TRUSTED CONNECTIVITY ALLIANCE

Integrated SIM: A Practical Approach

April 2022

Intellectual Property Rights (IPR) Disclaimer

Contents

1. Glossary of Terms

Term	Definition
eSIM	eSIM is the generic term applied to devices and eUICCs that support Remote SIM Provisioning as defined by GSMA.
eUICC	A UICC which enables the remote and/or local management of profiles in a secure way that meet GSMA requirements for Remote SIM Provisioning and are certified in accordance with the GSMA compliance programme. The term originates from "embedded UICC".
Discrete eUICC	An eUICC implemented on separate standalone hardware, including its own dedicated volatile and non-volatile memory. A Discrete eUICC can be removable or non-removable.
Integrated SIM	Either an integrated eUICC or an integrated UICC.
Integrated TRE	A TRE integrated inside a System-on-Chip (SoC), optionally making use of remote volatile and/or non-volatile memory.
Integrated eUICC	An eUICC implemented on an integrated TRE.
Integrated UICC	A UICC that is implemented on an integrated TRE and that does not support Remote SIM Provisioning as defined by GSMA.
Operator	A mobile network operator or mobile virtual network operator; a company providing wireless cellular network services. An operator owns one or more international mobile subscriber identity (IMSI) ranges.
Profile	A combination of data and applications to be provisioned on a UICC or an eUICC for the purpose of providing connectivity to mobile networks.
SIM	A generic term for the application(s) residing on the UICC that identify a subscriber and allow them to securely access a mobile network (e.g. 4G or 5G). SIM is sometimes used interchangeably with the term UICC or SIM card.
SIM Card	A SIM that has one of the physical plug-in form factors as defined by ETSI (i.e. plug-in, micro-SIM, nano-SIM)
SoC (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.
TRE (Tamper Resistant Element)	A security module consisting of hardware and low-level software providing resistance against software and hardware attacks, capable of securely hosting operating systems together with applications and their confidential and cryptographic data.
UICC	The platform, specified by ETSI, which can be used to run multiple security applications. These applications include the SIM for 2G networks, USIM for 3G, 4G and 5G networks, CSIM for CDMA, and ISIM (not to be confused with integrated SIM) for IP multimedia services. UICC is neither an abbreviation nor an acronym.

2. Introduction

In 'Integrated SIM Functionality: Drivers, Approaches to Standardisation and Use Cases', Trusted Connectivity Alliance (TCA) defined an integrated SIM as a solution where SIM or eSIM functionality is implemented on a hardware Tamper Resistant Element (TRE) integrated within a host System-on-Chip (SoC). In addition to considering market forces driving the integration trend, the paper also detailed potential use cases and explored the benefits of integration for device security.

As an advocate of global, open standards developed by recognised industry organisations, TCA also provided a conceptual analysis of ongoing standardisation initiatives. Specifically, TCA noted that GSMA's integrated eUICC solution – which has now been finalised – offers the most potential to meet increasing market demand for integrated SIM deployments due to its synergies with existing infrastructure established for eSIM technology.

Thanks to the success of standardisation initiatives, TCA's analysis concluded that stakeholders could be confident that integrated SIM technologies provide interoperability and security levels that match embedded and removable SIM counterparts.

The standardised integrated eUICC is therefore now recognised by the TCA as an innovative, new form factor, which sits alongside the established eSIM. It can bring numerous benefits to a broad range of secure connectivity use cases which require small SIM dimensions, low energy consumption, or high levels of accessible memory and/or advanced computing power.

Building on this foundation, this technical paper provides SIM vendors, SoC makers, operators, device manufacturers, service providers and test tool developers with insight into the practical considerations associated with the deployment of integrated SIM solutions. This paper offers:

An overview of architectural considerations to ensure flexible design that supports the delivery of advanced performance, without compromising security;

A summary of the impact of the integrated SIM on the mobile ecosystem and associated value chains to illustrate the relationships between stakeholders;

A comprehensive analysis of the GSMA compliance process, and its importance in promoting the global interoperability and security of integrated eUICC solutions;

A description of conformance testing considerations.

As market momentum builds and integrated SIM technology increasingly shifts from concept to reality, this practical overview should instil further confidence across the mobile ecosystem.

NOTE TO THE READER

The term 'integrated SIM' can collectively refer to both integrated eUICC and integrated UICC as outlined in the Glossary of Terms. While integrated UICC complies with legacy SIM standards (i.e. GlobalPlatform, Java Card, ETSI, 3GPP) to support security and functionality, Remote SIM Provisioning and its associated security requirements as defined by GSMA are applicable to integrated eUICC only. Therefore, it should be noted that when detailing the interoperability and security of the 'integrated SIM' throughout this paper, this is specifically referring to the 'integrated eUICC' and not the 'integrated UICC'.

3. Architectural Considerations

Integrated SIM: Technical commonalities

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

An iTRE commonly consists of its own central processing unit, random-access memory (RAM), one-time programmable (OTP) memory, hardware cryptographic accelerator, true random-number generator, and perturbation and environmental sensors.

If the iTRE is on the same die as the SoC that it serves, physical interfaces like ISO, Serial Peripheral Interface (SPI) or Inter-Integrated Circuit (I2C) are no longer required. In such cases, the logical and applicative commands are conveyed to and from the iTRE via direct access to the system bus of the SoC.

Considerations: Navigating memory variances in technical architecture

While architectural approaches to integrated SIM design can vary, there are common elements related to memory that support advanced performance and security for integrated solutions. Consideration should be given to the following for full optimisation of these factors:

- **Utilisation of external memory**

To realise the greatest performance benefits, the latest generation of SoCs embed the most advanced technology nodes. Due to current technological limitations, non-volatile memory (NVM) types such as flash – which is used for the storage of data after a power down initialisation – cannot be manufactured and therefore cannot be integrated within modern SoCs according to these technology nodes. Other types of NVM such as OTP memory can be used to fulfil the process and rules of these technology nodes. Due to the high cost of the OTP memory, however, its size is drastically limited which subsequently impacts performance. It should be noted that for larger technology nodes, new NVM types such as magnetoresistive random-access memory (MRAM) could be integrated in the SoC.

Consequently, SoCs are commonly designed to use external flash memory. This architectural consideration when designing the integrated SIM overcomes the technological constraints imposed by flash NVM, and lets integrators utilise large available memory to enable flexibility in their design.

- **Secure utilisation of external memory**

The use of external memory presents new security considerations when compared with memory that is contained within the TRE. Certain security countermeasures can however ensure the content of the external memory is fully protected by the iTRE.

To protect NVM memory – which should be considered as remote memory from the integrated TRE point of view – the iTRE embeds a remote memory protection function (RMPF). The RMPF enforces the confidentiality, integrity and replay-protection of the information stored in the NVM. This prevents a wide range of possible attacks such as rollback of data stored in the remote memory, cloning content from another device, and the swapping or corruption of data.

Depending on the design, the external flash memory may be shared between different SoC components such as the Rich Execution Environment (REE) and Trusted Execution Environment (TEE). In these instances, an area of the memory is dedicated to the iTRE. Only the iTRE that owns the RMPF is able to access, execute and process data in the dedicated remote memory area. The SoC may also provide access mechanisms to the shared flash memory to protect the iTRE area and to manage concurrent accesses between different SoC subsystems.

The flexibility provided by the RMPF could also be extended to volatile memory. In addition, the iTRE can rely on a TRE internal volatile memory to provide a seamless and secure paged memory for the code and the data being processed. That possibility provides greater design flexibility. An alternative approach allows the RMPF design to enable Execution-In-Place (XIP) directly from remote memory, avoiding the step of copying the code into the internal RAM.

In summary, these measures and functionalities allow the iTRE to remain self-contained with respect to security and to provide security assurance levels equivalent to the removable and embedded solutions, while taking full advantage of other architectural benefits such as performance, capacity and increased flexibility.

Regardless of the specific architectural approach used, however, the integrated SIM relies on an iTRE in place of removable or embedded counterparts. The next sections of this paper explore the impact this integration has for different mobile ecosystem stakeholders and associated value chains.

4. Integrated SIM: Ecosystem Overview

The main impact of SIM integration on the ecosystem is that the traditional bilateral relationship between an operator and SIM manufacturer is replaced by multi-lateral exchanges between all integrated eUICC stakeholders. This creates new roles for SIM, SoC and device manufacturers, as well as service providers.

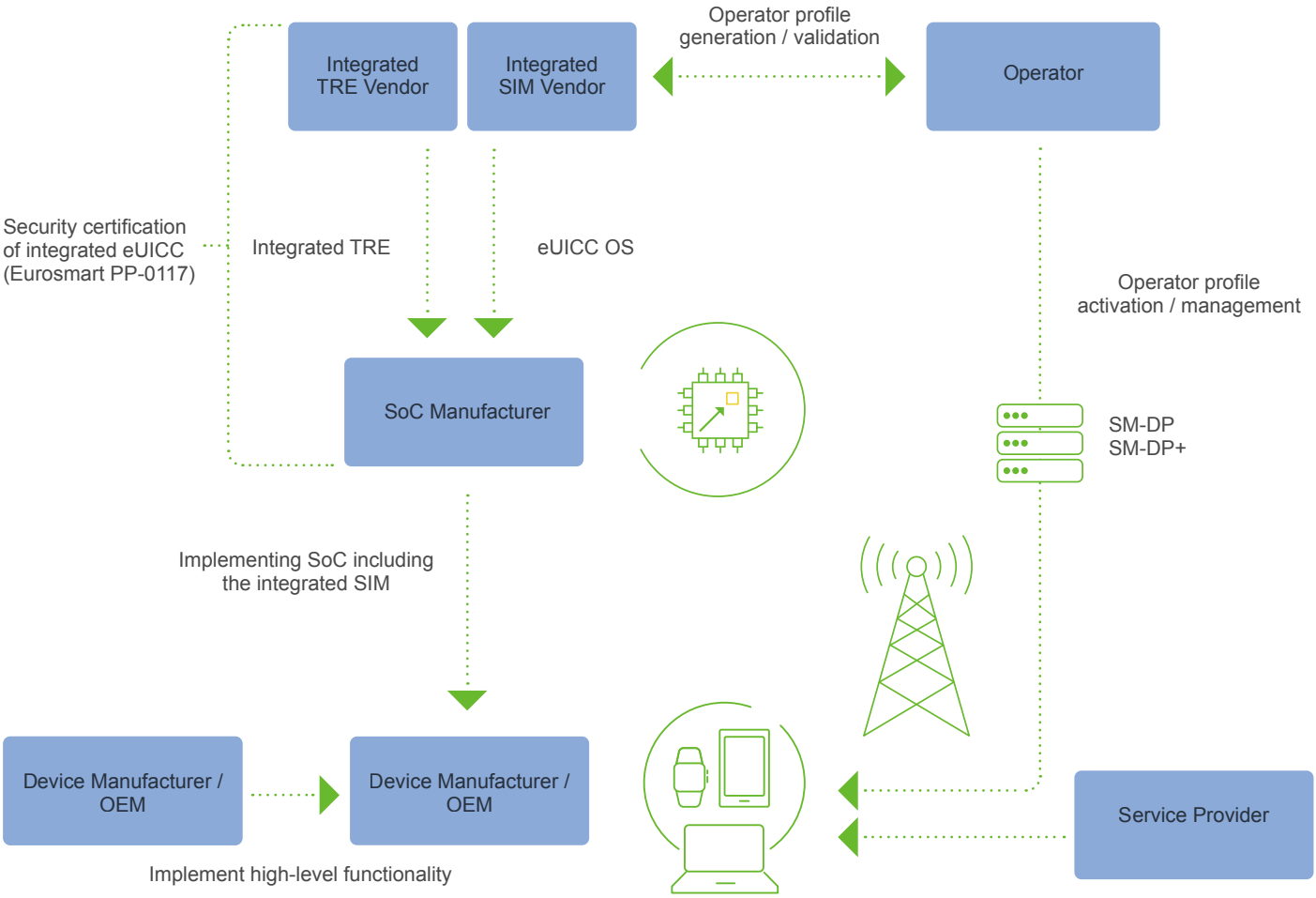

Figure 1: Integrated eUICC Ecosystem Overview

These changes are driven by the fact that the iTRE is directly implemented into the SoC. Consequently, a communication module within the device may be produced without any preinstalled connection to a mobile network. However, the integrated TRE has to be prepared to receive the operating system (OS), potentially together with one or several operator profiles. Once the device has been deployed in the field, Remote SIM Provisioning as defined by GSMA can then be used to download operator profiles.

While the role of traditional SIM manufacturers is to produce physical products, the role of issuing the **integrated SIM** follows a new process. The goal is, therefore, to develop a high-level OS (HLOS) that resides within the iTRE. The integrated SIM manufacturer may provide this HLOS to SoC manufacturers or OEMs that have already implemented the iTRE.

Both the integrated SIM manufacturer and SoC manufacturer are responsible for ensuring that the integrated eUICC addresses the requirements of the GSMA compliance process (see sections 6 and 7). This requires close collaboration, so a trusted relationship between these stakeholders is critical to achieving this goal.

As **device manufacturers** are responsible for incorporating the SoC as described above, SoC manufacturers are responsible for proper installation of the TRE low-level OS during the initial personalisation stage and for remote loading of subsequent updates. Device manufacturers are also responsible for the lifecycle management of the device.

The operator profile is installed either during the manufacturing stage or once a device is deployed in the field, and managed remotely by the end user or device fleet manager. This process uses the existing infrastructure established by operators to remotely provision and manage subscriptions to support the deployment of eSIM technology.

This proven, established remote SIM management infrastructure may enable **service providers** to deliver a range of value-added services over cellular networks. This allows them to benefit from the high levels of accessible memory available through the integrated SIM, while ensuring that sensitive data – especially when linked to the end user – is protected. Moreover, an integrated eUICC that is certified as per the GSMA specifications will ensure security, interoperability and scalability.

One example service offering, particularly for emerging IoT use-cases, is the IoT SAFE solution. This offers IoT service providers a common mechanism to use the integrated eUICC as a robust, scalable and standardised hardware root of trust to secure IoT data communications, rather than using proprietary and potentially less trusted hardware secure elements implemented elsewhere within the device.

The creation of multi-lateral exchanges across the ecosystem also impacts the associated value chains. The next section examines and highlights the implications of integration.

5. Integrated SIM: Impact on the Value Chain

This section compares the value chains for SIM, eSIM and integrated SIM, focusing predominantly on the changes introduced by integration. It should be noted that the examples provided offer an illustrative overview of respective value chains, but are not exhaustive and do not reflect the only approaches that could be implemented.

Value Chain Overview

The SIM value chain can be divided into the following three main sub-categories:

- **Hardware (HW)** – refers to all the process steps related to the production of the physical product, including fulfilment services and logistics flows. The physical product refers to hardware in its respective physical form factor containing SIM or eSIM functionality.
- **Software (SW)** – refers to the complete software stack of the SIM.
- **Data** – refers to the generation of data and profiles required to provision and individualise each SIM. It also covers personalisation services of data and profiles into the SIM or eSIM either during production in-factory or remotely in-field.

Figure 2: High level value chain

Hardware Value Chain

The hardware (HW) value chain can be further divided into several sub-components. Figure 3 shows the steps needed to produce the various removable SIM card form factors (FF) – 2FF (mini-SIM), 3FF (micro-SIM) and 4FF (nano-SIM) – and compares those steps with the production of both embedded and integrated SIM form factors:

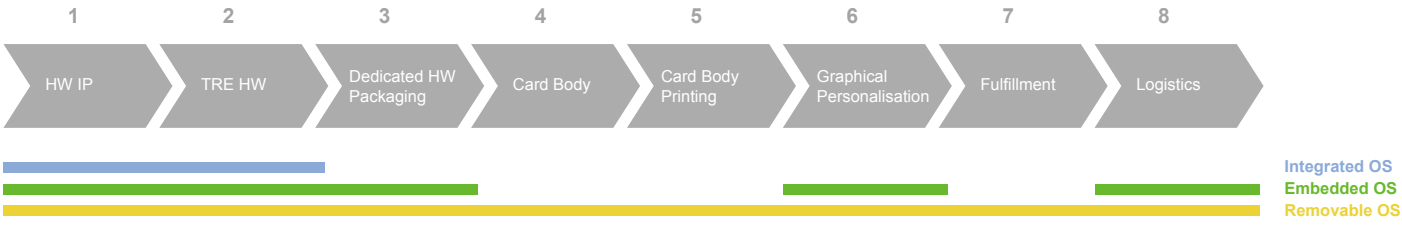

Figure 3: Hardware Value Chain

Explaining the HW Value Chain for Removable SIM

HW IP	This is provided by silicon IP providers and silicon / chip makers. A typical example of the HW IP is the processor core with its peripherals, which is then used as a basis for the development of a complete Secure Element (SE) chip.
TRE HW	Silicon makers enrich HW IP and develop a fully functional SE chip HW or SoC.
HW packaging	The final chip HW has to be packaged. Removable SIM cards are packaged in a SIM module which bonds the silicon to the contact plate on the card. eSIM modules are put into a package which is solderable onto a printed circuit board (PCB) (e.g. MFF2). This process is not applicable to the integrated SIM as it is covered by the packaging of the overall SoC.
Card body	This refers to the plastic card body of a removable SIM. A dedicated process step is required to produce the card body and embed the smart card module. This process is not applicable for eSIM and integrated SIM.
Card body printing	This involves the colour printing of logos and pictures onto the card body. This process is not applicable for eSIM and integrated SIM as these elements are typically delivered digitally to the end user.
Graphical personalisation	This enables removable SIM cards to carry individual data such as the SIM card's serial number (integrated circuit card identification number - ICCID) and initial personal identification number (PIN) / personal unblocking key (PUK) values. For eSIM, optical personalisation of the solderable package may be limited to the ICCID. For integrated SIM, this process is not applicable.
Fulfilment	In many cases the removable SIM card is attached to a paper carrier for shipment. The carrier contains additional information and may be enriched with marketing messages or other information for the end user. This process is not required for both eSIM and integrated SIM, where these elements are typically delivered digitally.
Logistics	This part of the supply chain covers the warehouse storage and shipping of the physical (discrete) products to the recipient. In the case of integrated SIM, no dedicated logistics flow exists for the physical SIM, as the TRE HW is integrated within a product with established logistic flows.

Summarising the Hardware Value Chain Impact

Changes are already evident when comparing production and hardware handling for removable SIM and eSIM. Integration further impacts the value chain, as the technological advancements in HW integration allow for the integrated SIM to be included as part of the SoC product. This leads to an overall reduction in the total number of components across the value chain.

For example, the packaging of the SIM module or the embedded chip is not relevant for the integrated SIM. Instead, the integrated SIM utilises the SoC package. Also, distribution of the integrated SIM is combined with the distribution of the SoC.

In addition, all value chain links related to optical appearance such as the card body, colour-printing or optical personalisation are no longer required. Other means to transport the operator brand may have to be introduced instead.

Software Value Chain

The software (SW) value chain can also be divided into several sub-components representing the overall software stack. Figure 4 shows the different SW components needed to build a SIM product, irrespective of its form factor. It also shows how the role of the SIM high-level OS (SIM HLOS) provider changes:

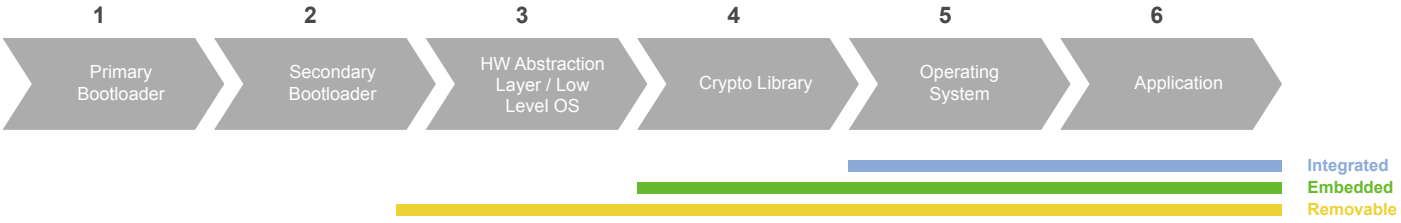

Figure 4: Role of SIM HLOS Provider for Respective Form Factors

Explaining the SW Value Chain:

Primary bootloader	This is the initial bootloader used to load firmware onto the chip. This may not be used for removable SIMs.
Secondary bootloader	This is the bootloader used to load the SIM HLOS.
HW abstraction layer / low level OS:	This provides access to the lower-level functionality of the chip.
Crypto library	A dedicated SW module utilising cryptographic accelerators of the HW and providing cryptographic functions and algorithms.
Operating system	This is a SIM HLOS providing the SIM or eSIM functionality.
Applications	These are use-case specific applications running on top of the SIM HLOS (e.g. JavaCard applets).

Summarising the Software Value Chain Impact

It should be noted that for removable or embedded SIMs, the SIM HLOS developer acts in a customer position towards the supplier of dedicated chips. In contrast, the relationship between the SoC manufacturer and the SIM HLOS developer can take on the form of a partnership for integrated SIM. It should also be noted that for integrated SIM, crypto algorithms may be provided by the HW provider rather than the SIM HLOS developer.

Data Handling Value Chain

With the introduction of remote SIM provisioning and the separation of logistics flows between HW and SW, data generation and provisioning have become integral parts of the value chain compared to traditional SIM. Figure 5 shows the four main areas related to data handling:

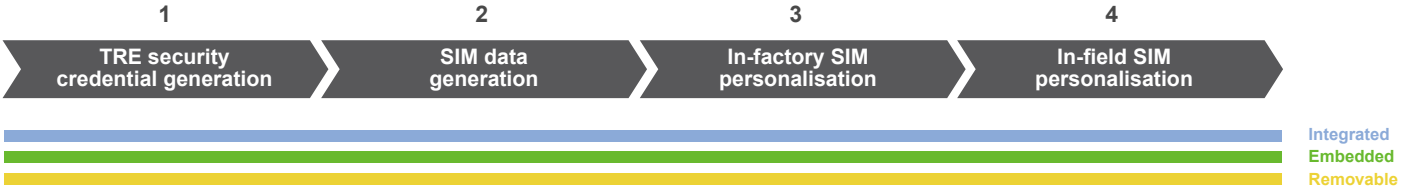

Figure 5: Data Handling Value Chain

Explaining the Data Handling Value Chain:

TRE security credential generation	This refers to the secure generation of TRE specific security credentials and their provisioning into the TRE. Those credentials are used to allow loading of a SIM HLOS to authenticated TREs only.
SIM data generation	This refers to the generation of SIM individual data / credentials and profiles.
In-factory SIM personalisation	This is the process of writing SIM individual data into the SIM HW platform within the production process of the chip / the device.
In-field SIM personalisation	This is the remote provisioning of profiles into eUICC products that are already deployed in the field using the GSMA standard for Remote SIM Provisioning. UICC products can only be provisioned with individual data using Remote File Management.

Summarising the Data Value Chain Impact

Whereas there are some changes to the value chain for hardware and software (see above sections), the data generation value chain remains relatively stable as the OS is also installed in-factory for embedded and integrated form factors. The main difference is that, with the advent of eSIM technology, in-field / remote SIM provisioning was enabled and has become increasingly important and widely adopted. This trend will be accelerated by the introduction of standardised integrated eUICCs. In addition, new solutions may be required to enable in-factory provisioning of profiles for integrated SIMs, which could be done by a different entity than the integrated SIM vendor (e.g. a device manufacturer). It should be noted, however, that the implementation of in-factory provisioning is specific to the device manufacturer.

This diversification of the mobile ecosystem and value chains reinforces the need for trusted relationships between different stakeholders. This trust is facilitated by global, open standards. The next sections of this paper provide a comprehensive analysis of the GSMA Compliance process, and its importance in promoting the global interoperability and security of integrated eUICC solutions. It also offers a description of conformance testing considerations.

6. Navigating GSMA Compliance for Integrated eUICC

GSMA first launched its integrated eUICC 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 now 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.

A key benefit of GSMA's integrated eUICC initiative is the synergies with the established infrastructure developed over recent years, including a comprehensive compliance process for eSIM-enabled devices, eUICCs and Subscription Management servers [SGP.24]. This compliance process covers security assurance by design, functionality and interoperability test cases, as well as a self-assessment notification process for product updates. This process fulfils ecosystem expectations to guarantee product compliance against technical specifications.

By leveraging this well-established eSIM infrastructure as a foundation, GSMA has now defined the whole compliance process related to integrated eUICC.

This covers two core aspects: production environment compliance and product compliance.

Figure 6: GSMA eUICC / Integrated eUICC Compliance Process (Source: GSMA)

- **Production environment compliance**

It is crucial to verify the security of the integrated eUICC production process. Ensuring production environment compliance is addressed by GSMA's established Security Accreditation Scheme (SAS), which defines the rules to be followed by any production environment with key roles in SIM creation and delivery processes. This scheme ensures that all sensitive assets – including those of the operator – are handled and inserted into the chip in a secure way, enhancing confidence and helping to increase adoption. The different security requirements are documented in Security Accreditation Scheme - Consolidated Security Requirements and Guidelines [FS.18].

- **Product compliance**

Product compliance comprises functional compliance and security certification (see section 7). GSMA has defined test specifications for functional compliance that applies to both eSIM and integrated eUICC. The test specifications are used by GlobalPlatform to define the functional compliance programme on behalf of the GSMA.

From a functional perspective, there is no difference between a discrete eUICC and an integrated eUICC and the same behaviour is expected. For this reason, the same GlobalPlatform functional certification process applies for both form factors.

7. Understanding Integrated eUICC Security Certification

The continuity and synergies with the established eSIM infrastructure offers significant benefits. However, integration does present new considerations and challenges to be addressed. Specifically, the main difference between eSIM and integrated eUICC compliance relates to the security certification process. This is mainly due to the use of external memory by the integrated SIM.

To reflect these requirements, a complete set of technical specifications that fully define the security evaluation methodology for the integrated eUICC have been finalised within GSMA and are now publicly available. When applying this methodology, vendors can demonstrate security assurance levels for integrated eUICC hardware platforms that are equivalent to embedded and removable solutions:

Common security compliance evaluation methodology

Over the years, GSMA has developed a comprehensive security compliance evaluation framework to demonstrate that the security of SIM solutions meet the highest industry expectations.

This proven framework now extends directly to integrated TRE hardware platforms. In particular, GSMA's Compliance Process Specification (since version 2.4 of [SGP.24] and version 1.3 of [SGP.16] for Consumer and M2M solutions respectively), introduces a new product type – the integrated eUICC – and refers to GSMA's newly developed specification describing its security evaluation [SGP.08]. The procedures described in [SGP.08] allow the expanded use of a well-established security assessment framework of GSMA across all SIM form factors.

Integrated eUICC security evaluation assurance level

[SGP.08] describes integrated eUICC hardware platform evaluation procedures. According to [SGP.08] the integrated TRE, which is a hardware sub-system (together with its low-level kernel) integrated within a SoC, needs to pass certification against the Security IC Protection Profile ([PP0084]), which is commonly used for the embedded and removable form factors.

Moreover, specifically for the integrated eUICC hardware platforms (i.e. the integrated TRE), GSMA has developed a set of additional obligatory security functional requirements. These requirements take into account the architectural novelties of the integrated solutions (see Section 3) and have been included in both consumer and M2M Architecture Specifications (Annex G of [SGP.01] and Annex J of [SGP.21] respectively). A vendor of an integrated TRE prepares a Security Target document in conformance to the Security IC Protection Profile and augments it with the requirements of the aforementioned Annexes. With that, the GSMA integrated eUICC hardware platforms demonstrate security assurance levels that are at least equivalent to its embedded and removable counterparts.

Streamlining the evaluation methodology for integrated TRE

In addition, further methodology streamlining efforts, specifically for integrated SIM, are currently ongoing.

To simplify the security evaluation of the integrated TRE, Eurosmart has developed a new Protection Profile for Secure Subsystem in SoC (3S in SoC PP [PP-0117]). This newly developed Protection Profile inherits the security functional requirements of the widely used Security IC Protection Profile, but also updates and augments them with considerations for integrated hardware platforms. These considerations include specifics related to SoC isolation, usage of external memories and product lifecycle.

As of early 2022, PP-0117 is under evaluation to be certified and added to the Common Criteria framework. Such evaluation process exposes the Protection Profile to the highest levels of scrutiny. With this in mind, GSMA lists the PP-0117 as candidate to become (upon its certification) a reference for a security evaluation methodology for integrated TRE hardware platform and to replace the [SGP.08] as well as the Annexes G/J. This means that in addition to the desirable level of scrutiny, the adoption of the PP-0117 by GSMA will reduce the effort on the vendor's side needed to prepare the Security Target document.

8. Conformance Testing for Integrated eUICC

Conformance testing is the process of ensuring whether an implementation meets the requirements of a technical specification or standard. Efficient conformance testing is crucial for promoting reliability, interoperability and competitiveness across product types.

It is distinctly important that the integrated eUICC largely utilises the existing and well-established testing infrastructure developed for eSIM conformance testing. However, it should be noted that the device conformance infrastructure for the integrated SIM may be slightly different from the infrastructure for devices with eSIMs.

Table 1 summarises how different test categories, relevant to both the integrated SIM and the host device, can make use of the existing test environments.

In particular, existing test environments which are applicable for eSIM – such as RSP testing [SGP.23] and other card conformance test systems [e.g. 3GPP 31.122; TCA eUICC Profile Package: Interoperable Format Test Specification] – can be used for the integrated eUICC.

Similarly, device conformance test environments for devices with eSIMs or integrated SIMs only (i.e. no removable SIM slots) can be the same for 5G/4G/3G protocol and performance tests. These environments can, however, slightly differ from the environments of devices with a removable SIM slot.

3GPP USIM and USIM application toolkit (USAT) test cases specified in UICC test specifications [3GPP 31.121, 3GPP 31.124] require explicit verification of communication and content of application data protocol units (APDUs) on the UICC-terminal interface. Test methods that exist today for these test cases require a physical UICC-terminal interface to be present and accessible. Consequently, new test methods must be adopted for executing 3GPP USIM and USAT conformance tests on devices with embedded or integrated SIM only (no removable SIM slot).

USIM test methods for devices, with integrated SIM only, may be different from test methods for devices with eSIM only. This is because, for the integrated SIM, the communication between the device and the SIM takes place over an internal SoC bus. The test method shall make sure APDUs sent over such a bus are not modified by present SW layers. For eSIM, on the other hand, a dedicated physical connection is available for such communication. This needs to be accounted for when standardising the test methodologies.

3GPP WG CT6 and ETSI SET groups are evaluating three test methods for verifying APDU communication and content in the UICC-Terminal interface that is a necessary requirement for USIM and USAT conformance tests for eSIM or integrated SIM:

- **Test toolkit events-based APDU verification**
- **Implicit APDU verification**
- **Baseband logging-based APDU verification.**

The goal is to identify and standardise reliable test methods that can verify all UICC conformance test requirements and are applicable to devices with any SIM type (eSIM or integrated SIM).

Test Category	Test Environment for Devices with Integrated eUICC
eUICC conformance tests • GSMA eUICC RSP • Other TCA and 3GPP card conformance	• Existing eUICC and card conformance test systems can be used. • Card Reader mode in the device shall be enabled. • In this mode, personal computer / smart card (PC/SC) or chip card interface device (CCID) protocol over USB can be used to communicate with test systems.
Device Local Profile Assistant (LPA) conformance tests • GSMA LPA RSP	• Existing device LPA conformance tests can be used. • No special settings are required in the device.
Device conformance tests • 3GPP USIM and USAT	• A recommended test profile (e.g. [GSMA TS.48]) shall be installed on the integrated SIM. • Elementary files shall be updated with test specific data defined under test case initial conditions. • A test applet shall be installed (e.g. for USAT testing). • Complete test environment is not yet defined. • Integrated SIM-specific requirements shall be considered when choosing a USIM test method and it may be different from the test method used for devices with eSIMs. • Currently under discussion in 3GPP CT6 and ETSI SET groups.
Device conformance tests • 3GPP 5G/4G/3G Protocol and Performance	• A recommended test profile (e.g. [GSMA TS.48]) shall be installed on the integrated SIM. • Elementary files shall be updated with test specific data defined under test case initial conditions. • The same test procedures and acceptance criteria as existing conformance tests can be used. • Test systems for devices with eSIMs are not yet available, but GSMA TS.48 guidelines are sufficient to develop test systems. • The test method applicable for devices with eSIMs can be used for devices with integrated eUICCs.

Table 1: Conformance testing for Integrated eUICC

9. Conclusion: Towards Secure, Interoperable Deployments

While architectural approaches to integrated SIM design can vary, there are common elements related to memory that support advanced performance and security for integrated solutions. Regardless of the specific architectural approach used, the implications of integration mean that the traditional bilateral relationship between operators and SIM manufacturers is replaced by multi-lateral exchanges between all integrated SIM stakeholders, and creates new roles for SIM manufacturers, SoC makers, device manufacturers and service providers. This subsequently impacts the associated hardware, software and data generation value chains.

This diversification of the mobile ecosystem and value chains reinforces the need for trusted relationships between different stakeholders. This trust is facilitated by global, open standards.

TCA has already confirmed its view that GSMA's Integrated eUICC solution – which has now been finalised – offers the most potential to meet increasing market demand for integrated SIM deployments and provides stakeholders with the reassurance that integrated SIM technologies provide security and interoperability levels that match embedded and removable SIM counterparts.

A key factor underpinning the success of incorporating the integrated form factor into GSMA's specifications is the almost direct applicability of the existing, proven infrastructure established for eSIM technology. This position is reiterated by a practical overview of the GSMA compliance process for integrated eUICC, which clearly demonstrates the extensive synergies. New architectural considerations introduced with the integrated form factor, such as the usage of external memories, have been taken into account and addressed within GSMA's security evaluation and certification methodologies. Moreover, further streamlining of these methodologies is envisioned.

In summary, these factors mean all mobile ecosystem stakeholders should have high levels of confidence in the security, interoperability and reliability of integrated SIM solutions. Looking ahead, TCA calls for the industry to continue to align existing and emerging infrastructures where possible.

There is also an opportunity for the benefits of the integrated SIM to be extended beyond pure telecom use-cases. In Integrated SIM Functionality: Drivers, Approaches to Standardisation and Use Cases, TCA has already noted the potential of ETSI's integrated Smart Secure Platform (iSSP) to offer 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. However, initiatives like GSMA's Secure Application for Mobile (SAM) have the potential to promote adoption of integrated SIM technology by allowing users to enable additional services.

As the market for integrated solutions develops, TCA will continue to work collaboratively across the ecosystem to enable trust in a connected future.

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

Annex A: Specifications Applicable to the Integrated eUICC

Specification	Impacted Section	First Version with Integrated eUICC
Consumer		
GSMA SGP.21	Requirements	v2.3
GSMA SGP.22	Eligibility Check	v2.3
GSMA SGP.23	Functional Testing	v1.10
GSMA SGP.08	Security Evaluation	v1.1
GSMA SGP.24	Compliance	v2.4
GSMA FS.04	SAS for UICC Production	v9.0
GSMA FS.17	Security Requirements	v3.0
GSMA FS.18	Security Guidelines	v3.0
M2M		
GSMA SGP.01	Requirements	v4.2
GSMA SGP.02	Eligibility Check	v4.2
GSMA SGP.11	Functional Testing	v4.2.1
GSMA SGP.08	Security Evaluation	v1.1
GSMA SGP.16	Compliance	v1.3
GSMA FS.04	SAS for UICC Production	v9.0
GSMA FS.17	Security Requirements	v3.0
GSMA FS.18	Security Guidelines	v3.0
Other Specifications Applicable to the Integrated eUICC		
GSMA SGP.05	eUICC M2M PP	
GSMA SGP.25	eUICC Consumer PP	
GSMA SGP.06	Security Assurance Principles	
GSMA SGP.07	Security Assurance Methodology	
TCA SAIP	Trusted Connectivity Alliance Profile Package Specification	