RSP Compliance Process

Version 2.6

27 January 2025

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

Disclaimer

The GSMA 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 GSMA 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 GSMA AA.35 - Procedures for Industry Specifications.

Contents

1 Introduction

1.1 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 and IoT eSIM Architecture and Technical PRDs; SGP.21 [1], SGP.22 [2], SGP.31 [18] and SGP.32 [19].

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 and IoT PRDs,
- Product security; Platform (hardware) and specific Consumer and IoT eUICCs security requirements,
- Consumer or IoT 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 GSMA Confirmation of PKI issuance and the subsequence issuance of the X.509 PKI certificates used in Consumer and IoT eSIM authentication to eUICC manufacturers and subscription management service providers (SM-DP+ and SM-DS).

eSIM compliance is an eligibility pre-requisite for the issuance of Confirmation of Compliance document used for LPA, IPA and eIM providers but there is no associated X.509 PKI certificates issued by the GSMA CI to these entities.

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

1.2 Scope

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

1. Consumer Devices supporting an LPA in the device (LPAd) or LPA in the Consumer eUICC (LPAe).
2. IoT Device supporting an IPA in the IoT Device (IPAd) or IPA in the IoT eUICC (IPAe).
3. Consumer eUICC, with or without an LPA.
4. IoT eUICC, with or without an IPA.
5. SM-DP+ and SM-DS providing a Subscription Management service.
6. eSIM IoT Remote Manager.

1.3 Intended Audience

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

1.4 Definition of Terms

Term	Description
Digital Certificate (Public Key)	As defined in RFC.5280 [9] or GlobalPlatform specifications Identifies its issuing certification authority Names or identifies the subscriber of the certificate Contains the subscriber's public key Identifies its operational period Is digitally signed by the issuing certification authority.
eSIM	As defined in SGP.21 [1].
Consumer Device	Device as defined in SGP.21 [1].
Consumer 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	Consumer or IoT eUICC, Field-Test eUICC, SM-DP+ (Subscription Manager Data Preparation), SM-DS (Subscription Manager Discovery Services), eIM (eSIM IoT Remote Manager) and Consumer or IoT 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
IoT eUICC	As defined in SGP.31 [18].
IoT Device	As defined in SGP.31 [18].
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

1.5 Abbreviations

Abbreviation	Description
eIM	eSIM IoT Remote Manager
eSA	eUICC Security Assurance
EUM	eUICC manufacturer
GCF	Global Certification Forum
GSMA CI	GSMA Certificate Issuer
IMEI	International Mobile Equipment Identity
IoT	Internet of Things
IPA	IoT Profile Assistant
IPAd	IoT Profile Assistant in the Device
IPAe	IoT Profile Assistant in the eUICC
LPA	Local Profile Assistant

Abbreviation	Description
LPAd	Local Profile Assistant in the Device
LPAe	Local Profile Assistant in the eUICC
OS	Operating System
PKI	Public Key Infrastructure
PRD	Permanent Reference Document
PTCRB	PCS Type Certification Review Board
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
TCA	Trusted Connectivity Alliance
TOE	Target of Evaluation
TRE	Tamper Resistant Element

1.6 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
[2]	GSMA PRD SGP.22	eSIM Technical Specification
[3]	GSMA PRD SGP.23	eSIM Test Specification
[4]	GSMA PRD SGP.25	eUICC for Consumer Devices Protection Profile
[5]	GSMA PRD FS.04	Security Accreditation Scheme for UICC Production – Standard
[6]	GSMA PRD FS.08	GSMA SAS Standard for Subscription Manager Roles
[7]	GSMA PRD SGP.14	GSMA eUICC PKI Certificate Policy
[8]	RFC 2119	“Key words for use in RFCs to Indicate Requirement Levels”, S. Bradner http://www.ietf.org/rfc/rfc2119.txt
[9]	RFC 5280	Internet X.509 PKI Certificate and CRL Profile
[10]	GSMA PRD SGP.06	eUICC Security Assurance Principles
[11]	GSMA PRD SGP.07	eUICC Security Assurance Methodology
[12]	Void	Void
[13]	GSMA PRD AA.35	Procedures for Industry Specifications Product
[14]	GSMA PRD SGP.08	Security Evaluation of Integrated eUICC based on PP-0084
[15]	eUICC Profile Package	Trusted Connectivity Alliance (TCA) eUICC Profile Package: Interoperable Format Technical specification

Ref	Document Number	Title
[16]	TCA Test	Trusted Connectivity Alliance (TCA) eUICC Profile Package: Interoperable Format Test Specification
[17]	GSMA PRD SGP.18	Security Evaluation of Integrated eUICC based on PP-0117
[18]	GSMA PRD SGP.31	eSIM IoT Architecture Specification and Requirements
[19]	GSMA PRD SGP.32	eSIM IoT Technical Specification
[20]	GSMA PRD SGP.33-1	eSIM IoT eUICC Test Specification
[21]	GSMA PRD SGP.33-2	eSIM IoT IPA Test Specification
[22]	GSMA PRD SGP.33-3	eSIM IoT eIM Test Specification

1.7 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].

2 Compliance Overview

The GSMA Consumer eSIM architecture PRD, SGP.21 [1] and GSMA eSIM IoT Architecture PRD SGP.31 [18], specifies the high level security and functional requirements for eSIM Product compliance. The eSIM Technical Specification, SGP.22 [2] and GSMA eSIM IoT Technical Specification PRD SGP.32 [19], 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 and IoT eSIM ecosystem. This document provides the framework within which:

- Consumer eUICC, IoT eUICC, SM-DP+ and SM-DS requiring eSIM PKI certificates for eSIM operation can demonstrate the prerequisite functional and security compliance to the Consumer and IoT eSIM requirements.
- An eSIM Consumer Device can demonstrate functional compliance to the Consumer eSIM requirements.
- An eSIM IoT Device can demonstrate functional compliance to the eSIM IoT requirements.
- An eIM can demonstrate functional compliance and attest security compliance according to the eSIM IoT 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.

Field-Test eUICCs requiring PKI certificates chaining to GSMA CI are exempt from compliance declaration and SHALL be operated according to requirements stated in SGP.21 [1] (version 2.4 or higher) or SGP.31 [18]. Compliance requirements applicable to the Field-Test eUICCs are described in this document in section 4.2 table 4.

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.

3 Compliance Declarations Types

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] or GSMA PRD SGP.31 [18] and GSMA PRD SGP.32 [19].
- 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 or A.6 or A.7 or A.8 or A.9 (as applicable): the compliance details of the declared eSIM Consumer or IoT Product or service.

The GSMA turnaround time for issuing a confirmation of compliance declaration, upon final validation of declaration forms, is 2 working days.

Product type	Details of Company and Product Declaration	Details of Product Compliance
Device (LPAd)	Annex A.1	Annex A.2
Consumer eUICC	Annex A.1	Annex A.3
SM-DP+	Annex A.1	Annex A.4
Alt SM-DS	Annex A.1	Annex A.5
eIM	Annex A.1	Annex A.6
Device (IPAd)	Annex A.1	Annex A.7
IoT eUICC	Annex A.1	Annex A.8
Self-Assessment of eUICC Certified products	Annex A.1	Annex A.9
eUICC Fast Track Update	Annex A.1	Annex A.10

Table 1: Compliance declaration templates

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

3.1 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.

3.1.1 New Declarations or Major Update Declarations

For Major update declarations, it is important to indicate in Annex A.1 that the declaration type is *'Major Product Update'*.

A new declaration is to be submitted for new eSIM product or major changes to previously declared eSIM products such as:

eUICC (Consumer/IoT) Products

- IC Platform Changes
- Major version update (e.g: v2.0 to v3.0)
- Software Security Changes (part of the security TOE)
- Addition of optional features of SGP.22/32

The process to follow for new or major update eUICC declarations is to fill and send the latest SGP.24 template (A.1 plus A.3 or A.8) with all the new information in it.

For addition of optional features, new functional testing SHALL be performed on the product using any of the allowed functional testing methods.

GSMA will issue a new or updated confirmation of compliance and a new RSP reference (if listed on GSMA Compliance data base) for the new declaration.

Device (LPAd/IPAd) Products:

- Major version update (e.g: v2.0 to v3.0)
- Changes on GCF/PTCRB certification
- Addition of optional features of SGP.22/32

The process to follow for new or major update Device (LPAd/IPAd) declarations is to fill and send the latest SGP.24 template (A.1 plus A.2 or A.7) with all the new information in it.

For addition of optional features, new functional testing SHALL be performed on the product using any of the allowed functional testing methods.

GSMA will issue a new or updated confirmation of compliance and a new RSP reference (if listed on GSMA Compliance data base) for the new declaration.

SM-DP+, SM-DS or eIM Products:

- Major version update (e.g: v2.0 to v3.0)
- Addition of optional features of SGP.22/32

The process to follow for new or major update SM-DP+, SM-DS or eIM declarations is to fill and send the latest SGP.24 template (A.1 plus A.4 or A.5 or A.6) with all the new information in it.

For addition of optional features, new functional testing SHALL be performed on the product using any of the allowed functional testing methods.

GSMA will issue a new or updated confirmation of compliance and a new RSP reference (if listed on GSMA Compliance data base) for the new declaration.

3.1.2 Minor Update Declarations

For Minor update declarations, it is important to indicate in Annex A.1 that the declaration type is *'Minor Product Update'*.
A minor update declaration is to be submitted for any minor change to eSIM product that impact RSP functionality such as:

eUICC (Consumer/IoT) Products:

- Addition or deletion of a SAS site for the production of the product.
- Minor Version update (e.g: v2.1 to v2.2)
- Removal of optional features of SGP.22/32

For SAS-UP site updates new or deleted SAS-UP certificate SHALL be provided.

In any other case new functional testing SHOULD be performed on the product using any of the allowed functional testing methods.

The process to follow for minor updated eUICC declarations is to fill and send the latest SGP.24 template (A.1 plus A.3 or A.8) reusing the previous information and updating only what is new or updated.

GSMA will issue an updated 'Confirmation of PKI Certificate Issuance' for the updated product and will update the GSMA Compliance data base (if listed) with:

- new updated information
- update date

In the cases detailed in sections 3.1.1 and 3.1.2, 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.

Device (LPAd/IPAd) Products:

- Minor Version support update (e.g: v2.1 to v2.2).
- Removal of optional feature of SGP.22/SGP.32.

For removal of optional features, new functional testing SHOULD be performed on the product using any of the allowed functional testing methods.

The process to follow for minor updated Device (LPAd/IPAd) declarations is to fill and send the latest SGP.24 template (A.1 plus A.2 or A.7) reusing the previous information and updating only what is new or updated.

GSMA will issue an updated ‘Confirmation of Device Compliance’ for the updated product and will update the GSMA Compliance data base (if listed) with:

- new updated information
- update date

In the cases detailed in sections 3.1.1 and 3.1.2, 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.

SM-DP+, SM-DS or eIM Products:

- Minor Version support update (e.g: v2.1 to v2.2).
- Removal of optional feature of SGP.22/SGP.32.

For SAS-SM site updates new or deleted SAS-SM certificate SHALL be provided.
In any other case new functional testing SHOULD be performed on the product using any of the allowed functional testing methods.

The process to follow for minor updated SM-DP+ or SM-DS declarations is to fill and send the latest SGP.24 template (A.1 plus A.4, A.5 or A.6) reusing the previous information and updating only what is new or updated.

GSMA will issue an updated ‘Confirmation of PKI Certificate Issuance’ for the updated product and will update the GSMA Compliance data base (if listed) with:

- new updated information
- update date

In the cases detailed in sections 3.1.1 and 3.1.2, 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.

3.1.3 Self-Assessment of eUICC Certified Products Update Declarations

For Self-Assessment declarations, it is important to indicate in the Annex A.1 declaration that the declaration type is *‘Self-Assessment of eUICC Certified Products Updates’*.

A Self-Assessment is to be submitted for any changes to eUICC (Consumer/IoT) product that do not impact the RSP functionality, SAS processes nor they are part of the security TOE.

The process to follow for Self-Assessment declarations is to fill and send the latest SGP.24 template A.9 Self-Assessment of eUICC Certified products update declaration including:

- List the changes made to the eUICC product
- Indicate the impact on the eUICCs deployed on the field.
- Add reference/report made by the eUICC Manufacturer or third party lab
- Indicate if the change is confidential to GSMA only or to be visible on the GSMA Compliance database.

GSMA will issue a revision of the previously issued ‘Confirmation of PKI Certificate Issuance’ and will update the GSMA Compliance data base (if listed) with:

- new SW version
- update date
- Note to indicate ‘Updated via self-assessment’

3.1.4 Product Withdrawal

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.

The process to follow for a withdrawal of compliance declaration is to complete Annex A.1 indicating the product withdrawal and the reason for it and send it to RSPCompliance@gsma.com with this information.

As a consequence, GSMA will remove the declaration from its GSMA Compliance data base.

3.1.5 eUICC Fast Track Update Declaration

For eUICC Fast Track Update declarations, it is important to indicate in Annex A.1 declaration that the declaration type is ‘eUICC Fast Track Update’.

The eUICC Fast Track Update declaration is to be submitted for any urgent fixes in eUICC products that support an EUM-specific eUICC OS update mechanism.

The eUICC Fast Track Update declarations is intended to allow updates of the eUICC product in order to fix errors or vulnerabilities which are discovered on already deployed Consumer and IoT eUICC Products. This includes scenarios in which the deployment of an update is time critical in order to:

- prevent exploitation of potential security issues of the eUICC;
- or to correct functional issues preventing the expected use of the eUICC.

For this reason, a process for an eUICC Fast Track Update declaration is defined which is intended for cases in which it is not acceptable to wait for the completion of the regular certification processes before deployment of eUICC OS update package, and allow deployments at the same time as submission of the declaration.

An EUM can use the eUICC Fast-Track Update declaration if all of the following conditions are met:

- The target Consumer or IoT eUICC Product has already declared compliance (i.e., the compliance declaration is "active" (NOTE1)) with either SOG-IS Common Criteria or GSMA eSA security evaluation schemes;
- The target Consumer or IoT eUICC Product maintains compliances to the same versions of SGP.21 [1] and SGP.22 [2] or SGP.31 [18] and SGP.32[19] in the updated compliance declaration;

- The updated Consumer or IoT eUICC support the same features (optional and mandatory) as the original Consumer or IoT eUICC, whether the update affects RSP functions then it is subject to GlobalPlatform functional certification; and
- The target eUICC Product either:
  - has been evaluated by the security laboratory and impact assessment report has been issued by the security laboratory (NOTE2) indicating that the updated eUICC product is resistant against high attack potential; or
    - had previously been successfully evaluated by a security laboratory and a new schedule for performing impact assessment with the security laboratory has been confirmed.

NOTE 1: While a Consumer or IoT eUICC is marked as "update ongoing" on the compliance declaration by the GSMA, there cannot be another fast-track certification update.

NOTE 2: Issuing the impact assessment report SHOULD be advised by the certification body in advance. Otherwise, the eUICC Fast-Track Update declaration might fail to provide a certification report, revoking the compliance declaration; see below.

An eUICC Fast Track Update declaration (Annex A.10) indicating fast-track SHALL:

- Be initiated from the EUM by sending the Fast Track Update (Annex A.10) to GSMA
- Be acknowledged by GSMA by:
  - marking the compliance declaration as "update ongoing"; indicating within the GSMA eSIM product database or the GSMA's internal records; and
  - responding a confirmation of the updated compliance status indicating that there is an eUICC update in progress;
- Be followed by an updated compliance declaration from the EUM upon the completion of full security certifications by sending Annexes A.1 and A.3 to GSMA with re-issued certification report references (including impact assessment report, if it was not previously submitted) 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 laboratory. Otherwise GSMA will remove the compliance declaration from its GSMA eSIM Compliance database data by marking it as "expired".

3.1.6 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 Consumer or IoT eUICC product.

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

4 Compliance Requirements

The compliance requirements are derived from the GSMA SGP.21 [1] eSIM Architecture specification and GSMA SGP.31 [18] eSIM IoT Architecture specification. This section details these requirements and their applicability to eSIM product as:

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

4.1 Site Security Requirements

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

To demonstrate site security compliance to SGP.22 [2] or SGP.32 [19], the permitted test methodologies are:

For Consumer or IoT eUICC:

- SAS-UP Certification as indicated in Table 2 below.

For SM-DP+:

- SAS-SM Certification as indicated in Table 2 below.

For SM-DS:

- SAS-SM Certification as indicated in Table 2 below.

For eIM:

- SAS-SM Certification as indicated in Table 2 below.
- Third party security evaluation

Accreditation is from the GSMA Security Accreditation Scheme (SAS). Further details can be found on the GSMA's SAS webpage.

The SAS-UP or SAS-SM certificate reference SHALL be included in the compliance declaration for a Consumer eUICC (annex A.3), SM-DP+ (annex A.4), Alternative SM-DS (annex A.5) or IoT eUICC (Annex A.8). The SAS-SM certificate reference SHALL be included in the compliance declaration for an eIM (annex A.6) only if SAS was used to attest eIM's compliance to the security requirements defined in SGP.31 [18].

Product type	SAS requirement		Compliance requirement
	Scheme	Required Scope	
Consumer or IoT 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
eIM	SAS-SM	• eIM Services	Provisional or Full certification

Table 2: Operational Security Compliance requirements per product type using SAS

In case the chosen method for eIM to demonstrate security compliance is other than SAS-SM, Table 3 below describes what SHALL be included in the compliance declaration for an eIM (annex A.6) to attest eIM's compliance to the security requirements defined in SGP.31 [18].

Product type	Methodology	Compliance Requirement / Proof
eIM	Third party security evaluation	• certificate type • certificate number • certificate expiry date • certificate URL

Table 3 Operational Security Compliance requirements for eIM using other methods

4.1.1 Specific Considerations for Consumer or IoT 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 Consumer or IoT eUICC.

- Details of all manufacturing sites used in the production of the Consumer or IoT 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 Consumer or IoT 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 Consumer or IoT eUICC

- have Management of PKI Certificates within its SAS-UP accreditation scope

4.2 Product Security Requirements (Consumer or IoT eUICCs only)

A protection profile has been developed for Consumer or IoT eUICC software implementing the GSMA eSIM architecture for Consumer Devices [1] and IoT Devices [18].

Note: SGP.25 [4] v1.1 covers GSMA eSIM architecture for Consumer Devices [1] and is registered as a Protection Profile by BSI, reference BSI-CC-PP-0100 and SGP.25 [4] v3.0 covers GSMA eSIM architecture for both Consumer Devices [1] and IoT Devices [18] and is not certified at this stage.

Consumer and IoT 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)

A discrete Consumer or IoT eUICC SHALL use a certified IC platform according to table 4.The Common Criteria certificates or certificate references (www.commoncriteriaportal.org/products) SHALL be included in the declaration as evidence of product security compliance.

Product type	Product Security Requirement	Compliance requirement
Discrete Consumer or IoT 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

Table 4: Product Security Compliance requirements for Discrete Consumer or IoT eUICC

A Field-Test eUICCs SHALL use a certified IC platform according to table 5:

Product type	Product Security Requirement	Compliance requirement
Discrete Field-Test Consumer or IoT 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.

Integrated Field-Test Consumer or IoT 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

Table 5: Secure IC Platform requirements for Field-Test eUICC

An integrated Consumer or IoT eUICC SHALL use a certified TRE according to table 6.

Product type	Product Security Requirement	Compliance requirement
Integrated Consumer or IoT 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

Table 6: Product Security Compliance requirements for Integrated Consumer or IoT eUICC

4.2.1 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 Consumer or IoT 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, A.5 and A.6).
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.

4.2.2 Security Recertification

For eUICC, the impact of the change(s) on the current security certification SHALL be evaluated as per the eSA or CC processes, when product maintenance is performed. An assessment of the eUICC operating system changes would be required to determine if a further security certification is required and eventually its type, e.g. a delta certification, full certification etc.

4.3 Functional Compliance Requirements

Functional compliance is a requirement for all eSIM Products to assure correct operation. The eSIM Consumer Test Specification, SGP.23 [3] and eSIM IoT Test Specifications SGP.33-1 [20], SGP.33-2 [21] and SGP.33-3 [22], provide 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].

Each test in SGP.33-1 [20], SGP.33-2 [21] and SGP.33-3 [22] can be mapped to a specific set of requirements in the eSIM IoT Technical Specification, SGP.32 [19].

To demonstrate product functional compliance to SGP.22 [2] or SGP.32 [19], the permittedtest methodologies are:

- Functional testing via industry partner certification schemes (for Consumer eUICC, IoT eUICC Consumer Devices (LPA) or IoT Device (IPA)),
- Functional testing via vendor implemented test methodologies referencing SGP.23 [3] tests (for SM-DP+ and SM-DS) or SGP.33-3 (for eIM).
- Functional testing using third party test tool referencing SGP.23 [3] test (for SM-DP+ and SM-DS) or SGP.33-3 (for eIM).

4.3.1 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 Consumer eUICCs , IoT eUICC, Consumer Devices (LPA) and IoT Devices (IPA), referencing the SGP.23 [3], SGP.33-1 [20] or SGP.33-2 [21] test requirements.

Consumer eUICC (annex A.3), IoT eUICC (annex A.8), Consumer Devices (annex A.2) and , IoT Device (annex A.7) 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
Consumer Device (LPA)	GCF	GCF Certification including eSIM	GCF
		GCF eSIM Standalone certification	GCF
	PTCRB	PTCRB Certification including eSIM	PTCRB

IoT Device (IPA)	GCF	GCF Certification including eSIM	GCF
		GCF eSIM Standalone certification	
	PTCRB	PTCRB Certification including eSIM	PTCRB
Consumer eUICC	GlobalPlatform	GP Product Functional Certification to: (1) GSMA eUICC Consumer functional test suite (2) TCA Interoperable Profile' test suite (eUICC Profile Package [14])	GlobalPlatform
IoT eUICC	GlobalPlatform,	GP Product Functional Certification to: (1) GSMA eUICC IoT functional test suite (2) TCA Interoperable Profile' test suite (eUICC Profile Package [14])	GlobalPlatform

Table 7: Functional compliance via GSMA industry certification scheme partners

4.3.2 Functional Compliance via Vendor/ Third Party Implemented Test Plan or Third Party Test Tool Permitted

Permitted for Subscription Management products (SM-DP+,SM-DS and eIM). The vendor specified test plans SHALL reference all SM-DP+/SM-DS/eIM tests from the eSIM test specification, SGP.23 [3] or SGP.33-3[22]. Annex A.4 Annex A.5 and Annex A.6 provide further details.

Product type	Vendor specified test plan permitted	Third party test tool permitted	Reference
SM-DP+	Yes	Yes	SGP.23 [3]
Alt SM-DS	Yes	Yes	SGP.23 [3]
eIM	Yes	Yes	SGP.33-3 [22]

Table 8: Functional compliance via Vendor/ Third Party Implemented Test Plan or Third party test tool permitted

4.3.3 Functional Compliance Re-testing

Functional compliance SHALL be re-established following a change of either the eUICC operating system, the LPA/IPA, the SM-DP+ / SM-DS or the eIM. The change MAY be triggered by a bug fix or by an update to fix or mitigate a security vulnerability.

- eUICC

  - For minor eUICC fixes or updates, functional re-testing SHALL be repeated using a 3rd party GlobalPlatform accredited test tool, and the results SHALL be submitted to GSMA. Re-application for GlobalPlatform re-certification is not required.
  - For all other eUICC updates, the GlobalPlatform eUICC functional certification SHALL be repeated and the new GlobalPlatform certificate SHALL be submitted to GSMA.

- LPA/IPA
  - For all LPA/IPA fixes or updates, functional re-testing SHALL be repeated using a 3rd party GCF or PTCRB accredited test tool following the GCF or PTCRB validation process.
- SM-DP+, SM-DS and eIM
  - For all SM-DP+, SM-DS and eIM fixes or updates where the changes are located on the software functional blocks that are related to the RSP functions of the SM-DP+/SM-DS/eIM platform (not on the underlying system components, e.g. OS, VM and database management systems), full functional re-testing SHALL be repeated using one of the methodologies accepted, and the results SHALL be submitted to GSMA.

5 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 (Consumer or IoT)
- 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.

5.1 Specific Considerations for Consumer and IoT 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 Consumer or IoT eUICC product is also allowed to be used with additional Consumer or IoT eUICC product(s). The following provisions apply:

- A new SGP.24 declaration SHALL be submitted for each additional Consumer or IoT 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 Product Functional Certification,
    - 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 Consumer or IoT 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 Consumer or IoT eUICC product.

An issued EUM (PKI) certificate for the initially declared Consumer or IoT 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.

Annex A Declaration Templates

An eSIM Product declaration consists of Annex A.1 plus either Annex A.2, A.3, A.4, A.5, A.6, A.7, A.8, A.9 or A.10 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 (LPAd)
- A.3 Details of Declared Consumer eUICC
- A.4 Details of Declared SM-DP+
- A.5 Details of Declared SM-DS
- A.6 Details of Declared eIM
- A.7 Details of Declared Device (IPAd)
- A.8 Details of Declared IoT eUICC
- A.9 Self-assessment of eUICC Certified product update
- A.10 Details of Declared eUICC Fast Track Update

Annex B VOID

Annex C eSIM Certification Applicability (Normative)

This Annex identifies the current requirements and specification versions for Consumer and IoT eSIM compliance declarations. Refer to the SGP.24 Annex C for this information.

Annex D Document Management

D.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 reuse RSPCERT39 Doc 8r1: Section 3.1 added on compliance maintenance. RSPCERT39 Doc 13r0: Annex C updated RSPCERT42 Doc 7r0: Section 4.2 and A.3 on security assurance (interim methodology) RSPCERT42 Doc 6r1: Annex C update to security assurance RSPCERT42 Doc19r2: editorials RSPCERT43 Doc 8r2: editorials	eSIM Group	Valerie Townsend, GSMA

		RSPCERT43bis Doc 3r1:updates following working group review. eSIMWG4#1 Doc 018: updates to Section 3.1 and A.3.4.2 (option 2)		
V2.3		CR001R002 Addition of eUICC Assurance Scheme Annex A.3 CR004R005 Annex A.4 - Details of SGP.23 testing related to Application Note Issues and check box for revised declaration CR006R001 SGP.24 Introduce GSMA eSA CR007R001 Changes in Annex C	eSIM Group	Gloria Trujillo, GSMA
V2.4	30 June 2021	CR0009R01 Clarification of the SGP.22 V2.2 eSIM Application Note CR0012R01 eUICC Statement of Security Evaluation Completion validity five years CR0013R01 Deadline to commence interim solution evaluations CR0014R01 Add of Integrated eUICC CR0015R00 Evaluation project start and finalisation CR0016R00 Optional SetEditDefaultDpAddr and SetEditNickname CR0017R00 Optional support of downloading PPR to removable eUICC CR0018R02 Change SIMalliance to TCA in SGP.24 CR0019R01 Change SIMalliance to TCA in SGP.24 Annex A.3 CR0020R00 - Fix in Annex C CR0021R02 eUICC Supporting multiple TCA ePP specs	ISAG	Gloria Trujillo, GSMA
V2.4.1	16th December 2021	CR0025R01 - NFC compliance CR0026R00 - Editorial change section 4.2 table 4 CR0027R01 - Alignment of Table C2 with chapter 3.1 CR0029R00 - Removing self-reference in Table C1 CR0023R02 – Interim Security Certification Extension	ISAG	Gloria Trujillo, GSMA
V2.4.2	28th January 2022	CR0034R01 - Add Consumer v2.4 to Annex C CR0028R04 - 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 use CR0032R03 – 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-DS CR0065R02 - Removal of interim methodology in Annex A.3 CR0068R01 - eUICC Category Note V2.4.4 CR0069R00 - Annex A.1, add linkage to other SGP.24 annexes CR0070R00 - Update SGP.08 reference	ISAG	Gloria Trujillo, GSMA
V2.5	28 March	CR0074R01 - Remove application note from Core Spec CR0075R00 - Remove application note from Annex A.4 CR0077R01 - Add reference to SGP.09 CR0079R01 - Add SGP.09 in Annex A.3 CR0080R02 - Add SGP.18 V1.0 reference CR0081R02 - Add SGP.18 V1.0 in Annex A.3 CR0089R01 - Add SGP.21 V2.5 reference CR0084R04 - Fast Track for updated compliance declarations of Euicc CR0085R02 - Add certification expiration CR0091R01 - Product declaration type definiton	ISAG	Gloria Trujillo, GSMA
V2.6	27 January 2025	CR0098R02 – eSIM IoT Changes in section 1 and 2 CR0099R02 – eSIM IoT Changes in section 3, 4, 5 and Annex A CR0100R02 – eSIM IoT Changes - applicability table CR0109R00 – eSIM IoT New Annex A.6 for eIM CR0101R02 - CR Annex A.1 CR0103R04 – eSIM IoT Changes Annex A.3 for product variant and GP section CR0104R01 – CR Annex A.4 CR0105R01 – CR Annex A.5 CR0107R01 – CR Annex A.7 (IPA only) CR0108R02 – CR Annex A.8 (eUICC IoT only)	ISAG	Gloria Trujillo, GSMA

		CR0114R01 – Product Variant clarifications on Core Spec CR0119R01 - Annex A.1 GSMA Database Visibility CR0116R05 - Annex A.7 Optional Features CR0117R05 - Annex A.8 Optional Features CR0118R03 - Annex A.6 Optional Features CR0124R03 - Deletion of Product declaration type from Annex A.3 CR0125R05 - Compliance Maintenance Clarification v2.6 CR0130R01 - New Annex A.9 – Self-Assessment CR0134R00 - Add new SGP.25, SGP.06 and SGP.07 V2.0 CR0136R00 - Change title to Fast Track Update CR0138R01 - Product declaration type in Annex A.1 CR0139R01 - Corrections to Applicability Table for eSIM IoT products CR0150R01 - Security Recertification v2 CR0132R04 - Annex A.4 Updates CR0142R00 - Removal of Product declaration table from Annex A.8 CR0144R01 - Applicability Table Changes in SGP.24 V2.6 CR0146R04 - Further changes on Compliance Declaration type section CR0147R00 - Annex A.1 changes SGP.24 V2.6 CR0148R01 - Clarifying Root SM-DS in SGP.24 v2.6 CR0151R00 - Clarification to compliance processes for field test Euicc CR0152R00 - Clarification to eUICC hardware platform certification requirements CR0159R01 - Add newest version of SGP.08 and SGP.18 into applicability table CR0161R00 - Clarifying SAS-SM declaration for eIM CR0162R01 - Adding declaration of options for Secure Connection - IPA CR0163R01 - Adding declaration of options for Secure Connection - eUICC CR0164R01 - Clarification on eIM security compliance		

		CR0154R01 - Functional_Compliance_Re-testing_v2 CR0165R01 - Add self-assessment in Annex A list at the end of document CR0166R01 - Clarification to compliance processes for field test eUICCs - follow up CR0167R01 - Add optional features for eIM Annex A.6 CR0174R01 - Further changes to Functional Compliance re-testing CR0170R04 - Applicability Table changes CR0178R03 - Fast Track update improvement CR0179R00 - Add eUICC Fast Track in Annex A.1 CR0180R04 - Add Annex A.10 CR0181R01 - Update of Applicability table for integrated Euicc CR0183R01 - Remove GSMA turnaround time CR0186R01 - Small missing change on title CR0184R02 - Mirror CR - Fast Track update improvement for V.26 CR0187R01 - New field on GSMA Certificate Issuer name Annex A.3 CR0189R02 - New field on GSMA Certificate Issuer name Annex A.4 CR0190R02 - New field on GSMA Certificate Issuer name Annex A.5 CR0191R02 - New field on GSMA Certificate Issuer name Annex A.6 CR0192R01 - New field on GSMA Certificate Issuer name Annex A.8 CR0195R01- GlobalPlatform Test Suite Correlation table CR0197R00 - Clarification on eIM/IPA compliance CR0198R01_Clarification on IPAe Certification CR0199R01_Clarification on LPAe Certification CR0201R01_Extract Applicability table from SGP.24 V2.6 core doc CR0202R01_Deletion of Annex C from SGP.24 V2.6 CR0205R01_Remove eIM vendor's assessmer as accepted evidence for eIM from core spec CR0206R00_Remove eIM vendor's assessmer as accepted evidence for eIM from Annex A.6 CR0207R01_Clarification of security evaluation eIM in Annex A.6		

D.2 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.