TRUSTED CONNECTIVITY ALLIANCE

Realising the Potential of Secured Applications for Mobile (SAM)

A TCA Position Paper

February 2023

Intellectual Property Rights (IPR) Disclaimer

Contents

1. Glossary of Terms

Term	Definition
Applet	Java Card-based technology that allows Java-based applications to be run securely on Secure Elements.
eSIM	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 to 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.
Hardware Security Module (HSM)	A physical computing device considered tamper-resistant that safeguards and manages digital keys (e.g. for strong authentication, encryption, and authorisation), and provides crypto-processing to external entities.
Integrated SIM	Either an integrated eUICC or an integrated UICC.
Integrated eUICC	An eUICC that is implemented on an integrated TRE.
IoT SAFE	Developed by the mobile industry, IoT SAFE (IoT SIM Applet For Secure End-2-End Communication) enables IoT device manufacturers and IoT service providers to leverage the SIM as a robust, scalable and standardised hardware Root of Trust to protect IoT data communications.
Multiple Logical Interface (MLI)	Mechanism defined by ETSI 102 221 that allows the multiplexing of several logical SE interfaces in a single physical ISO interface.
Near Field Communication (NFC)	Short-range high frequency wireless communication technology that enables the exchange of data between devices.
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.
Public Key Infrastructure (PKI)	Set of roles, policies, hardware, software and procedures required to create, manage, distribute, use, store and revoke digital certificates and manage public-key encryption.

1. Glossary of Terms

Term	Definition
Profile	A combination of data and applications provisioned on a UICC or an eUICC for the purpose of providing connectivity to mobile networks.
Remote Sim Provisioning (RSP)	Defined by GSMA and specifies two architectures: M2M and Consumer.
Secure Element (SE)	Tamper-resistant hardware platform, capable of storing sensitive, confidential and cryptographic data alongside executing certain applications in a secure manner
Secured Application for Mobile (SAM)	A specification that defines the capability for cellular connected devices to use a wide range of secure applets within an eUICC. Such applets can be managed by a service provider and may be paired with applications in the device itself
Security Domain (SD)	An on-card entity which provides support for the control, security, and communication requirements of an off-card entity such as the Card Issuer, an Application Provider, or a Controlling Authority.
Subscriber Identity Module (SIM)	A generic term for the application(s) residing on the UICC that identifies a subscriber and allows them to securely access a mobile network (e.g. 4G or 5G). SIM is sometimes used interchangeably with the term UICC or SIM card.
Smart Secure Platform (SSP)	A highly secure, scalable, thus cost-efficient solution optimised to fit many requirements, from IoT applications to complex solutions, hosting several applications such as banking and payment, ID management and access to mobile networks
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.
Trusted Execution Environment (TEE)	An execution environment that runs alongside but is isolated from a Rich Execution Environment (REE). A TEE has security capabilities and meets certain security-related requirements.
Trusted Service Manager (TSM)	As defined by GlobalPlatform Messaging Specification for Management of Mobile-NFC Services.
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.

1. Introduction

According to GSMA, there are around 5.5 billion mobile device users around the world. *(Source: GSMA)* **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:**

1 Payments

The COVID-19 pandemic has accelerated the adoption of digital payments, with mobile devices enabling touchless methods such as EMV® contactless and QR codes. There 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)*

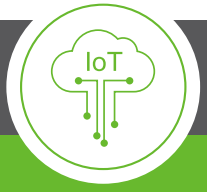
2 Transport Ticketing

The days of relying on paper tickets are over as many public transit authorities are now offering passengers increased convenience, lexibility 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 variety 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 driving 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.

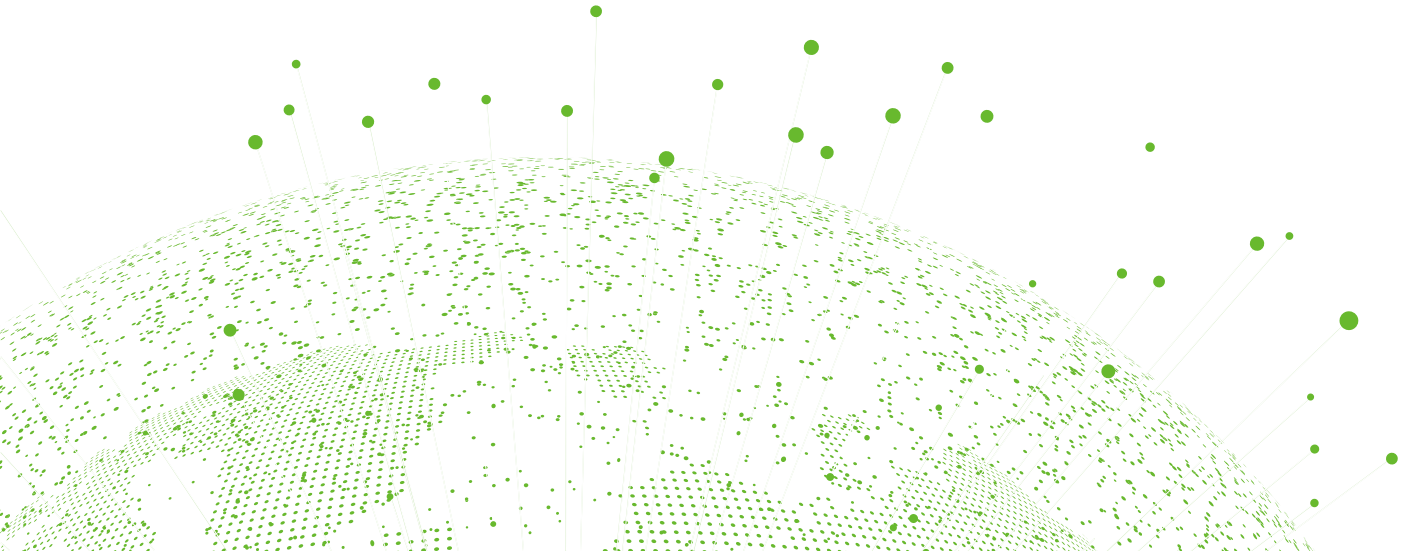
Given the sensitivity of these applications, their critical role and the data they contain and share, it is crucial that the mobile telecoms industry has the appropriate security mechanisms to protect users and enable the market to reach its full potential.

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.

To support the trend for leveraging 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 eUICC that enables access to applications regardless of the operator profile used, it is TCA's position that this initiative presents significant opportunities to support new use-cases through proven, secure and reliable hardware technology.

To support a broader industry understanding of SAM, this paper – which aims to address all industry participants with an interest in the use of eSIM (whatever the form factor) – will:

- **Analyse the market context surrounding the development of multi-application secure element (SE) technologies.**
- **Explore the GSMA SAM concept, architecture and ecosystem.**
- **Provide an overview of key SAM use-cases.**
- **Summarise potential deployment scenarios.**
- **Discuss potential challenges and limitations.**



2. Why SAM: Understanding the Market Context

The concept of hosting multiple applets in a SE is not new. Today, SEs are used to host various applets to support different mobile services that are deployed globally. This includes banking and payment applets (e.g. from American Express, Mastercard and Visa) to support contactless payments, transport applets (e.g. FeliCa) to support mobile ticketing, various e-government applets that support identity services such as electronic driving licenses, and dedicated security applets.

Industry Implementations

Several parallel initiatives have progressed across various industry forums that aim to standardise the approach to hosting applets in SEs. For example:

- GlobalPlatform has developed the generic SE specification for components, command sets, transaction sequences and interfaces that can serve various applications. Alongside the specification is a dedicated certification and training programme to establish common criteria for SE manufacturers using the GlobalPlatform specification to help meet the needs of digital service providers.
- ETSI has standardised its Smart Secure Platform (SSP) as a multi-application, multi-purpose SE. This offers an open platform for multiple applications and authentication methods with physical interfaces and form factors, helping address key connectivity market trends such as increasing IoT adoption and 5G infrastructure.
- GSMA established the IoT SAFE (IoT SIM Applet For Secure End-2-End Communication) initiative. This enables IoT device manufacturers and service providers to leverage the SIM /eSIM as a robust, scalable hardware Root of Trust (RoT) to secure connections.
- Google has created the Android Ready SE Forum to create the StrongBox feature. This supports tamper-resistant key storage for Android apps, supporting services like digital keys (for physical access control to cars, offices, and homes), mDLs, ePassports and digital wallets.

Proprietary Implementations

In parallel to these industry initiatives, proprietary implementations that support secure multi-application environments have emerged. Broadly, these implementations / configurations can be segmented into the following groups:

- Proprietary implementations of eSIM + eSE (known as ‘combo’ solutions) with or without NFC and with one or more physical interfaces.
- NFC SIM with supplementary security domains (SDs).
- Full Java Card operating system (OS) running secure applets.

Although all of these are secure implementations that leverage either SIM / eSIM or SE, the main drawback with proprietary implementations is the significant risk of market fragmentation due to different industries requesting solutions that are similar but usually not interoperable.

Towards a Standardised Solution

Considering the various stakeholders, industry initiatives and proprietary solutions, it is clear that there is an immediate market need for a secure, interoperable, scalable, standardised solution for a multi-application capable SE in a multi-application environment.

In addition, operators have flagged the opportunity to leverage the eSIM for use-cases beyond network access. TCA believes that leveraging eSIM provides the mobile industry with a solid, consistent and market-proven foundation for flexible, secure applet development, and helps establish eSIM’s role beyond telecoms into the wider IoT ecosystem.

For this reason, the industry has collaborated on the development of SAM technology. The next section of this paper explains the SAM concept, provides an overview of the architecture and ecosystem, and explores key use-cases.

3. What is SAM?

The overarching ambition of the SAM initiative is to leverage existing eSIM technology to host secure applets which previously would have been hosted on a separate SE. According to GSMA, the SAM Specification "defines a capability allowing cellular connected devices to use a wide range of secured applets within an eUICC." *(Source: GSMA)*

In short, SAM is proposing to translate some of the functional and security requirements from current SE standards onto the eUICC. This represents the convergence of two established and standardised technologies with separate ecosystems onto a single hardware platform: the eUICC (specified by GSMA) and the SE for secure applets (from the most diverse domains).

To support this aim, the GSMA SAM Specifications describe how SE applets can be managed in a standardised way (i.e. loaded, installed, updated, deleted) in the SAM area of the eSIM completely independently of the co-existing telecom area, with a clear and secure isolation. Any operations performed by the user or operator on profiles – such as switching – will not impact the applets in the SAM area. Likewise, any operation performed by the end-user or applet issuers in the SAM area will not impact the telecom area content.

Importantly, SAM is designed to be flexible. It is acknowledged that different issuers may have developed, and will continue to rely on, different public key infrastructure (PKI) architectures and RoT models to deploy and manage secure applets. The intention of SAM is not to change these existing ecosystems, but instead to offer the flexibility to reuse the existing infrastructures.

This approach promises significant benefits to stakeholders:

For device manufacturers,
the bill of materials (BOM) is reduced as the eSIM can be leveraged for additional use-cases, reducing the number of components (e.g. SEs).

For eUICC and eSE providers,
there is the opportunity to create innovative products that combine the respective benefits of each technology, reducing fragmentation.

For application providers,
the number of target devices for the different applications is increased significantly, addressing all the potential use-cases that SAM provides.

For operators and service providers,
there is an increased opportunity to leverage the eSIM for value-added services.

3.1. SAM Architecture Overview and Ecosystem Participants

SAM technology enables a logical area called the SAM Security Domain (SAM SD).
This is completely isolated from the operator profiles installed within the eUICC (as represented by Figure 1).

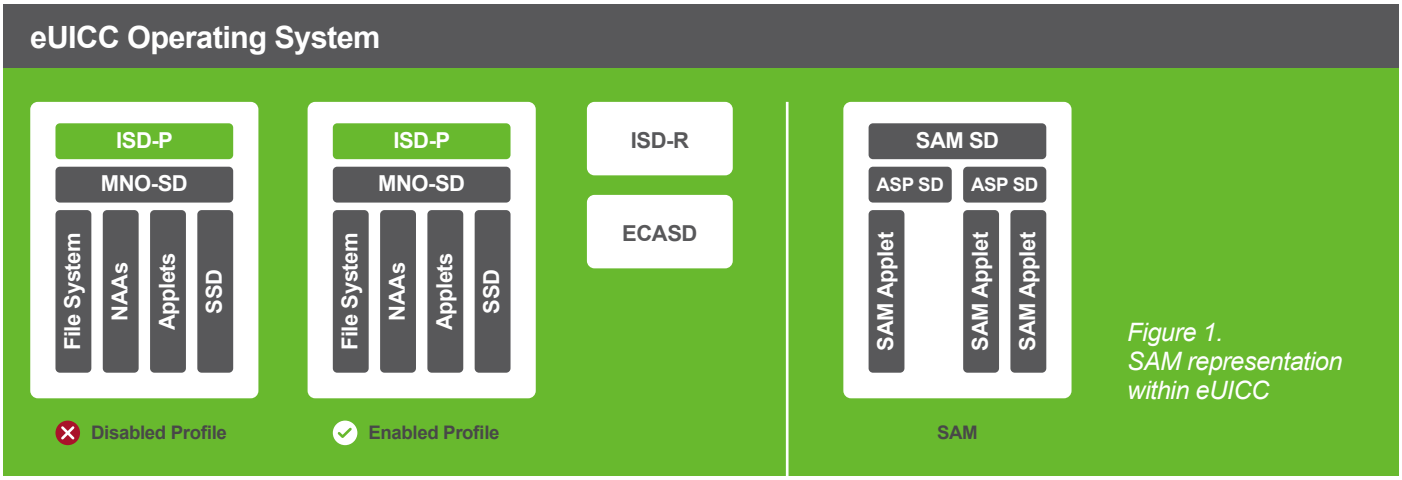


Figure 1.
SAM representation within eUICC

It is within this isolated area where end users can install their own applets and store the associated credentials. These remain untouched regardless of the operator subscriptions installed or enabled.

SAM architecture comprises the following entities *(see Figure 2):*

- **Service Provider (SP):** Responsible for providing a specific service through the SAM applets running on the eUICC SAM area. An example of a Service Provider could be a payment scheme.
- **Application Service Provider (ASP):** Responsible for the provisioning and maintenance of SAM applets and their associated credentials in the eUICC SAM area, with the objective of enabling a specific service for the end user.
- **SAM Service Manager (SAM SM):** Responsible for managing SAM applets within the eUICC SAM area on behalf of ASP.
- **SAM SD:** Security Domain in charge of managing SAM services, as well as supporting the deployment of ASP SDs and SAM applets.
- **Application Service Provider (ASP) SD:** Security Domain managed by the ASP which is used to host SAM applets for a dedicated service.
- **SAM Applet:** An applet installed in ASP SD in charge of running a certain secure service as per end user demand.
- **Device Application:** Third-party application installed in a device which provides functionality to the end user based on the services running on eUICC SAM area.
- **Local Applet Assistant (LAA):** Dedicated software element in the device that provides the capability to manage SAM services.

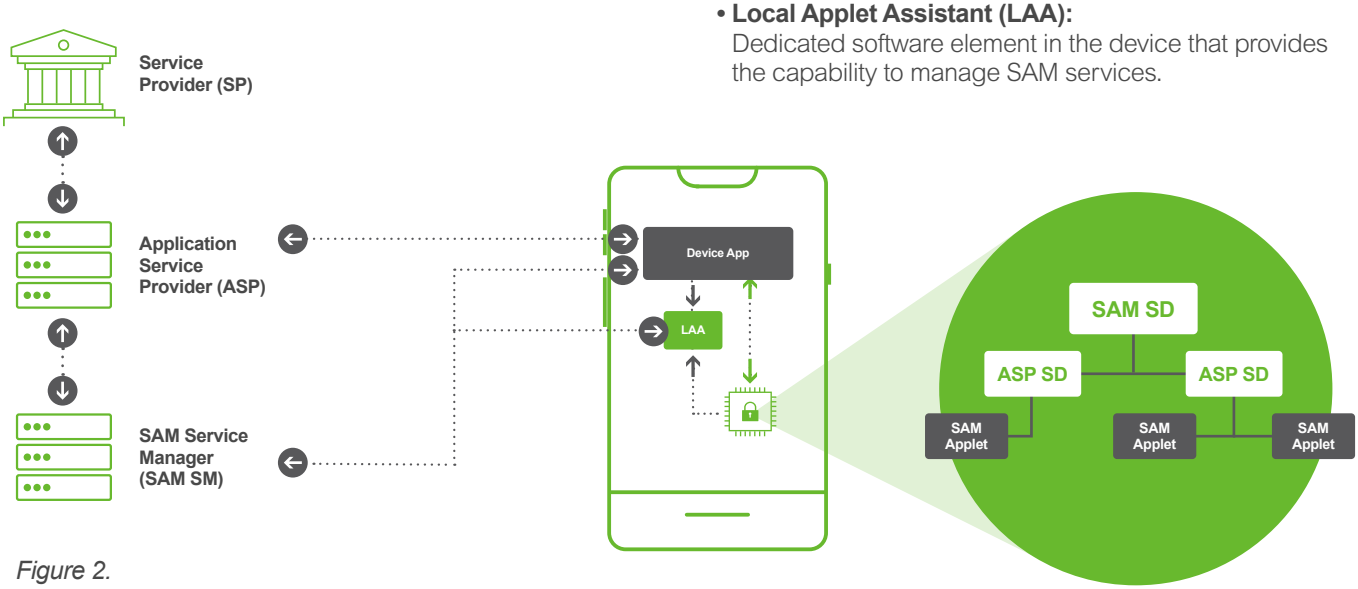


Figure 2.
SAM overall system architecture

3.2. Deploying New Services with SAM

Whenever a new service needs to be deployed within the eUICC SAM area, the following steps shall be performed:

- SAM SM shall create a new ASP SD under SAM SD for the new service by communicating with the eSIM through either the LAA or device application (depending on the use case).
- SAM SM shall establish a PKI-based secure channel (e.g., Secure Channel Protocol '11' [SCP11]) with the SAM SD and install a new ASP SD.
- The ASP SD shall then be confidentially personalised with new symmetric secure channel credentials through any of the existing confidential methods defined by GlobalPlatform based on Controlling Authority Security Domain (CASD).
- SAM applet download, installation and personalisation can be performed either by the ASP or delegated to the SAM SM depending on the use-case. In doing this, special attention is dedicated by the SAM Specification to solve the potential "application identifier (AID) conflict" issue (i.e., the possibility that the same AID is used on the same SE by different ASPs). The solutions currently being defined in such cases are described within the 'Deployment Options' section of this paper.

As previously noted, communication with the SAM SD shall occur within a PKI-based secure channel to ensure authenticity, integrity and confidentiality. A SAM Certificate Issuer (SAM CI) is responsible for issuing PKI certificates to SAM SMs and SAM SD issuers. Subsequently, SAM SD issuers will issue individual certificates to SAM SDs as required for each individual use case, as shown in Figure 3. Therefore, a SAM SD can verify the validity of the SAM SM certificate (i.e. not expired, valid signature and issuer is its SAM CI) while establishing the secure channel.
If the SAM SM certificate is not successfully validated, a secure channel will not be established and it would not be possible to perform any operation in the SAM SD. In addition, the SAM CI is able to revoke any certificate signed by itself whenever is required.

3.3. SAM Use-Cases

The GSMA SAM Working Group identified a set of potential of use-cases for the SAM architecture. These include:

Banking services

The end user leverages the payment application installed in the device with its secure counterpart residing in the SAM SD within the eUICC. The SAM Applet will provide access to a set of available services, such as contactless payment and other financial services.

Transport application

The end user leverages the transport application installed in the device with its secure counterpart residing in the SAM SD within the eUICC. The SAM Applet will provide access to a set of available services such as contactless access and other mobility services.

ID application

The end user leverages the identity application installed in the device with its secure counterpart residing in the SAM SD within the eUICC. The SAM Applet will provide access to a set of available services such as controlling authority services or Mobile ID uses.

GSMA IoT SAFE

This use case is related to the IoT domain. GSMA IoT SAFE enables IoT device manufacturers and IoT service providers to protect IoT data communications from IoT device to the cloud, relying on the SIM as a robust, scalable and standardised hardware Root of Trust.

Note that a comprehensive description of the above use cases is included within SAM.01 "Secured Applications for Mobile – Requirements" published by GSMA.

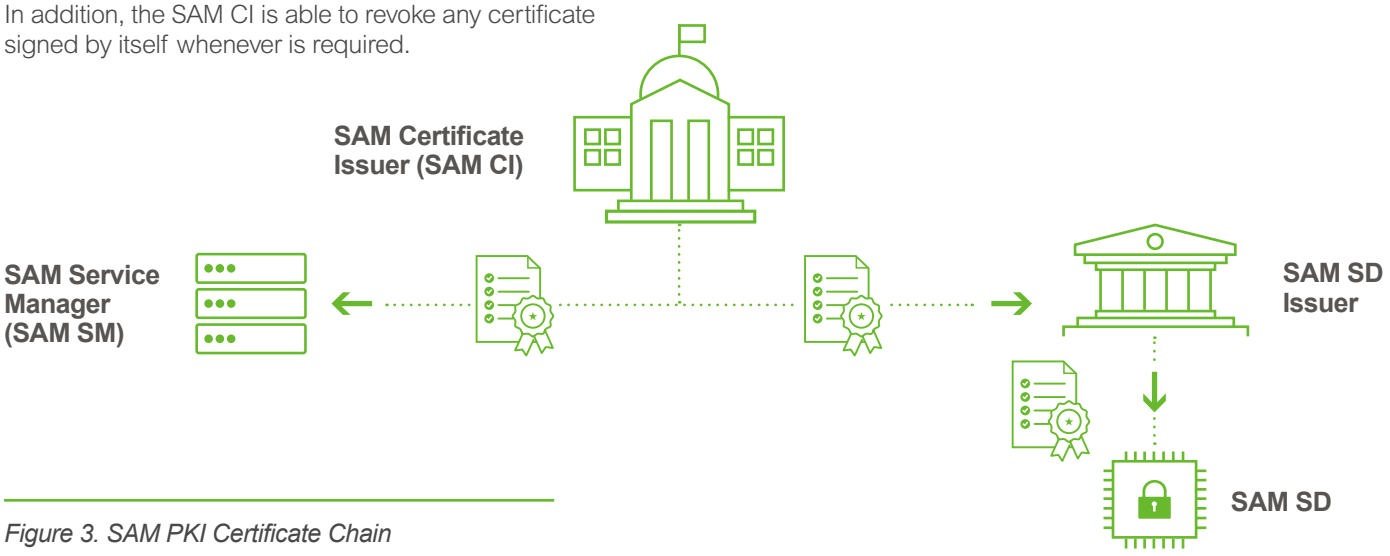


Figure 3. SAM PKI Certificate Chain

4. SAM: Deployment Options

For several years, secure microcontroller providers have produced chips that can be used to build System on Chip (SoC) solutions that support both eUICC and embedded Secure Element (eSE) functionality.

The segregation between the memory area dedicated to the telecom profiles, and the area dedicated to the SE functions, is typically ensured through Java Card and GlobalPlatform specifications, plus several implementation-specific choices.

The deployment of pre-standard solutions, however, is limited by the lack of a certification scheme that sets a minimum security level agreed by the industry for the use-cases it addresses.

The SAM technical specification could be a game changer, as a standardised solution is generally preferred compared to a non-interoperable proprietary deployment. This section explores the different deployment options for SAM technology.

Single physical legacy

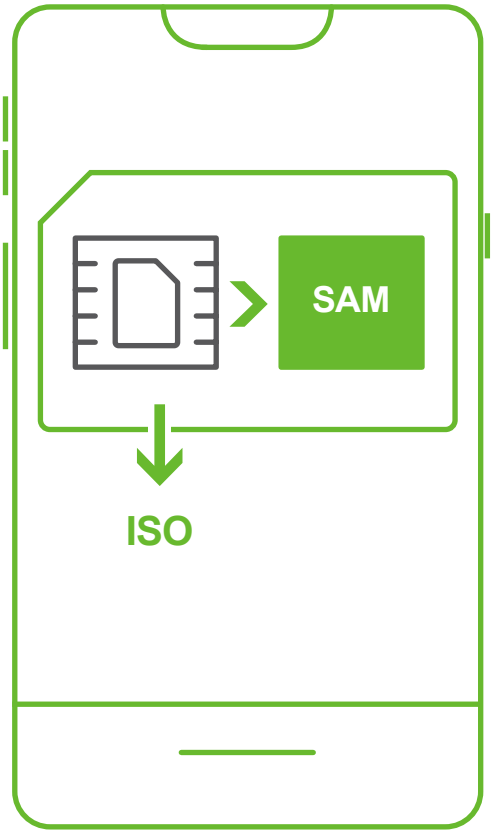
Currently, in any eSIM architecture, the physical interface connecting to the device is the interface as defined in ISO7816. This interface is widely deployed as it was inherited from the legacy SIM cards that have been in use for more than 30 years.

In this scenario, the SAM applications are stored within the eUICC in their own dedicated secure areas outside of the operator areas. The dedicated SAM areas could be remotely managed through existing over-the-air (OTA) protocols (SCP80, SCP81, etc) as any security domain are currently managed.

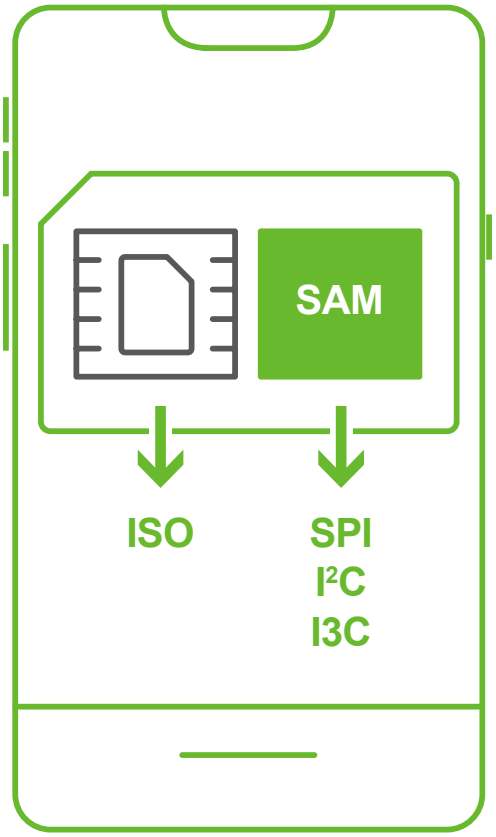
The advantage of this scenario is that it directly leverages existing eUICC technologies. However, the main drawback is that it may create Application Identifier (AID) or other resource conflicts (e.g. Toolkit Application Reference [TAR], channel / timer sharing) between applications inside the operator's area and the SAM area.

This potential issue can be addressed outside of the eUICC using the different service-level agreements (SLAs), or alternatively by defining a prioritisation mechanism within the eUICC.

The disadvantage of this scenario is that some use cases, such as payments and ID, that require access to additional resources from the device (such as biometric sensors or NFC) need additional integration efforts as the ISO interface is used for the connection between the eSIM and the baseband.



ISO interface for eSIM and other interface for SAM



While all communication to and from the eSIM uses the interface as defined in IS07816, another interface is required for the SAM applications to run in parallel.

Current hardware usually supports additional interfaces such as I2C, I3C or Serial Peripheral Interface (SPI). For the purpose of a multi-application scenario, these interfaces can be leveraged for the SAM operations.

This model is a natural evolution from the current situation where two separate chips are used for the standalone eSIM and the standalone eSE. This means that the two separate physical interfaces for the two entities are retained (which in this deployment scenario are no longer physical, but logical), while still allowing the printed circuit board (PCB) design to be optimised with a single physical chip.

Additionally, this model offers a solution to the AID conflict issue. When addressing a SAM applet through the dedicated physical interface, the physical interface may provide the capability to use more than one logical interface (i.e. dedicated logical interfaces between one device application and its corresponding SAM applet). Two SAM applets by different ASPs, even when they share the same AID, are accessed on two different SAM logical interfaces, removing any ambiguity due to the AID conflict.

It should be noted that some of these alternative physical interfaces have the capability to provide more than one logical interface (e.g. I3C), while others may require a specific mechanism to be put in place (similarly to MLI on ISO).

Multiplexed ISO

The idea of multiplexing[2] the ISO interface was developed within GSMA in order to allow the eSIM to enable more than one profile at the same time.

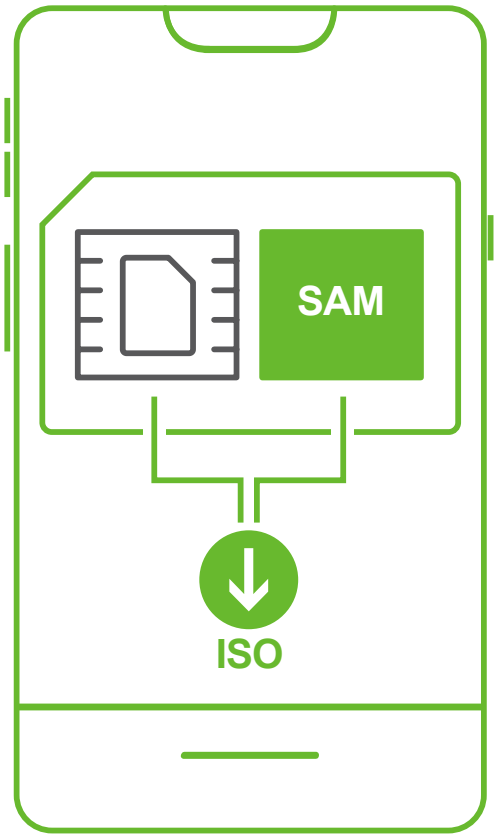
To make this feasible, ETSI developed the Multiple Logical Interface (MLI) feature that allows multiplexed communications of various logical channels in one single physical ISO interface. This creates two logical ISO interfaces based on a single physical ISO interface that can also be switched depending on the use case: one for the eSIM and the other for SAM use-cases. The idea is to have the SAM application residing as a logical SE with a logical ISO interface, while at the same time having the eSIM with another logical ISO interface.

The advantage of this model is that it relies on one single interface to connect the eSIM and the eSE logical parts.

However, since this approach uses ETSI's MLI to multiplex between the eSE and eSIM parts, the disadvantage is that the OS shall implement MLI in devices that do not support multiple enabled profile (MEP). Another disadvantage is that when the ISO interface is used for eSE communication, it cannot be used at the same time for the communication with the profile. This may introduce additional latency (e.g. in authentication).

In addition, and similar to the 'single physical legacy option', more integration efforts are required to access the additional resources from the device.

It should also be noted that this model offers a different solution to the AID conflict issue. When addressing a SAM applet, the latter can be addressed through a dedicated eSIM port. Two SAM applets by different ASPs, even when they share the same AID, shall be accessed through two different eSIM ports, so removing any ambiguity due to the AID only. Nevertheless, the more eSIM ports that are used at the same time, the higher the potential latency in communication between the baseband and the profile(s)



[2]Multiplexing is a method by which multiple signals are combined into one over a shared medium, enabling multiple connections to run at once.

Integrated ecosystems

Regarding integrated technologies, physical Interfaces are not present (although logical connections are required). These architectures implement these previously external interfaces internally to the architecture of the chip, to be able to communicate with external entities.

For example: in the case of an integrated SIM and integrated SE (iSE) integrated in a baseband, the ISO interface will not be visible externally to the SoC. Regarding SAM, the different applets will be able to make use of the I2C, I3C, SPI or any other technology provided by the SoC and the OS maker.

The AID conflict issue can be solved through either of the solutions above, assuming that at least one of the physical interfaces to the SE is made available externally to the iSE.

5. SAM: Overcoming the Limitations and Challenges

The introduction of eSIM technology has had a transformative effect across the entire industry, impacting many aspects of the value chain for solution providers and OS manufacturers. As with any new architecture, it is anticipated that the new SAM architecture – particularly in conjunction with the eSIM architecture – may present challenges across different areas:

Hardware Limitations

The requirement for greater capacity and more power to run larger applications presents ongoing challenges for silicon suppliers, mainly due to the limited physical size of the hardware.

Logical Limitations

Related to the hardware limitations, the physical or logical interface domain may also present constraints. For example, the need for more than one interface or the multiplexing of a single ISO interface are potential limitations that need to be considered.

Development Limitations

Traditional eSIM OS suppliers also face challenges to develop this new architecture, especially if it is in combination with the eSIM architecture.

Also, there is the potential for new market challengers as SAM opens the platform to other industries across the expanding IoT ecosystem.

To be accepted by the industry, the standardised solution must take into account the evolution and enhancement of the existing technologies, otherwise it will not have the required acceptance.

Certifications and Certificate Tree(s)

At the time of writing this paper, the certification process is under discussion as well as the chain of trust for the different applications hosted in SAM.

Regarding certifications, it is possible that the different industries making use, or developing, their own ASP-SDs may require their own certification processes to be applied (e.g. EMVCo for payments, Car Connectivity Consortium for keyless car entry, and eIDAS for ID). Different compliance programmes will make hosting all the target applications the SAM is considering increasingly complex.

Regarding the Certificate Tree(s) or Root of Trust(s), different models can be proposed: one SAM CA managed by GSMA, different CAs for the different ASP-SDs, different CAs for different SAM-SDs, different CAs for each SAM-SD and more CAs for the different ASP-SDs. Certainly, the last two points may over-complicate the ecosystem if it is not handled appropriately.

Other Considerations

The key rule when it comes to simplifying and increasing the speed of adoption of the SAM technology may be based on industry regulations. There are specific applications (such as the European Digital Wallet), on which governments have significant stakes, and may want to push their own security and functional requirements.

Therefore, time to market is a key driver when deploying a new solution. Today, non-standardised versions of the solution are already deployed in the field and could be considered as a “de facto standard” because they are proposed and managed by leaders in the mobile market (devices and applications).

6. Conclusion: Realising the Potential of SAM Technology

Rising demand for applications running on mobile devices like payments, transport ticketing, identity management and secure IoT services has created an immediate market need for a secure, interoperable, scalable, standardised solution for a multi-application capable SE in a multi-application environment.

It is TCA's position that GSMA's SAM initiative is a potentially transformative technology. The eSIM is already deployed across hundreds of millions of devices to deliver flexible, trusted cellular connectivity. By leveraging this proven and reliable platform to host secure applets, SAM technology should be considered as a natural evolution of eSIM that can significantly increase and extend its utility across various additional use cases beyond pure telecoms. This will deliver value to stakeholders across the entire mobile and connectivity ecosystem.

Despite this potential, there remains considerable challenges. In particular, mitigating the risk and impact of market fragmentation and interoperability issues must be an industry priority.

TCA will continue work to influence the development of the SAM specifications through its extensive engagement with GSMA, and is committed to working collaboratively with our members and partners across the ecosystem to promote the development and deployment of standardised SAM solutions.

7. 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
Kigen
Linxens crafting the future of connections
NXP
OASIS Embed. Connect. Activate
Qualcomm
life.augmented
THALES
Valid
WORKZ
TIANYU