

RSP Compliance Process

Version 2.5

28 March 2023

This Industry Specification is a Industry Specification of the GSMA

Security Classification: Non-confidential

Access to and distribution of this document is restricted to the persons permitted by the security classification. This document is subject to copyright protection. This document is to be used only for the purposes for which it has been supplied and information contained in it must not be disclosed or in any other way made available, in whole or in part, to persons other than those permitted under the security classification without the prior written approval of the Association.

Copyright Notice

Copyright © 2023 GSM Association

Disclaimer

The GSM Association (“Association”) makes no representation, warranty or undertaking (express or implied) with respect to and does not accept any responsibility for, and hereby disclaims liability for the accuracy or completeness or timeliness of the information contained in this document. The information contained in this document may be subject to change without prior notice.

Compliance Notice

The information contain herein is in full compliance with the GSM Association’s antitrust compliance policy.

This Permanent Reference Document is classified by GSMA as an Industry Specification, as such it has been developed and is maintained by
GSMA in accordance with the provisions set out in GSMA AA.35 - Procedures for Industry Specifications.

# Introduction

## Overview

This document describes the common set of compliance requirements by which Remote SIM Provisioning (eSIM) products can demonstrate and declare compliance with the GSMA Consumer eSIM Architecture and Technical PRDs; SGP.21 [1] and SGP.22 [2].

Specific requirements to declare compliance are described according to the eSIM product or service, and include the following:

* Functional compliance to GSMA’s Consumer eSIM PRDs,
* Product security; both platform (hardware) and specific eUICC security requirements,
* eUICC production site security, referencing GSMA’s SAS-UP audit scheme
* Subscription Management server site security, referencing GSMA’s SAS-SM audit scheme

eSIM compliance is an eligibility pre-requisite for the issuance of the X.509 PKI certificates used in Consumer eSIM authentication to eUICC manufacturers and subscription management service providers.

This version of SGP.24, including its associated annexes, supersedes previous versions, as detailed in Annex C.

## Scope

The requirements within this document are applicable to the following Products:

1. Devices supporting an LPA in the device (LPAd) or LPA in the eUICC (LPAe)
2. eUICC, with or without an LPA
3. SM-DP+ and SM-DS providing a Subscription Management service

## Intended Audience

Consumer eSIM product vendors, telecom service providers, test and certification bodies, and other industry organisations working in the area of eSIM.

## Definition of Terms

| Term  | Description |
| --- | --- |
| Digital Certificate (Public Key) | As defined in RFC.5280 [9] or GlobalPlatform specificationsIdentifies its issuing certification authorityNames or identifies the subscriber of the certificateContains the subscriber’s public keyIdentifies its operational periodIs digitally signed by the issuing certification authority. |
| eSIM | As defined in SGP.21 [1]. |
| eUICC | As defined in SGP.21 [1]. |
| Evidence Documentation | Evidence of product compliance to the requirements detailed within this document. |
| Field-Test eUICC | A pre-production eUICC whose functional or security certifications are not yet completed by the EUM. |
| eSIM Product | eUICC, Field-Test eUICC, SM-DP+ (Subscription Manager Data Preparation), SM-DS (Subscription Manager Discovery Services) and Devices that are designed to support the GSMA defined Remote SIM Provisioning feature. |
| eSIM Product Vendor | The manufacturer or service provider of an eSIM Product  |
| Tamper Resistant Element | As defined in SGP.21 [1]. |
| Type Allocation Code | Initial eight-digit portion of the 15-digit IMEI used in 3GPP mobile devices |

## Abbreviations

| Abbreviation | Description |
| --- | --- |
| EID | eUICC identifier |
| eSA | eUICC Security Assurance |
| EUM | eUICC manufacturer |
| IMEI | International Mobile Equipment Identity |
| LPA | Local Profile Assistant |
| PRD | Permanent Reference Document |
| SAS | GSMA Security Accreditation Scheme |
| SAS-SM | SAS for Subscription Management  |
| SAS-UP | SAS for UICC Production |
| SM-DP+ | Subscription Manager Data Preparation + |
| SM-DS | Subscription Manager (Root or Alternative) Discovery Service |
| TAC  | Type Allocation Code |
| TRE | Tamper Resistant Element |

## References

Refer to the eSIM Certification Applicability table in Annex C of this document to identify the valid versions(s).

| Ref | Document Number | Title |
| --- | --- | --- |
| 1.
 | GSMA PRD SGP.21 | eSIM Architecture Specification |
| 1.
 | GSMA PRD SGP.22 | eSIM Technical Specification |
|  | GSMA PRD SGP.23 | eSIM Test Specification |
|  | GSMA PRD SGP.25 | eUICC for Consumer Devices Protection Profile |
|  | GSMA PRD FS.04  | Security Accreditation Scheme for UICC Production – Standard |
|  | GSMA PRD FS.08 | GSMA SAS Standard for Subscription Manager Roles |
|  | GSMA PRD SGP.14 | GSMA eUICC PKI Certificate Policy |
|  | RFC 2119 | “Key words for use in RFCs to Indicate Requirement Levels”, S. Bradner http://www.ietf.org/rfc/rfc2119.txt |
| 1.
 | RFC 5280 | Internet X.509 PKI Certificate and CRL Profile |
|  | GSMA PRD SGP.06  | eUICC Security Assurance Principles  |
|  | GSMA PRD SGP.07  | eUICC Security Assurance Methodology  |
|  | Void | Void   |
|  | GSMA PRD AA.35 | Procedures for Industry Specifications Product  |
|  | GSMA PRD SGP.08  | Security Evaluation of Integrated eUICC based on PP-0084 |
|  | eUICC Profile Package  | Trusted Connectivity Alliance (TCA) eUICC Profile Package: Interoperable Format Technical specification   |
|  | TCA Test  | Trusted Connectivity Alliance (TCA) eUICC Profile Package: Interoperable Format Test Specification   |
|  | GSMA PRD SGP.18 | Security Evaluation of Integrated eUICC based on PP-0117 |

## Conventions

The key words “MUST”, “MUST NOT”, “REQUIRED”, “SHALL”, “SHALL NOT”, “SHOULD”, “SHOULD NOT”, “RECOMMENDED”, “MAY”, and “OPTIONAL” in this document are to be interpreted as described in RFC2119 [[8]](#RFC2119).

# Compliance Overview

The GSMA Consumer eSIM architecture PRD, SGP.21 [1], specifies the high level security and functional requirements for eSIM Product compliance. The eSIM Technical Specification, SGP.22 [2], provides the technical description of the eSIM architecture, and is the technical reference for test and compliance requirements.

Compliance is essential for interoperability within the Consumer eSIM ecosystem. This document provides the framework within which:

* eUICC, SM-DP+ and SM-DS requiring eSIM PKI certificates for eSIM operation can demonstrate the prerequisite functional and security compliance to the Consumer eSIM requirements.
* Field-Test eUICC requiring eSIM PKI certificates for eSIM operation are exempted from the compliance rules set in this document if the Field-Test eUICC is operated according to the requirements set for Field-Test eUICCs in SGP.21 [1] (version 2.4 or higher) and SGP.22 [2] (version 2.4 or higher).
* An eSIM Device can demonstrate functional compliance to the Consumer eSIM requirements.

The expected means to demonstrate compliance are detailed in this document, together with the declaration templates to be used for an SGP.24 declaration.

Specific references for all compliance requirements can be found in Annex C, categorised as either “Site Security Requirements”, “Product Security Requirements” or “Functional Requirements”.

It is recommended to refer to Annex C when planning a product or service compliance in order to identify the validity and applicability of referenced specifications and requirements.

# Compliance Declarations

To declare compliance with SGP.24, the product SHALL:

* Be compliant with the technical requirements defined in the GSMA PRD SGP.21 [1] and GSMA PRD SGP.22 [2].
* Have demonstrated its compliance using the means described in SGP.24, and its Annex C.

The compliance declaration templates are in Annex A of this document, and SHALL be submitted to RSPCompliance@gsma.com for verification once all compliance requirements have been met. The Compliance declaration comprises:

* Completed template Annex A.1: the Product Declaration, which also provides details of the organisation responsible for the declaration,
* Completed template Annex A.2 or A.3 or A.4 or A.5 (as applicable): the compliance details of the declared eSIM Product or service.

The GSMA turnaround time for issuing a confirmation of compliance declaration is 2 working days.

|  |  |  |  |
| --- | --- | --- | --- |
| Product type | Product Declaration | Details of Security Compliance | Details of Functional Compliance |
| Device | Annex A.1 | n/a | Annex A.2 |
| eUICC | Annex A.1 | Annex A.3 | Annex A.3 |
| SM-DP+ | Annex A.1 | Annex A.4 | Annex A.4 |
| Alt SM-DS | Annex A.1 | Annex A.5 | Annex A.5 |

1. : Compliance declaration templates

NOTE: No compliance declarations are required for Field-Test eUICC products.

## Compliance Maintenance

A compliance declaration is an indication of:

* the initial compliance of the product, at the time of declaration,
* the ongoing compliance of the product, including any hardware or software updates affecting eSIM features.

A new declaration (i.e. latest SGP.24 template) is to be submitted for any changes to eSIM product e.g. change in eSIM features.

An updated declaration (i.e. update of the initial SGP.24 declaration made for the product) is required for SAS related production changes – e.g. the addition of a new SAS site for the production of the product.

In either case, the declaration will be verified to check the product has demonstrated compliance using the applicable version of SGP.24 (i.e. the initial or latest version) according to the reason for compliance maintenance.

Changes to a compliant product that result in it no longer being compliant to the initially declared specifications shall be notified to the GSMA with a request for compliance to be withdrawn. As a consequence, GSMA will remove the declaration from its InfoCentre data.

### Specific Considerations for eUICC

To expedite urgent fixes of the eUICCs that already declared compliance, an updated compliance declaration can indicate fast-track if all of the following conditions are met:

* The eUICC has already declared compliance (i.e., the compliance declaration is "active"(NOTE)) with either SOG-IS Common Criteria or GSMA eSA security evaluation schemes;
* The updated eUICC maintains compliances to the same versions of SGP.21 [1] and SGP.22 [2] in the updated compliance declaration;
* The updated eUICC support the same features (optional and mandatory) as the original eUICC; and
* The updated eUICC has been evaluated (with code review and, if the update affects RSP functions, functional testing) by the security laboratory and impact assessment report has been issued by the security laboratory indicating that the updated eUICC product is resistant against high attack potential.

NOTE: While an eUICC is marked as "update ongoing" on the compliance declaration by the GSMA, there cannot be another fast-track certification update.

An updated compliance declaration indicating fast-track shall:

* Be acknowledged by GSMA by marking the compliance declaration as "update ongoing";
* Provide the security certification report reference of the existing declaration of the eUICC (see also Annex A.3);
* Be followed by an updated compliance declaration with re-issued certification report references as soon as they are available. This must be completed within 4 months, where GSMA may allow additional 2 months upon request from the security lab. Otherwise GSMA will remove the compliance declaration from its GSMA eSIM Compliance database data by marking it as "expired".

### eUICC Compliance Expiration

The eUICC manufacturer SHALL maintain SAS-UP accreditation by proper renewal of sites security audits according to GSMA Security Accreditation Scheme (SAS) requirements during the whole manufacturing life of the declared eUICC product.

Functional and security certifications have no expiration dates. Functional and security certifications are valid during the whole life cycle of the eUICC for existing products in the field unless otherwise updated during its lifecycle.

# Compliance Requirements

The compliance requirements are derived from the GSMA SGP.21 [1] eSIM Architecture specification. This section details these requirements and their applicability to eSIM product as:

* Site security requirements for eUICC production sites and Subscription Management service sites,
* Product security requirements (eUICC only),
* Functional requirements, including interoperability.

## Site Security Requirements

All eUICC production sites and all SM-DP+ and SM-DS service sites used in GSMA eSIM must hold a valid site security accreditation for the entire time they are being used for eUICC production or Subscription Management service provision.

Accreditation is from the GSMA Security Accreditation Scheme (SAS). Further details can be found on the GSMA’s [SAS](http://www.gsma.com/aboutus/leadership/committees-and-groups/working-groups/fraud-security-group/security-accreditation-scheme) webpage.

The SAS-UP or SAS-SM certificate reference shall be included in the compliance declaration for an eUICC (annex A.3), SM-DP+ (annex A.4) or SM-DS (annex A.5).

|  |  |  |
| --- | --- | --- |
| Product type | SAS requirement | Compliance requirement |
| Scheme | Required Scope |
| eUICC | SAS-UP | * Management of PKI certificates
* Generation of data for personalisation
* Personalisation
 | Provisional or Full certification |
| SM-DP+ | SAS-SM | * Data centre operations & management
* Data Preparation +
 | Provisional or Full certification |
| SM-DS | SAS-SM | * Data centre operations & management
* Discovery Service
 | Provisional or Full certification |

1. : Operational Security Compliance requirements per product type

### Specific Considerations for eUICC

All SAS-UP scope requirements must be fulfilled; either at the same production site or at multiple production sites, according to the SAS accredited production arrangements for the eUICC.

* Details of all manufacturing sites used in the production of the eUICC shall be provided in its Annex A.3 declaration, clearly identifying the SAS scope for each site,
* All three SAS scope requirements shall be covered by the eUICC production site(s),
* The organisation and site intending to apply for the Digital (PKI) Certificate from the GSMA Root CI shall:
	+ - * be named on the Annex A.1 declaration for the eUICC
			* have Management of PKI Certificates within its SAS-UP accreditation scope

## Product Security Requirements (eUICCs only)

A protection profile has been developed for eUICC software implementing the GSMA eSIM architecture for Consumer Devices. The protection profile is published as GSMA PRD SGP.25 [4], and registered as a Protection Profile by BSI, reference BSI-CC-PP-0100.

eUICC security evaluations are expected to include:

* the complete Target of Evaluation defined in SGP.25 [4]
* the secure IC platform and OS
* the runtime environment (for example Java Card system)

The IC/hardware platform on which the eUICC is based shall be certified to either PP-0084 or PP-0035

The Common Criteria certificates or certificate references ([www.commoncriteriaportal.org/products](https://www.commoncriteriaportal.org/products/#IC)) shall be included in the declaration as evidence of product security compliance.

|  |  |  |
| --- | --- | --- |
| Product type | Product Security Requirement | Compliance requirement |

|  |  |  |
| --- | --- | --- |
| Discrete eUICC | Security IC Platform Protection Profile with Augmentation Package Certification (PP-0084)or Security IC Platform Protection Profile, Version 1.0 (PP-0035) | Common Criteria certified and listed, or scan of certificate attached. |
| Security evaluation reflecting the security objectives defined in SGP.25 [4], with resistance against high level attack potential.See Annex A.3 for permitted methodologies.Testing to be performed at a SOG-IS lab, accredited in the Smartcards & similar devices technical domain. | Refer to Annex A.3, section A.3.4.2  |

1. : Product Security Compliance requirements for Discrete eUICC

A Field-Test eUICCs SHALL use a certified IC platform according to table 4:

|  |  |  |
| --- | --- | --- |
| Product type   | Product Security Requirement   | Compliance requirement   |
| Discrete Field-Test eUICC | Security IC Platform Protection Profile with Augmentation Package Certification (PP-0084)or Security IC Platform Protection Profile, Version 1.0 (PP-0035) | Common Criteria certified and listed |
| Integrated Field-Test eUICC   | Integrated TRE certified following SGP.08 [14] methodology  or SGP.18[17] methodology.     Note: the applicability period of SGP.08 [14] and SGP.18[17] are defined in Annex C.   | Certification Report |  |
|  |

1. : Secure IC Platform requirements for Field-Test eUICC

|  |  |  |
| --- | --- | --- |
| Product type   | Product Security Requirement   | Compliance requirement   |
| Integrated eUICC   | Integrated TRE certified following SGP.08 [14] methodology   or SGP.18[17] methodology.    Note: the applicability period of SGP.08 [14] and SGP.18[17] are defined in Annex C.   | Certification Report  |  |
| Security evaluation reflecting the security objectives defined in SGP.25 [4], with resistance against high level attack potential.  See Annex A.3 for permitted methodologies.  Testing to be performed at a SOG-IS lab, accredited in the Smartcards & similar devices technical domain.   | Refer to Annex A.3, section A.3.4.2    |  |

1. : Product Security Compliance requirements for Integrated eUICC

### Lapse of Compliance

In case of any lapses of RSP compliance as a consequence of a lapse in any individual SAS-UP or SAS-SM certification at eUICC production sites, SM-DP+ or SM-DS services sites used in GSMA eSIM, the following provisions SHALL apply:

1. The GSMA RSP Compliance Team SHALL notify the above loss of SAS certification to all the stakeholders using the listed sites in their eSIM Product declarations (see. Annexes A.3, A.4 and A.5).
2. If all the SAS certifications used by a declared eSIM Product lapse, the GSMA RSP Compliance Team SHALL highlight this loss of compliance to relevant stakeholders (primarily participants in the eSIM PKI ecosystem) via the GSMA RSP compliance products database, and via other GSMA communications (e.g. relevant GSMA mailing lists, newsletters, meetings) considered appropriate to inform those stakeholders.

Following a restoration of any individual SAS-UP or SAS-SM certification after a lapse, it will normally be sufficient for a site to submit a valid SAS-UP or SAS-SM certificate to the GSMA RSP Compliance Team in order to regain RSP compliant status. Resubmission of other declaration templates required by this PRD to gain initial RSP compliance is normally not needed unless the information in those declarations has changed.

## Functional Compliance Requirements

Functional compliance is a requirement for all eSIM Products to assure correct operation. The eSIM Test Specification, SGP.23 [3], provides details of all applicable interface and procedural testing.

Each test in SGP.23 [3] can be mapped to a specific set of requirements in the eSIM Technical Specification, SGP.22 [2].

To demonstrate product functional compliance to SGP.22 [2], an eSIM Product shall successfully pass all tests applicable to its supported eSIM capability. The permitted, product dependent, test methodologies are:

* Functional testing via industry partner certification schemes (for eUICC and Devices),
* Functional testing via vendor implemented test methodologies referencing SGP.23 [3] tests (for SM-DP+ and SM-DS).

### Functional Compliance via Industry Partner Certification Schemes

eSIM Compliance test programmes have been established by industry certification schemes GlobalPlatform, GCF and PTCRB. These provide the required means of test for eUICCs and Devices, referencing the SGP.23 [3] test requirements.

eUICC (annex A.3) and devices (annex A.2) are judged to have met the eSIM functional compliance requirement for a named product if they have a valid, product specific, certification reference from either Global Platform, GCF or PTCRB.

|  |  |  |  |
| --- | --- | --- | --- |
| Product  | Functional test organisation | Compliance requirement (see Annex C for details) | Link to industry certification scheme  |

|  |  |  |  |
| --- | --- | --- | --- |
| Device | GCF  | GCF Certification including eSIM | [GCF](http://www.globalcertificationforum.org/) |
| GCF eSIM Standalone certification | [GCF](https://www.globalcertificationforum.org/rsp.html) |
| PTCRB | PTCRB Certification including eSIM | [PTCRB](https://www.ptcrb.com/) |
| eUICC | GlobalPlatform,  | GP Product Qualification to: (1) GSMA eUICC Consumer functional test suite (2) SIMalliance Interoperable Profile’ test suite (eUICC Profile Package [14]) | [GlobalPlatform](https://globalplatform.org/) |

1. : Functional compliance via GSMA industry certification scheme partners

### Functional Compliance via Vendor Defined Test Plan

Permitted for Subscription Management products (SM-DP+ and SM-DS). The vendor specified test plans shall reference all SM-DP+/SM-DS tests from the eSIM test specification, SGP.23 [3]. Annex A.4 and Annex A.5 provide further details.

|  |  |  |
| --- | --- | --- |
| Product type | Vendor specified test plan permitted | Reference |

|  |  |  |
| --- | --- | --- |
| SM-DP+ | Yes | SGP.23 [3] |
| Alt SM-DS | Yes | SGP.23 [3] |

1. : Functional compliance via Vendor defined test plan

# eSIM Digital Certificates (PKI)

GSMA eSIM uses a Public Key Infrastructure (PKI) Digital Certificate to authenticate the following eSIM system entities that have been confirmed as SGP.24 compliant:

* eUICC
* SM-DP+
* SM-DS

The Public Key Infrastructure (PKI) Digital Certificate of GSMA eSIM may also be used for a Field-Test eUICC which is considered as SGP.24 compliant for the purpose of certificate use if it is operated according to the requirements set for Field-Test eUICCs in SGP.21 [1] (version 2.4 or higher) and SGP.22 [2] (version 2.4 or higher).

Digital Certificates are issued and managed in accordance with GSMA’s PKI Certificate Policy, SGP.14 [9]. Digital Certificate issuance to SGP.24 compliant product is operated on a commercial basis by GSMA appointed Root CIs.

## Specific Considerations for eUICC Certificates

The manufacturer of an SGP.24 compliant eUICC is eligible to request *an* EUM Certification Authority Certificate from the GSMA CI. The issued EUM CA certificate can be used by the eUICC manufacturer to generate eUICC certificates, as needed.

An issued EUM (PKI) Certificate for the initially declared eUICC product is also allowed to be used with additional eUICC product(s). The following provisions apply:

* A new SGP.24 declaration SHALL be submitted for each additional eUICC product intending to re-use an existing EUM CA certificate,
* The additional product reusing an existing EUM CA Certificate SHALL:
	+ - * Have its own evidence of GlobalPlatform functional compliance,
			* Have its own evidence of security evaluation using a GSMA approved methodology valid at the time of declaration (as identified in SGP.24 Annex C),
			* Be manufactured at a SAS accredited site.

Different EUM CA Certificates MAY be requested for the same eUICC product. A new/updated SGP.24 declaration shall be submitted for any change of SAS site(s) intended to be used to manufacture of a declared eUICC product.

An issued EUM (PKI) certificate for the initially declared eUICC product is also allowed to be used with additional Field-Test eUICC product(s). In this case the provisions set in SGP.21 [1] (version 2.4 or higher) and SGP.22 [2] (version 2.4 or higher) for Field-Test eUICC product(s) apply instead of the requirements for functional compliance and security evaluation. The SAS requirements for handling the PKI certificates and credentials apply in any case. The Field-Test eUICC SHALL use a certified hardware according to section 4.2 of this document.

1. Declaration Templates

An eSIM Product declaration consists of Annex A.1 plus either Annex A.2, A.3, A.4 or A.5, according to the product type. Refer to the SGP.24 zip file for the following Annex A templates:

* A.1 eSIM Product Declaration
* A.2 Details of Declared Device
* A.3 Details of Declared eUICC
* A.4 Details of Declared SM-DP+
* A.5 Details of Declared SM-DS
1. VOID
2. eSIM Certification Applicability (Normative)

This Annex identifies the current requirements and specification versions for Consumer eSIM compliance declarations, and includes:

* Security requirements,
* Functional requirements, including means of test.
* Currently recognised exemptions from compliance.

Organisations either planning SGP.24 compliance activities, or interested in the current status of compliance requirements are recommended to reference this table when planning product compliance.

 Table C.1 eSIM Certfication Applicability

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
|   | **Reference** | **Version** | **Applicability** | **Current status for compliance** | **Active from** | **Expiry Date** | **Notes** |
| **GSMA PRDs** | **GSMA PRD SGP.23**  eSIM Test Specification  |                 1.x  Refer to: https://www.gsma.com/esim/esim-specification/   | All eSIM product  | Active  | -  | Refer to: https://www.gsma.com/esim/esim-specification/   |       |
| **GSMA PRD SGP.22**  eSIM Core Specification: Technical  | 2.0  | All eSIM product  | Expired  | 2017-02-06  | 2018-04-30  |   |
| 2.1  | All eSIM product  | Expired  | 2017-02-27  | 2019-12-31  |   |
| 2.2, 2.2.1  (and later 2.2.x)  | All eSIM product  | Active  | 2017-09-01  |   |   |
|  2.3 |  All eSIM product  |  Active  |  2021-06-30 |   |   |
| 2.4 |  All eSIM product  |  Active  | 2021-10-28 |  |  |
| **GSMA PRD SGP.21**  eSIM Core Specification: Architecture  | 2.0  | All eSIM product  | Expired  | 2017-02-06  | 2018-04-30  |   |
| 2.1  | All eSIM product  | Expired  | 2017-02-27  | 2019-12-31  |   |
| 2.2  | All eSIM product  | Active  | 2017-09-01  |   |   |
|  2.3 |  All eSIM product  |  Active  |  2021-06-30 |   |   |
|  | 2.4 |  All eSIM product  |  Active  | 2021-08-03 |  |  |
| 2.5  |  All eSIM product  |  Active  | 2022-11-17 |  |  |
| **Security Compliance** | **BSI-CC-PP-0084-2014**  Security IC Platform Protection Profile with Augmentation Packages Certification (PP-0084)  | 1.0  | eUICC  | Active  | 2017-10-16  |   |   |
| **BSI-CC-PP-0035-2007**  Security IC Platform Protection Profile (PP-0035)  | 1.0  | eUICC  |   |   |   |   |
| **GSMA PRD SGP.25**  Embedded UICC for Consumer Devices Protection Profile  | 1.0  | eUICC  | Active Ref Annex A.3.4.2(b) Option 1  | 2019-11-15  |   |   |
| **SGP.24 Annex A.3 section A.3.4.2(b), option 2:**  Interim methodology – implementation focussed security evaluation  | SGP.24 v2.2 Annex A.3  | eUICC  | Active Ref Annex A.3.4.2(b) Option 2  | 2019-11-15  |    **Existing product in the field**: no expiration if used for the initial security evaluation**Existing product variant**: 2023-01-31**New product**: 2022-07-31 1 and 2 | See table C.2 |
| **GSMA PRD SGP.06** eUICC Security Assurance Principles   | 1.0  | eUICC  | Active  |  2020-07-07   |     |  |
| **GSMA PRD SGP.07** eUICC Security Assurance Methodology   | 1.0  | eUICC  | Active  |  2020-07-07  |   |  |
| **GSMA PRD FS.04**  SAS for UICC production  | Refer to: GSMA.com/SAS for details  | eUICC  | Active  | Refer to GSMA.com/SAS  |   |   |
| **GSMA PRD FS.08**  SAS for SM roles  | Refer to: GSMA.com/SAS for details  | SM-DP+/SM-DS  | Active  | Refer to GSMA.com/SAS  |   |   |
|  | **GSMA PRD SGP.08**Security Evaluation of Integrated eUICC    | 1.1   | Integrated eUICC   | Expired   | 2021-06-30 |    |  |
| 1.2 | Integrated eUICC   | Active   | 2022-09-19 |  |  |
|  | **GSMA PRD SGP.18**Security Evaluation of Integrated eUICC based on PP-0117 | 1.0 | Integrated eUICC   | Active | 2022-09-19 |  |  |
| **Functional Compliance** | **Vendor specified RSP Functional test**  | n/a  | SM-DP+  | Active  | SGP.24v1.0  |   |   |
| SM-DS  | Active  | SGP.24v1.0  |   |   |
| **GCF: GCF-CC**  GCF RSP Functional Test (Devices)  | Refer to GCF for applicable version(s)  | Device  | Active  | SGP.24v2.0  |   |   |
| **Global Platform test suite**  'GP Configuration: eUICC Consumer v2.1 and v2.2 (SGP.22 Spec.)   GP Test Suites:  '- eUICC Consumer SGP.23 Compliance Test Suite (eUICC Consumer SGP.23 Test Spec)   '- eUICC Consumer - SIMalliance Interoperable Profile Test Suite (TCA Test Spec)  | Refer to GP for applicable version(s)  | eUICC  | Active  | SGP.24v2.0  |   | All TCA eUICC Profile Package versions declared in Annex A.3.2 must be covered  by the product functional compliance test.  |
| **Permitted Exceptions** | **Permitted Exceptions agreed for SGP.24 declarations**  | no agreed exceptions in this version of SGP.24  |   |   |   |

(1) A SOGIS Laboratory will only accept new eUICC evaluation projects for Interim Methodology until 2022-05-30 (2 months before expiry date of interim evaluation for new products) to ensure the project is completed or on a mature stage before the expiry date of 2022-07-31. GSMA will accept late entrance of New product until 2022-10-30 for New products that can demonstrate that the evaluation project started before 2022-05-30.

(2) In the situation that a project may be delayed, due to exceptional circumstances, the laboratory responsible for Interim Methodology evaluation may request an extension from GSMA.

Table C.2 Product Type Validity Period of ‘*Interim methodology*’

|  |  |  |  |
| --- | --- | --- | --- |
| **Product Types** | **Description** | **Security Assurance Scheme Allowed** | **Re-Certification Trigger** |
| Existing product in the field | An eSIM product that is produced and ready to be inserted in a device or is inserted in a device which is being used by an end customer or which is in the supply chain from the factory of the device OEM to a store | Throughout the life cycle of an Existing product in the field:* Interim methodology can be used, if it was used originally, assuming updates do not change the initial scope of the product.
* eSA scheme whether it was used originally, or not.
* SOG-IS CC scheme whether it was used originally, or not.
* Certification methodology can be switched at the discretion of the EUM throughout the life cycle of the Existing product in the field.
 | Changes accepted as an update of the Existing product in the field (update of declaration required) constituting a re-certification:  |
| Existing product variant | Any eSIM product type with an approved compliance declaration, that has not been inserted in a device in the field (not yet produced) | On creation of a variant of an Existing product:* Interim methodology can be used, if it was used originally, until the date defined in Table C.1, after which only the eSA scheme or SOG-IS CC scheme will be allowed.
* eSA scheme;
* SOG-IS CC scheme;
* Certification methodology can be switched at the discretion of the EUM throughout the life cycle of the Existing product in the field.
 | Changes accepted as an update of the Existing product variant (update of declaration required) constituting a re-certification:                         * Updates for functional and/or security issues within the initial scope.
* Updates within minor versions of SGP.21 [1] and/or SGP.22 [2] and TCA eUICC Profile Package specifications [15] e.g.
	+ Consumer (SGP.22 [2]) v2.1 to 2.2 , or
	+ TCA eUICC Profile Package [15] v2.2 to v2.3.1.
* IC maintenance release of the same IC even if SOG-IS CC certificate is changed or updated.
* eSIM feature related OS modification(s) requiring a new product declaration as described in chapter 3.1
 |
| New product | Any eSIM product with a new IC platform, a new major version of SGP.21/22 spec or new major version of the profile package specification | For the certification of a New product:* Interim methodology can be used, until the date defined in table C.1, after which only the eSA scheme or SOG-IS CC scheme will be allowed.
* eSA scheme;
* SOG-IS CC scheme;
 | Situations in which a certification as a New product is required :* Change of the IC platform (new IC type/vendor, new technology).
* Support for major updates versions of SGP.21 [1] and/or SGP.22 [2] specification, e.g. SGP.22 [2] v**1**.2 to v**2**.1.
* Support for major updates versions of the TCA eUICC Profile Package [15] specification e.g. v**2**.1 to v**3**.x
 |

Table C.3 Status of Compliance

|  |  |
| --- | --- |
| **Status for Compliance**  | **Description**  |
| Active:   | Specification or reference that is currently valid for SGP.24 declarations. Where multiple versions of the same specification or reference are active, the certifier shall identify which version has been used.   |
| Planned:   | Specification or reference that is under development.   |
| Expired:   | Specification or reference that is no longer valid for SGP.24 declarations.   |
| Deprecated:   | Specification or reference for which an expiry date has been stated, and will no longer be recognized for GSMA eSIM compliance after the expiry date.   |
| Permitted:   | Permitted as an alternative to a mandatory requirement until the indicated expiry date.   |
| Active from:   | The start date from when a specification or reference can be used for SGP.24 declaration.   |
| Expiry date:   | The last date on which an SGP.24 declaration can reference the specification or reference. Declarations using an expired specification or reference will not be accepted.   |

Update requests for this annex, including new requirements, transition timing to new requirements, and expiry dates for deprecated requirements, are via the GSMA CR process. Approved CRs will be reflected in an updated version of this document.

For further details, contact: RSPcompliance@gsma.com.

1. Document Management
	1. Document History

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Version | Date | Brief Description of Change | Approval Authority | Editor / Company |
| V1.0 | 6th Feb 2017 | Initial version of SGP.24 V1.0 eSIM Compliance Products | RSPLEN/PSMC | Gloria Trujillo, GSMA |
| V1.1 | 30th May 2017 | Minor revision to SGP.24 V1.1 ESIM Compliance Products | RSPLEN | Gloria Trujillo, GSMA |
| V2.0 | 15th Feb 2018 | Introduction of functional testing via industry certification schemes.Addition of IC based PP for eUICC (PP-0084) as an interim PP (hardware only) whilst the SGP.25 PP is under development.Addition of an eSIM Certification Applicability table as the means to manage compliance requirements and spec dependencies.Restructure of document to be requirements centric. | RSPLEN | Valerie Townsend, GSMA |
| V2.1 | 7th Dec 2018 | Addition of references, Fast Track process added, Certif expiration and declaration type | RSPLEN | Valerie Townsend, GSMA |
| V2.2 | 29th May 2019 | Updated to include the following CRs: RSPCERT39 Doc 7r1: Section 5: align with SAS on PKI reuseRSPCERT39 Doc 8r1: Section 3.1 added on compliance maintenance.RSPCERT39 Doc 13r0: Annex C updatedRSPCERT42 Doc 7r0: Section 4.2 and A.3 on security assurance (interim methodology)RSPCERT42 Doc 6r1: Annex C update to security assuranceRSPCERT42 Doc19r2: editorials RSPCERT43 Doc 8r2: editorials RSPCERT43bis Doc 3r1:updates following working group review.eSIMWG4#1 Doc 018: updates to Section 3.1 and A.3.4.2 (option 2)  | eSIM Group | Valerie Townsend, GSMA |
| V2.3 |  | CR001R002 Addition of eUICC Assurance Scheme Annex A.3CR004R005 Annex A.4 - Details of SGP.23 testing related to Application Note Issues and check box for revised declaration CR006R001 SGP.24 Introduce GSMA eSACR007R001 Changes in Annex C | eSIM Group | Gloria Trujillo, GSMA |
| V2.4 | 30 June 2021 | CR0009R01 Clarification of the SGP.22 V2.2 eSIM Application NoteCR0012R01 eUICC Statement of Security Evaluation Completion validity five yearsCR0013R01 Deadline to commence interim solution evaluationsCR0014R01 Add of Integrated eUICCCR0015R00 Evaluation project start and finalisationCR0016R00 Optional SetEditDefaultDpAddr and SetEditNicknameCR0017R00 Optional support of downloading PPR to removable eUICCCR0018R02 Change SIMalliance to TCA in SGP.24CR0019R01 Change SIMalliance to TCA in SGP.24 Annex A.3CR0020R00 - Fix in Annex CCR0021R02 eUICC Supporting multiple TCA ePP specs | ISAG | Gloria Trujillo, GSMA |
| V2.4.1 | 16th December 2021 | CR0025R01 - NFC complianceCR0026R00 - Editorial change section 4.2 table 4CR0027R01 - Alignment of Table C2 with chapter 3.1CR0029R00 - Removing self-reference in Table C1CR0023R02 – Interim Security Certification Extension | ISAG | Gloria Trujillo, GSMA |
| V2.4.2 | 28th January 2022 | CR0034R01 - Add Consumer v2.4 to Annex CCR0028R04 - Enable field test eUICC and add Consumer v2.4 to Annex C | ISAG | Gloria Trujillo, GSMA |
| V2.4.3  | 18h May 2022 | CR0033R02 – Add flexibility on EUM PK Certificate useCR0032R03 – Lapses in Compliance | ISAG | Gloria Trujillo, GSMA |
| V2.4.4  | 8th August 2022 | CR0057R02 – Bug fixing related to contradictory dates CR0060R01 – SAS-UP subsequent update v2.4.4 CR0062R01 – SAS-SM subsequent update v2.4.4 - SM-DP+CR0064R01 – SAS-SM subsequent update v2.4.4 - SM-DSCR0065R02 - Removal of interim methodology in Annex A.3CR0068R01 - eUICC Category Note V2.4.4CR0069R00 - Annex A.1, add linkage to other SGP.24 annexesCR0070R00 - Update SGP.08 reference | ISAG | Gloria Trujillo, GSMA |
| V2.5  | 28 March | CR0074R01 - Remove application note from Core SpecCR0075R00 - Remove application note from Annex A.4CR0077R01 - Add reference to SGP.09CR0079R01 - Add SGP.09 in Annex A.3CR0080R02 - Add SGP.18 V1.0 referenceCR0081R02 - Add SGP.18 V1.0 in Annex A.3CR0089R01 - Add SGP.21 V2.5 referenceCR0084R04 - Fast Track for updated compliance declarations of EuiccCR0085R02 - Add certification expirationCR0091R01 - Product declaration type definiton | ISAG | Gloria Trujillo, GSMA |

* 1. Other Information

|  |  |
| --- | --- |
| **Type** | **Description** |
| Document Owner | Gloria Trujillo |
| Editor / Company | GSMA |

It is our intention to provide a quality product for your use. If you find any errors or omissions, please contact us with your comments. You may notify us at prd@gsma.com

Your comments, suggestions or questions are always welcome.