RSP Compliance Process
Version 2.2
17 September 2019

This is a Non-binding Permanent Reference Document 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 confidential to the Association and 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 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.

Antitrust Notice

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

Table of Contents

1 Introduction

1.1 Overview

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

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

- Functional compliance to GSMA's Consumer RSP 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

RSP compliance is an eligibility pre-requisite for the issuance of the X.509 PKI certificates used in Consumer RSP 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.

1.2 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

1.3 Intended Audience

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

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.
Evidence Documentation	Evidence of product compliance to the requirements detailed within this document.

Term	Description
RSP Product	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.
RSP Product Vendor	The manufacturer or service provider of an RSP Product
Type Allocation Code	Initial eight-digit portion of the 15-digit IMEI used in 3GPP mobile devices

1.5 Abbreviations

Abbreviation	Description
EID	eUICC identifier
eUICC	Embedded UICC
eSIM	General term used to describe GSMA remote SIM provisioning
EUM	eUICC manufacturer
IMEI	International Mobile Equipment Identity
LPA	Local Profile Assistant
PRD	Permanent Reference Document
RSP	Remote SIM Provisioning
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

1.6 References

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

Ref	Document Number	Title
[1]	GSMA PRD SGP.21	RSP Architecture Specification
[2]	GSMA PRD SGP.22	RSP Technical Specification
[3]	GSMA PRD SGP.23	RSP 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

Ref	Document Number	Title
[9]	RFC 5280	Internet X.509 PKI Certificate and CRL Profile

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

Compliance is essential for interoperability within the Consumer RSP network. This document provides the framework within which:

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

3 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 RSP 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

Table 1: Compliance declaration templates

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 RSP features.

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

4 Compliance Requirements

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

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

4.1 Site Security Requirements

All eUICC production sites and all SM-DP+ and SM-DS service sites used in GSMA RSP 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 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

Table 2: Operational Security Compliance requirements per product type

4.1.1 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

4.2 Product Security Requirements (eUICCs only)

A protection profile has been developed for eUICC software implementing the GSMA RSP 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) shall be included in the declaration as evidence of product security compliance.

Product type	Product Security Requirement	Compliance requirement
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 3: Product Security Compliance requirements

4.3 Functional Compliance Requirements

Functional compliance is a requirement for all RSP Products to assure correct operation. The RSP 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 RSP Technical Specification, SGP.22 [2].

To demonstrate product functional compliance to SGP.22 [2], an RSP Product shall successfully pass all tests applicable to its supported RSP 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).

4.3.1 Functional Compliance via Industry Partner Certification Schemes

RSP 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 RSP 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 RSP	GCF
		GCF RSP Standalone certification	GCF
	PTCRB	PTCRB Certification including RSP	PTCRB
eUICC	GlobalPlatform, (including SIMalliance profile packages)	GP Product Qualification to: (1) GSMA eUICC Consumer functional test suite (2) SIMalliance Interoperable Profile' test suite	GlobalPlatform

Table 4: Functional compliance via GSMA industry certification scheme partners

Functional Compliance via Vendor defined test plan

4.3.2 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 RSP 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]

Table 5: Functional compliance via Vendor defined test plan

5 RSP Digital Certificates (PKI)

GSMA RSP 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

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 eUICC certificates

The manufacturer of an SGP.24 compliant eUICC is eligible to request *an EUM certificate* from the GSMA CI. The issued EUM certificate can be used by the eUICC manufacturer to generate subCA certificates, as needed, to facilitate mass production of the declared eUICC.

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 EUM certificate,
- The additional product reusing a certificate shall:
    - Be designed to the same major version of SGP.22 [2] as the initial eUICC,
    - 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.

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 product.

Annex A Declaration Templates

An RSP 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 RSP 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

Annex B VOID

Annex C RSP Certification Applicability Table (Normative)

This Annex identifies the current requirements and specification versions for Consumer RSP 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.

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.

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 RSP Compliance Products	RSPLEN/PSMC	Gloria Trujillo, GSMA
V1.1	30th May 2017	Minor revision to SGP.24 V1.1 RSP 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 RSP 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	Incorporate CRs agreed by RSP CERT	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	eSIM group	Valerie Townsend, GSMA

		RSPCERT42 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)		

D.2 Other Information

Type	Description
Document Owner	Valerie Townsend
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.