An essential guide to GSMA eSIM certification

Kigen

Guide

Contents:

About Kigen

Kigen has been at the forefront of challenging traditional SIM and SIM technology delivery to customers and into cellular devices. From allowing a flexible approach to SIM hardware selection, personalization and supply through to driving the evolution of SIM technology with remote SIM provisioning and the SIMs transition and introduction into a secure enclave on a System on Chip (SoC).

Kigen's SIM and remote SIM provisioning technologies are the foundation on which the cellular IoT revolution will be built and will pave the way for transforming the way people live and businesses operate. Its advanced, GSMA-compliant SIM solutions deliver eSIM functionality, remote management and high security for cellular IoT. They also pave the way toward iSIM-based devices, enabling higher integration and lower total cost of ownership.

Through our technology partners and support from key ecosystem players, Kigen is driving IoT innovation so chip makers, device makers, mobile network operators, and IoT platforms can realize the full potential of cellular IoT.

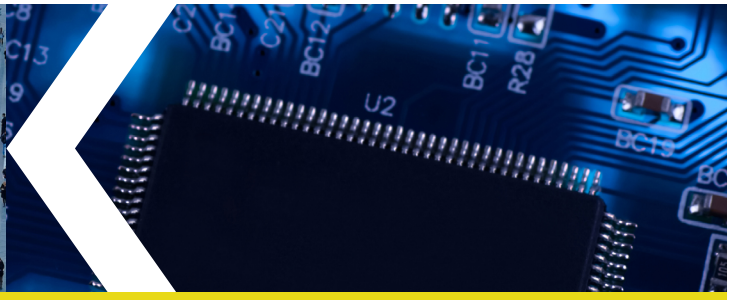
Confused about terms?

Visit www.kigen.com/glossary/.

Introduction

Embedded SIM (eSIM) provides numerous advantages over conventional SIM. Primarily, it allows for the design of smaller cellular-enabled devices and the ability to store and remotely change network operator's connectivity credentials, known as operator profiles, to enable access to different cellular networks without having to physically swap SIM cards. This ability to manage, or provision, operator profiles 'over the air' brings greater flexibility and convenience to how we connect and manage cellular-enabled devices.

Are eSIMs as secure and interoperable as SIM cards? Yes, thanks to the multi-layered GSMA eSIM certification scheme that protects device makers, device owners and mobile network operators (MNOs). The ability to provision operator subscription data securely requires encrypted connections, data protection and system reliability. eSIM certification helps to create a truly standardized and secure ecosystem where certified devices are assessed and validated to ensure full interoperability and security.



Two groups – or solutions - of GSMA eSIM specifications currently exist:

The consumer solution serves the needs of customer electronics sectors, where device end users actively authorize/change their network connectivity provider.

The machine-to-machine (M2M) solution serves the needs of B2B customers, specifically in the Internet of Things (IoT) market.

This guide covers the key areas of ensuring compliance with the GSMA specifications for the M2M solution.

Similar, yet different:consumer and M2M solutions

Want to find out more about the eSIM consumer solution?
Visit www.gsma.com/esim.

The GSMA eSIM solution for M2M predates the consumer one, and they use similar yet different architectures. Both solutions are based on a secure element in the device, the embedded UICC (eUICC), for the storage and management of profiles. Both use common features such as a remote SIM provisioning (RSP) system and secure channels. However, the solutions are fundamentally technically different, reflecting the different use cases and business requirements they fulfil.

The key differences are the direction of control and server management relationship. The consumer solution relies on local end-user control: consumers trigger new profile downloads as they select operators though their device interfaces. In M2M, profiles are managed remotely, without any local human control (other than fallback recovery).

Furthermore, the M2M eUICC can only be managed by a single, pre-determined M2M RSP server as opposed to the consumer eUICC, which can communicate with and receive profiles from any compliant consumer RSP server.

For a list of key documents related to RSP for M2M,

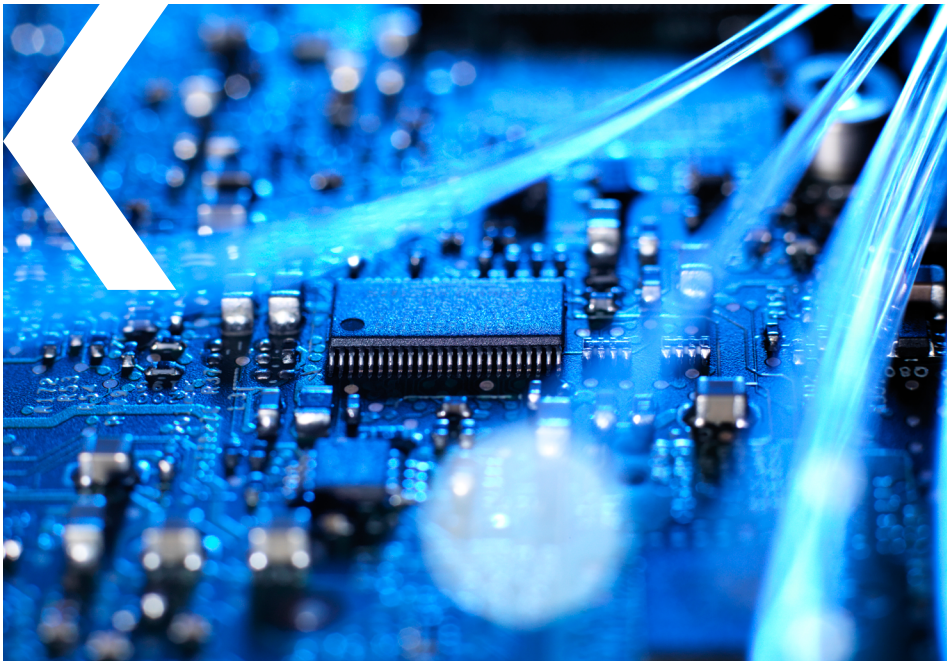
visit https://www.gsma.com/iot/embedded-sim/.

Compliance process overview

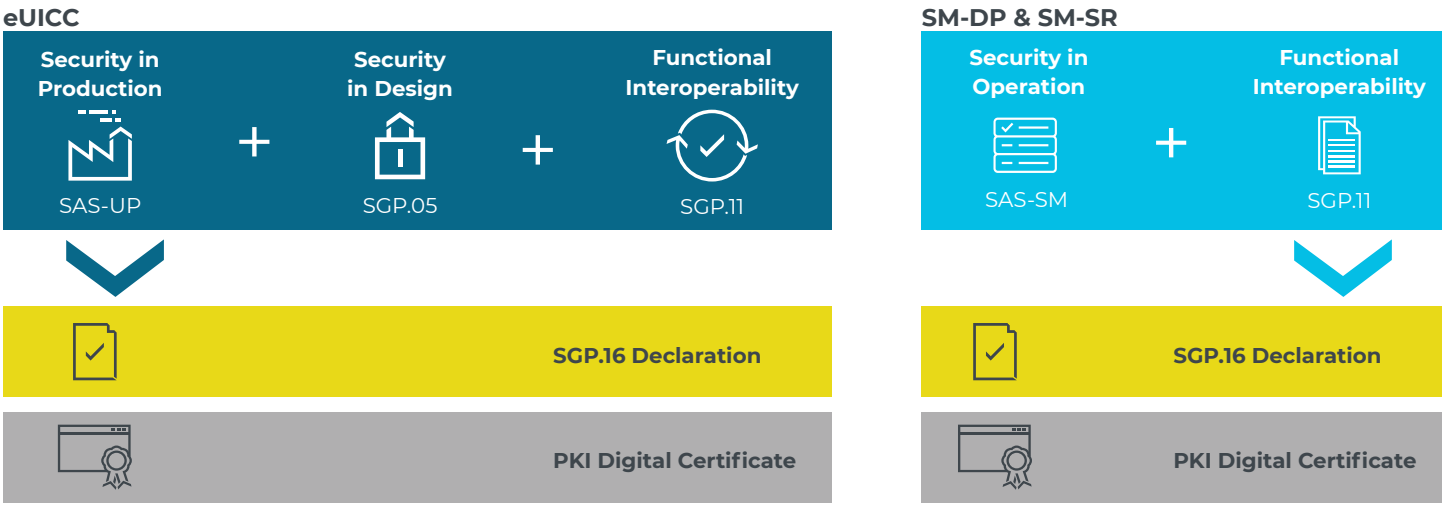
The industry's assurance requirements for the M2M solution have been consolidated into a comprehensive compliance process defined and managed by the GSMA, as documented in SGP.16 M2M Compliance Process.

The process covers the following areas of compliance, based on distinct GSMA reference documents:

- Functional certification of the remote provisioning architecture for eUICC under SGP.11 Remote Provisioning Architecture for Embedded UICC Test Specification
- Security certification:
  - Evaluation of security by design for eUICC under BSI-CC-PP-0089 eUICC Protection Profile (against the features specified in SGP.05 Embedded UICC Protection Profile) and hardware under BSI-CC-PP-0084 Security IC Platform Profile with Augmentation Package (or its predecessor BS-CC-PP-0035).
  - eUICC production site security (SAS-UP) audit under FS.04 Security Accreditation Scheme for UICC Production and FS.17 SAS Consolidated Security Requirements.
  - Subscription management server site security (SAS-SM and SAS-DP) testing under FS.08 SAS Standard for Subscription Manager Role and FS.17 SAS Consolidated Security Requirements.



The GSMA compliance process



The GSMA compliance scheme requires that each of these components and associated processes are subjected to assessment and testing, with submission of the evidence or results to the GSMA for review. Only the products and services that successfully fulfil all the above compliance requirements are eligible for an SGP.16 declaration and Public Key Infrastructure (PKI) digital certificates. The certificates are trust tokens confirming compliance with the relevant GSMA standards.

Functional interoperability testing

As a starting point, eSIMs must demonstrate the required functionality and security as set out in the following documents:

- SGP.01 RSP Architecture
- SGP.02 Remote Provisioning Architecture for eUICC Technical Specification

Functional compliance testing under SGP.11 Remote Provisioning Architecture for Embedded UICC Test Specification handles both interface compliance and system behavior against features specified in SGP.02, and provides test scenarios that are deemed as key for a compliant product. Black box testing ensures the functional integrity and interoperability of eSIMs.

For a list of GlobalPlatform qualified labs,

visit www.globalplatform.org/laboratories.

The SGP.11-based M2M test plan and certification program are managed by GlobalPlatform on behalf of the GSMA. Testing can be done through a qualified lab that has successfully met the GlobalPlatform criteria and demonstrated expertise for functional and/or security certification. Self-testing and validation by the eUICC vendor using qualified test tools is also permitted, with the results and compliance claim submitted to the GlobalPlatform website. Qualification against the GlobalPlatform functional certification enables eUICC providers to demonstrate that their product complies with SGP.01 and SGP.02 specifications, supporting interoperability.

In addition, eSIMs must also offer the required interoperable profile package as defined by the Trusted Connectivity Alliance (TCA), formally known as the SIMalliance, in eUICC Profile Package: Interoperable Format Technical Specification.

GSMA-compliant eSIMs are readily verified and provisioned by subscription management servers they're associated with. Let's further explore eSIM certification and how it instills confidence and trust in M2M devices and networks.

Common Criteria (CC) is an international scheme used to assure security-enforcing products.

EAL is its security assurance level standard, ensuring that the designed security features are properly implemented.

Evaluation of security by design

Security by design is assessed by penetration testing at both the hardware and software levels. Tests are performed in accordance with BSI-CC-PP-0089 (against features specified in SGP.05 Embedded UICC Protection Profile) and BSI-CC-PP-0084 (or its predecessor BS-CC-PP-0035).

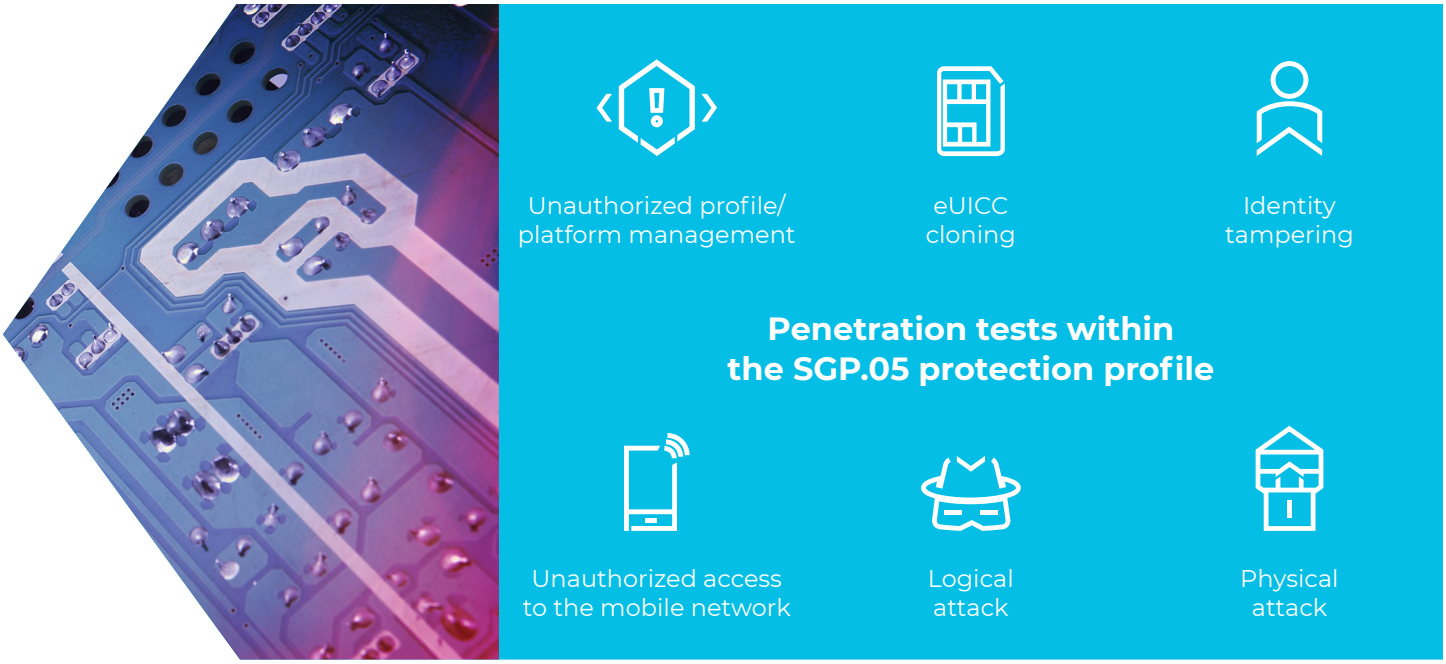
These documents describe the target for the assessment, methodology and the Common Criteria security assurance level that is achieved. An eUICC must be certified in composition to an assurance level of EAL4+ mandated by SGP.05. Assessment and issuance of the certification report is performed by a security laboratory (for example, IT Security Evaluation Facility), qualified by a Common Criteria certification body such as ANSSI or BSI. A list of the qualified laboratories is available here.

Two threat agents are considered: an off-card actor or an on-card application. Off-card actors attempt to use the external interfaces of the eUICC, primarily the interfaces to the mobile network, mobile devices and over-the-air mechanisms. On-card applications can access resources, including APIs, policy enforcement interfaces, the APDU buffer and global byte array, as well as runtime environment interfaces such as the Java Card virtual machine and runtime environment.

Penetration tests defined within the SGP.05 protection profile consider a range of first and second-level threats:

- Unauthorized profile/platform management
- eUICC cloning: using a legitimate profile on an unauthorized eUICC or simulator
- Identity tampering: leaking or modifying identity data belonging to a legitimate actor
- Unauthorized access to the mobile network: accessing the mobile network in place of the legitimate profile
- Logical attack: bypassing security measures by manipulating code and data
- Physical attack: bypassing security measures through physical tampering

These penetration tests assure subscriber and network security through a review of the software implementation. eSIM technology also provides physical security against tampering and many other physical attacks, since eSIMs cannot be readily accessed and removed.



The GSMA Security Accreditation Scheme (SAS) includes SAS-UP (covering security of eUICC manufacturing) and SAS-SM (covering security of subscription management operations).

Testing of security in production

The compliance declaration requires the submitting party to identify and assess the production sites in which the eSIM will be personalized. The SAS-UP audit against FS.04 Security Accreditation Scheme for UICC Production assesses security in the production sites' systems and processes, including looking at how sensitive data is handled during eUICC production. eUICCs can join the trusted ecosystem only if their production site has been certified as secure.

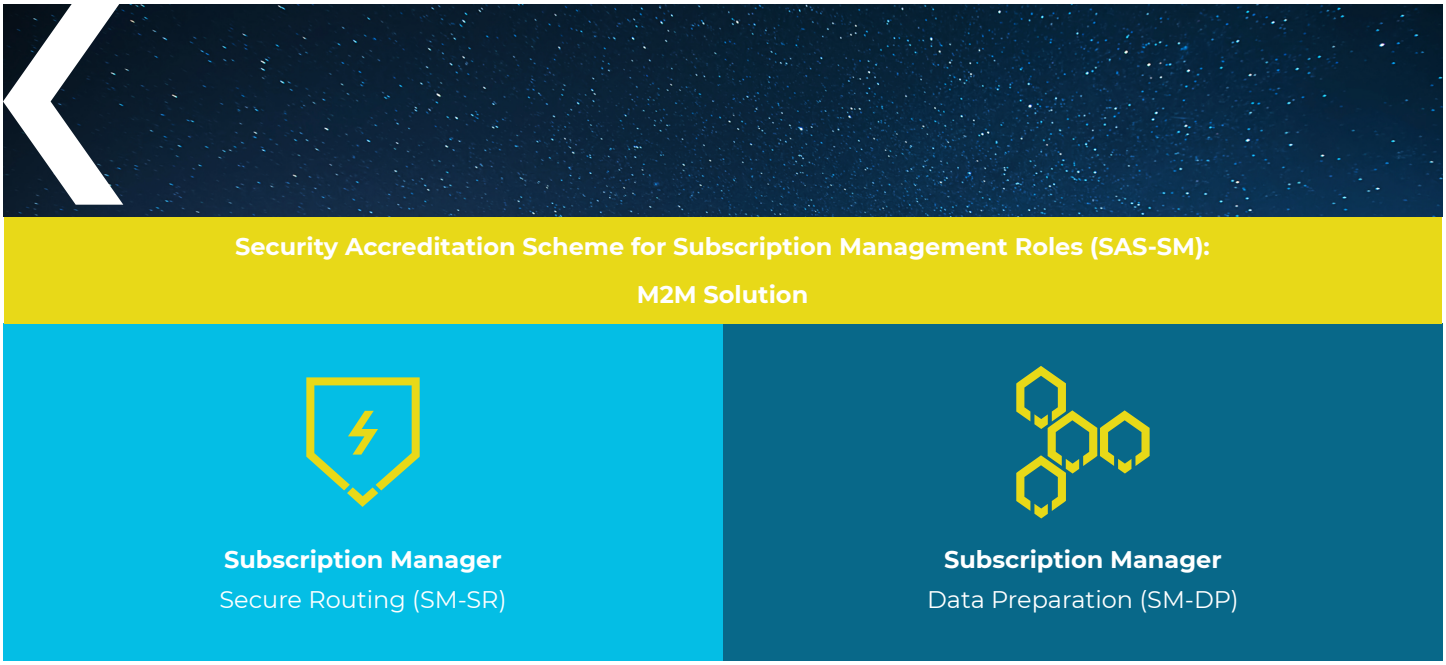
Certification is issued to a specific site. If manufacturing is conducted at more than one site, separate audits are conducted, and separate certificates are issued. All processing stages conducted at a certified site are considered within the scope of an SAS-UP audit.

Each SAS-UP certificate is issued for a defined period. Typically, first-time certificates are issued for one year. When an existing certified production site renews, the renewal certificate generally lasts for two years.

Testing of subscription management server security

The GSMA Security Accreditation Scheme for Subscription Management Roles (SAS-SM) is a scheme through which eSIM service suppliers subject their operational sites to a comprehensive security audit to ensure that adequate security measures to protect the network security have been implemented. The following services are covered by the audit:

- Subscription Manager – Secure Routing (SM-SR)
- Subscription Manager – Data Preparation (SM-DP)



For the consumer RSP solution, the audit also covers the Subscription Manager - Discovery Server (SM-DS) and Subscription Manager - Data Preparation Plus (SM-DP+) services.

The SAS-SM audits against FS.08 assess the RSP server deployment, considering its implementation, processes and system architecture. They help achieve end-to-end server compliance, reducing the risk of subscriber and network security breaches.

There is an audit for each type of service and, in combination, these audits assess how profile data is generated, how profiles are introduced into an eUICC and how profiles are managed over their life cycle. The audits cover:

- Security policy
- Personnel and physical security
- Certificate and key management
- Sensitive process data management
- Logistics management
- Computer and network security, and more.

The GSMA maintains a public list of suppliers accredited for SAS-UP and/or SAS-SM.

Ensuring confidence and trust in the eSIM ecosystem

eSIM is relatively new to the market, so growing a healthy ecosystem is key to its adoption. Interoperability and security specifications from GSMA help ensure a truly standardized ecosystem for eSIM-enabled IoT devices. The multi-level eSIM certification scheme delivers confidence through a thorough security review that is uniformly applied for every certified supplier. When an operator provisions a device with eSIM technology, both the network and device owners are protected.

The path to a trillion connected devices depends directly on trust. eSIM certification is the only route to obtain the necessary digital certificates for RSP, which in turn ensures secure identities for M2M devices. With multi-level certification testing in place, network operators need not vet every single eSIM-enabled device attempting to join their network. All eSIM ecosystem participants can unequivocally rely on these M2M solution certification benefits.

Find out more about Kigen solutions at www.kigen.com

GSMA-compliant eSIM solutions from Kigen

Kigen have progressed two secure server sites, hosting their SM-DP & SM-SR solutions, through the GSMA M2M SAS-SM accreditation and compliance to achieve full RSP certification. These are managed in a full operational stance, hosting key partners RSP services and integration. Kigen's SIM data generation capabilities, also hosted in one of our secure server sites, have also been progressed through the respective SAS-UP accreditation. Our eSIM OS products, using the SAS-UP capability, have also successfully achieved security evaluation and functional compliance to meet the GSMA interim product declaration and EUM certification.

Kigen's cutting edge eSIM and iSIM technology comprises of two elements:

Kigen OS helps create secure eSIMs and secure iSIMs that enable lower power, lower cost devices. Its secure, GSMA-compliant eUICC SIM OS stack is optimized for compactness and portability to multiple hardware form factors.

Kigen

Kigen server solutions provide a certified, complete RSP solution for eSIM and iSIM technology. The modular design offers flexibility and easy integration into environments at MNOs and IoT platform providers.

Note: all links to reference and specification documents are correct at the time of writing.

Kigen