Q.5052-202009-I/en

Security is a critical consideration if any ecosystem is to fully realise the performance and cost advantages of integration. Security levels must not be compromised.

It is TCA's position that integrated SIM technologies for secure connectivity and services can provide security levels that are at least equivalent to their embedded and removable SIM counterparts. TCA supports standardisation efforts and activities intended to reduce the overall time and cost of certification for integrated SIM solutions, without compromising quality. Standardisation bodies could drive further enhancements in the future. These could include: enabling the portability of evaluation evidence across multiple products hosting the same integrated solution; and facilitating and accelerating the certification of integrated solutions which utilise pre-evaluated hardware IP blocks.

9. 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 are: Card Centric, COMPRION, Eastcompeace, Giesecke+Devrient, IDEMIA, KONA I, Kigen, Linxens, NXP Semiconductors, Qualcomm, STMicroelectronics, Thales, Valid, Watchdata, Workz Group and Wuhan Tianyu.

www.trustedconnectivityalliance.org | News and Blog | Twitter | LinkedIn | YouTube

Intellectual Property Rights (IPR) Disclaimer

Attention is drawn to the possibility that some of the elements of any material available for download from the specification pages on Trusted Connectivity Alliance's website may be the subject of Intellectual Property Rights (IPR) of third parties, some, but not all, of which are identified below. Trusted Connectivity Alliance shall not be held responsible for identifying any or all such IPR, and has made no inquiry into the possible existence of any such IPR. TRUSTED CONNECTIVITY ALLIANCE SPECIFICATIONS ARE OFFERED WITHOUT ANY WARRANTY WHATSOEVER, AND IN PARTICULAR, ANY WARRANTY OF NON-INFRINGEMENT IS EXPRESSLY DISCLAIMED. ANY IMPLEMENTATION OF ANY TRUSTED CONNECTIVITY ALLIANCE SPECIFICATION SHALL BE MADE ENTIRELY AT THE IMPLEMENTER'S OWN RISK, AND NEITHER TRUSTED CONNECTIVITY ALLIANCE, NOR ANY OF ITS MEMBERS OR SUBMITTERS, SHALL HAVE ANY LIABILITY WHATSOEVER TO ANY IMPLEMENTER OR THIRD PARTY FOR ANY DAMAGES OF ANY NATURE WHATSOEVER DIRECTLY OR INDIRECTLY ARISING FROM THE IMPLEMENTATION OF ANY TRUSTED CONNECTIVITY ALLIANCE SPECIFICATION.