M2M Compliance Process
Version 1.3
25 March 2021

This Industry Specification is a Non-binding Permanent Reference Document of the GSMA

Security Classification: Non-confidential

Copyright Notice

Disclaimer

Antitrust Notice

This GSMA Permanent Reference Document (PRD) 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.

Table of Contents

1 Introduction

1.1 Overview

This document describes the framework for a M2M (Machine to Machine) Product to demonstrate and declare compliance with the GSMA M2M embedded SIM Remote Provisioning Architecture and Technical PRDs, SGP.01 [1] and SGP.02 [2].

Specific requirements to declare compliance are described according to the M2M product or service, and include the following:

- Functional compliance to GSMA's M2M embedded SIM Remote Provisioning 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

M2M compliance is an eligibility pre-requisite for the PKI certificates used for M2M authentication. These Digital Certificates are issued by the GSMA Root CI for GSMA M2M compliant embedded UICCs, SM-DP and SM-SR.

This version of SGP.16, including its associated annexes, supersedes previous versions, as detailed in Annex B.

1.2 Scope

The requirements within this document are applicable to the following M2M Products:

1. SM-SR - Subscription Manager Secure Routing
2. SM-DP - Subscription Manager Data Preparation
3. eUICC - Embedded UICC

1.3 Intended Audience

M2M Product Vendors, Telecommunication Service Providers, test and certification bodies, and other industry organisations working in the area of M2M/IoT.

1.4 Definition of Terms

Term	Description
M2M Product	eUICC, SM-SR (Subscription Manager Secure Routing) or SM-DP (Subscription Manager Data Preparation) products intended to be used for M2M.
M2M Product Vendor	The manufacturer or service provider of an M2M Product.

1.5 Abbreviations

Abbreviation	Description
eUICC	Embedded UICC
EUM	eUICC Manufacturer
M2M	Machine to machine
PRD	Permanent Reference Document

Abbreviation	Description
SAS	GSMA Security Accreditation Scheme
SAS-SM	SAS for Subscription Management
SAS-UP	SAS for UICC Production
SM	Subscription Manager
SM-DP	Subscription Manager Data Preparation
SM-SR	Subscription Manager Secure Routing

1.6 References

Please refer to the M2M Certification Applicability table in Annex B of this document to identify the valid versions(s).

Ref	Document Number	Title
[1]	GSMA PRD SGP.01	Embedded SIM Remote Provisioning Architecture
[2]	GSMA PRD SGP.02	Remote Provisioning Architecture for Embedded UICC Technical Specification
[3]	GSMA PRD SGP.11	Remote Provisioning Architecture for Embedded UICC Test Specification
[4]	GSMA PRD SGP.05	Embedded UICC Protection Profile
[5]	RFC 2119	"Key words for use in RFCs to Indicate Requirement Levels", S. Bradner http://www.ietf.org/rfc/rfc2119.txt
[6]	RFC 5280	Internet X.509 PKI Certificate and CRL Profile
[7]	FS.08	GSMA SAS Standard for Subscription Manager Roles
[8]	FS.04	Security Accreditation Scheme for UICC Production – Standard
[9]	GSMA PRD SGP.14	GSMA eUICC PKI Certificate Policy
[10]	GSMA PRD AA.35	Procedures for Industry Specifications Product
[11]	GSMA PRD SGP.06	eUICC Security Assurance Principles
[12]	GSMA PRD SGP.07	eUICC Security Assurance Methodology
[13]	GSMA PRD SGP.08	Security Evaluation of Integrated eUICC
[14]	RFC 8174	Ambiguity of Uppercase vs Lowercase in RFC 2119 Key Words https://www.rfc-editor.org/info/rfc8174

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 RFC 2119 [5] and clarified by RFC8174 [14], when, and only when, they appear in all capitals, as shown here.

2 Compliance Overview

The M2M architecture PRD, SGP.01 [1], specifies security and functional requirements for M2M Products, developed into a technical description by SGP.02 [2]. The technical

references for the compliance requirements, split into “Site Security Requirements”, “Product Security Requirements” and “Functional Compliance Requirements” are listed in Annex B of this document.

Annex B identifies all current requirements and specification versions, and should be referenced when planning product compliance.

Product compliance is essential in proving correct functional interoperability as well as product security within the M2M network. This document provides the framework within which:

- An eUICC, SM-DP or SM-SR can demonstrate functional and security compliance to SGP.01 [1] and SGP.02 [2].

Annex A provides declaration templates to be used by M2M Product Vendors.

3 Compliance Declarations

3.1 Compliance declaration definition

A compliance declaration is an indication of:

- the initial compliance of the product, at the time of declaration,
- the compliance maintenance of the product, including any hardware or software updates affecting remote provisioning features.

3.2 Process for compliance declaration

The compliance declaration templates for M2M Products are detailed in Annex A of this document. A compliance declaration can be made once all compliance requirements have been met, and shall be comprised of:

- A completed template Annex A.1, the M2M Product declaration, which also provides details of the organisation responsible for the declaration,
- A completed template Annex A.2 or A.3 or A.4 providing full compliance details of the declared M2M Product.

Once completed in full, the signed and dated compliance declaration shall be submitted to M2MCompliance@gsma.com for verification.

The declaration will be verified to check that the product has demonstrated compliance using the applicable version of SGP.16 (i.e. the initial or latest version) according to the reason for declaration (see section 3.3 and 3.4).

The GSMA turnaround time for verifying compliance is 2 working days.

Product type	Product Declaration	Details of Security Compliance	Details of Functional Compliance
eUICC	Annex A.1	Annex A.2	Annex A.2
SM-DP	Annex A.1	Annex A.3	Annex A.3
SM-SR	Annex A.1	Annex A.4	Annex A.4

Table 1: M2M Compliance declaration templates

3.3 Initial compliance declaration

A new declaration (i.e. latest SGP.16 template) is to be submitted for the initial compliance declaration of a new product.

3.4 Compliance Maintenance

An updated declaration (i.e. update of the initial SGP.16 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.
- Any change of the product, which affects the existing remote provisioning features (e.g. changes that may affect the result of a functional test as defined in SGP.11 [3] or changes that may affect the security certification according to SGP.05 [4]).

3.5 Rules for declaration of urgent updates deployed with eUICC OS Update

Updates to the eUICC OS in the field are permitted, in accordance with the SGP.01 V4 [1] eUICC OS update mechanism. This functionality is intended to enable updates of the eUICC product in order to fix errors in existing features, which are discovered on already deployed 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 emergency 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 the update with OS Update. This emergency update declaration process is sketched in Annex C and comprises the following steps after detection of an issue:

- impact analysis with assessment of the criticality and urgency (out of scope of this specification): this step is under the responsibility of the declaring organisation.
- notification to GSMA compliance secretariat that an urgent update will be deployed by sending a completed and signed template A.5 to the GSMA compliance secretariat;
- updated compliance declaration after completion of the compliance certifications by sending a completed and signed template A.1 and A.2 to the GSMA compliance secretariat.

On receipt of a notification of an urgent update GSMA, will:

- add a flag to the product on GSMA's internal records,
- add a flag on the GSMA compliant product list indicating that an OS update process is in progress, and
- send an acknowledgement with a unique reference number.

On receipt of the compliance declaration update GSMA will:

- clear the flag set previously on GSMA's internal records,

- add a flag on the GSMA compliant product list indicating that the OS update was verified, and
- send an updated compliance confirmation to the declaring organisation.

3.6 Declaration of discontinuation of compliance

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 flag the declaration as “withdrawn”, on its compliant product list.

4 Compliance Requirements

This section details the M2M compliance requirements and their applicability to M2M Products.

4.1 Site Security Requirements

All eUICC production sites and all SM-DP and SM-SR hosting sites in the M2M ecosystem must hold a valid site security accreditation for the entire time they are being used for eUICC production or SM hosting.

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

The SAS-UP [8] or SAS-SM [7] certificate reference shall be included in the compliance declaration for an eUICC, SM-DP and SM-SR as appropriate (Annexes A.2, A.3 and A.4).

Product type	SAS requirement		Compliance requirement
	Scheme	Required Scope	
eUICC	SAS-UP	• Processing of data for subscription management • eUICC personalisation	Full or Provisional certification
SM-DP	SAS-SM	• Data Centre Operations & Management • Data Preparation	Full or Provisional certification
SM-SR	SAS-SM	• Data Centre Operations & Management • Secure Routing	Full or Provisional certification

Table 2: Operational Security Compliance requirements per M2M product type

4.2 Product Security Requirements (eUICCs only)

A protection profile has been developed for eUICC software implementing the GSMA Embedded SIM Remote Provisioning architecture for M2M. The protection profile is published as GSMA PRD SGP.05[4], and registered as a Protection Profile by BSI, reference BSI-CC-PP-0089.

eUICC security evaluations are expected to include:

- the complete Target of Evaluation defined in SGP.05
- the secure IC platform and OS
- the runtime environment (for example Java card system)

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

The Common Criteria certificate 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 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 or certificate attached.
	Security evaluation reflecting the security objectives defined in SGP.05[4], with resistance against high level attack potential. See Annex A.2 for permitted methodologies. Testing to be performed at a SOG-IS lab, accredited in the *Smartcards & similar devices* technical domain.	Refer to Annex A.2, section A.2.5.2

Table 3: M2M Product Security Compliance requirements for Discrete eUICC

Product type	Product Security Requirement	Compliance requirement
Integrated eUICC	Integrated TRE certified following SGP.08 [17] methodology Note: the applicability period of SGP.08 [13] is defined in Annex B.	Common Criteria certified and listed or scan or certificate attached.
	Security evaluation reflecting the security objectives defined in SGP.05[7], with resistance against high level attack potential. See Annex A.2 for permitted methodologies. Testing to be performed at a SOG-IS lab, accredited in the *Smartcards & similar devices* technical domain.	Refer to Annex A.2, section A.2.4.2

Table 4: M2M Product Security Compliance requirements for Integrated eUICC

4.3 Functional Compliance Requirements

Functional compliance is a requirement for all M2M Products to assure correct operation. The M2M Test Specification, SGP.11 [3], provides details of all applicable interface and procedural testing.

Each test in SGP.11 [3] can be mapped to a specific set of requirements in the M2M Technical Specification, SGP.02 [2].

To demonstrate product functional compliance to SGP.02 [2], a M2M Product shall successfully pass all applicable tests as per the selected functional options.

The permitted product dependent test methodologies are either:

- Functional testing via industry partner certification schemes (in the case of eUICC products), or
- Functional testing via vendor or third party implemented test methodologies referencing SGP.11 [3] tests (in the case of SM-SR and SM-DP only).

4.3.1 Functional Compliance via Industry Partner Certification Schemes

A M2M compliance test programme for eUICC M2M Products has been established by GlobalPlatform. This programme covers the SGP.11 [3] test requirements and provides the means to test eUICCs according to these requirements.

eUICCs are judged to have met the M2M functional compliance requirement if:

- They can include a valid certification reference for the named M2M Product in their Annex A.2 declaration.

Product	Functional test organisation	Compliance requirement (see Annex B for details)	Link to industry certification scheme
eUICC	GlobalPlatform, (including SIMalliance profile packages)	GP Product Qualification to: • 'GSMA eUICC M2M' functional test suite • 'SIMalliance Interoperable Profile' test suite	GlobalPlatform

Table 5: M2M Functional compliance via GSMA industry certification scheme partners

4.3.2 Functional Compliance via Vendor or Third Party Implemented Test Plan

Permitted for subscription management products (SM-DP and SM-SR) only. The M2M Vendor specified test plans shall reference all SM-DP/SM-SR tests from the M2M test specification, SGP.11 [3]. Annexes A.3 and A.4 provide further details.

Product type	Vendor or third party specified test plan permitted	Reference
SM-DP	Yes	SGP.11

SM-SR	Yes	SGP.11

5 M2M Digital Certificates (PKI)

The GSMA embedded SIM remote provisioning architecture uses a Public Key Infrastructure (PKI) Digital Certificate to authenticate the following eSIM system entities that have been confirmed as SGP.16 compliant:

- M2M embedded SIM
- SM-DP
- SM-SR

Digital Certificates are issued and managed in accordance with GSMA's PKI Certificate Policy, SGP.14 [9]. Digital Certificate issuance to SGP.16 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.16 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 eUICC certificates, as needed, for 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.16 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.02 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.16 Annex B),
    - Be manufactured at a SAS accredited site,

A new/updated SGP.16 declaration shall be submitted for any change of SAS site(s) intended to be used to manufacture of a declared product.

Annex A M2M Declaration Templates

An M2M Product declaration consists of a completed template Annex A.1 plus a completed template from either Annex A.2, A.3 or A.4, according to the product type.

In case of an urgent update of an eSIM product a completed notification consisting of template Annex A.2 and A.5 needs to be sent to GSMA compliance secretariat. Refer to the SGP.16 zip file for the following Annex A templates:

- *A.1 M2M Product Declaration*
- *A.2 Details of Declared eUICC*
- *A.3 Details of Declared SM-DP*
- *A.4 Details of Declared SM-SR*
- *A.5 Notification of urgent eUICC Update*

Annex B M2M Certification Applicability (Normative)

This Annex identifies the status for compliance declarations of all M2M specifications and associated processes dependencies (active, planned, expired or deprecated) including:

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

M2M Vendors and service providers/hosts are invited to use this table as reference when planning product compliance.

This following table identifies all requirements and dependencies for M2M Compliance, including the current valid specification versions for declarations. It is recommended to review the dates in this table when planning an SGP.16 product compliance.

	Reference	Version	Product Applicability	Status for compliance	Active from	Expiry Date	Note
GSMA PRDs	**M2M Early Adopter Process**	~	All	Expired	April 2018	2019-07-24	
	GSMA PRD SGP.16 M2M Compliance Process	1.0	All	Expired	2018-07-25	2019-09-17	
		1.1	All	Expired	2019-09-17	2020-06-12	
		1.2 (this version)	All	Active	2020-06-12		
	GSMA PRD SGP.11	2.0	All	Expired	2015-11-02	2018-07-31	

	Remote Provisioning Architecture for Embedded UICC Test Specification	3.1	All	Expired	2016-05-31	2018-07-31	
		3.2	All	Expired	2017-06-27	2018-07-31	
		3.3 and later	All	Active	2018-07-31		
		4.0	All	Expired	2019-05-20	2020-06-12	
		4.2.1	All	Active	2020-10-13		
	GSMA PRD SGP.02 Remote Provisioning Architecture for Embedded UICC Technical Specification	2.1	All	Expired	2015-11-02	2019-07-24	
		3.1	All	Deprecated	2016-05-27	2021-03-31	
		3.2	All	Active	2017-06-27	-	
		4.0	All	Expired	2019-02-25	2020-05-14	
		4.2	All	Active	2020-07-07		
	GSMA PRD SGP.01 Embedded SIM Remote Provisioning Architecture	1.1	All	Active	2014-01-30		
		4.0	All	Expired	2019-02-25	2020-05-14	
		4.2	All	Active	2020-07-07		
	BSI-CC-PP-0084-2014	1.0	eUICC	Active	2017-10-16		

Security Compliance requirements	Security IC Platform Protection Profile with Augmentation Packages Certification (PP-0084).						
	BSI-CC-PP-0035 Security IC Protection Profile (PP-0035)	1.0	eUICC	Active	2007-06-15		
	GSMA PRD SGP.05 (BSI-CC-PP-0089-2014) Embedded UICC Protection Profile	1.1	eUICC	Active	2015-08-15		
	SGP.16 Annex A.2 section A.2.5.2(b), option 2: Interim methodology – implementation focused security evaluation		eUICC	Active	2019-07-24	**Existing product in the field**: no expiration if used for the initial security evaluation **Existing product variant**: 2022-07-31 **New product**: 2022-01-31 (1) and (2)	See Table B.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	eUICC	Active	2017-03-31		
	GSMA PRD FS.08 SAS for SM roles	Refer to GSMA.com/SAS	SM-DP & SM-SR	Active	2017-03-31		
	GSMA PRD SGP.08 Security Evaluation of Integrated eUICC	1.0	Integrated eUICC	Active	2021-03-01	24 months after publication	Has to be reviewed by 12 months after the publication of the current document. During said review, the Expiry date and its extension will be discussed and accordingly updated. NOTE: The interim methodology defined in SGP.08 [13] can be discontinued before the expiry date if a protection profile for Integrated TRE is adopted by the GSMA.

Functional Compliance requirements	**GlobalPlatform test suite** GP Test Suites: eUICC M2M Compliance Test Suite eUICC M2M - SIMalliance Interoperable Profile Test Suite	'Refer to GP for applicable version(s)	eUICC	Active	2018-07-25		
	Vendor specified Functional test	n.a	SM-DP & SM-SR	Active	2018-07-27		
Permitted Exceptions	**Permitted Exceptions agreed for SGP.16 declarations**	SGP.01 V1.1 requirement PRO12 does not apply in the case where activation of emergency profiles for emergency calling is required by regulation.			2019-04-04		

(1) A SOGIS Laboratory will only accept new eUICC evaluation projects for Interim Methodology until 2021-11-30 (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 2022-01-31. GSMA will accept late entrance of New product until 2022-04-30 for New products that can demonstrate that the evaluation project started before 2021-11-30.

(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 B.2 Product Type Validity Period of '*Interim methodology*'

Product Types	Description	Security Assurance Scheme Allowed	Re-Certification Trigger

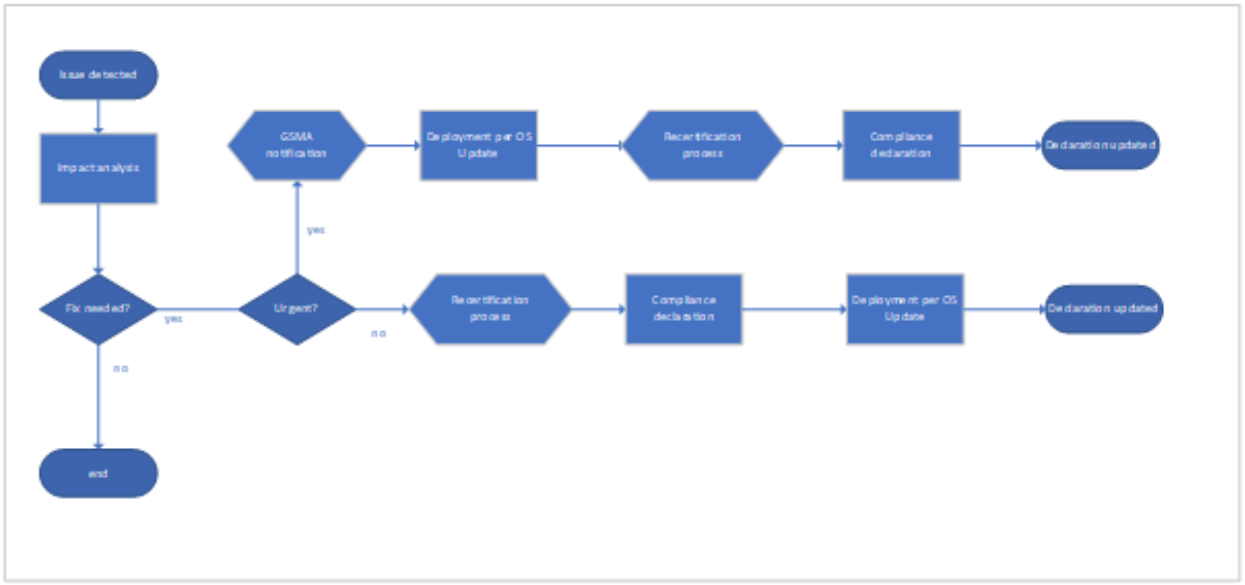
Existing product in the field	An eSIM product that is produced and ready to be inserted in a device or is inserted in a device which is being used by an end customer or which is in the supply chain from the factory of the device OEM to a store	Throughout the life cycle of an Existing product in the field: • 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: ▪ Updates for eSIM functional and/or eSIM security issues within the initial scope deployed using the eUICC OS Update as defined in SGP.02 (see statement below) and as referenced in SGP.16 Section 3.5. *SGP.02: 'An eUICC should support a secure mechanism to allow the eUICC OS Update when the eUICC is in the field. Such mechanism allows the eUICC Manufacturer to correct errors in existing features on the eUICC*'.
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, for 24 months starting July 2020 and until July 2022, 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.01/02 and IPP specifications e.g. o M2M (SGP.02) v3.1 to 3.2 , or o SIMalliance IPP v2.2 to v2.3.1. ▪ IC maintenance release of the same IC even if SOG-IS CC certificate is changed or updated. ▪ Non-GSMA related OS modification (example: MNO specific features , telco part updates; optimisation and general enhancements).
New product	Any eSIM product with a new IC platform, a new major version of SGP.01/02 spec or new major version	For the certification of a New product: • Interim methodology can be , for 18 months starting July 2020 and until January 2022, after which only the eSA scheme or SOG-IS CC scheme will be allowed.	Situations in which a certification as a New product is required : ▪ Change of the IC platform (new IC type/vendor, new technology).

	of the profile package specification	• eSA scheme; • SOG-IS CC scheme;	▪ Support for major updates versions of SGP.01/02 specification, e.g. SGP.02 v**3**.2 to v**4**.1. ▪ Support for major updates versions of the SIMalliance IPP specification e.g. v**2**.1 to v**3**.x

Table B.3 : Status for Compliance

Status for Compliance	Description
Active:	Specification or reference that is currently valid for SGP.16 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.16 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.16 declaration.
Expiry date:	The last date on which an SGP.16 declaration can reference the specification or reference. Declarations using an expired specification or reference will not be accepted.

Annex C Process for declaration updates (informative)



Annex D Document Management

D.1 Document History

Version	Date	Brief Description of Change	Approval Authority	Editor / Company
V1.0	25th Jul 2018	Initial version of SGP.16 V1.0 M2M Compliance Products	SIM Group/TG	Gloria Trujillo, GSMA
V1.1	29th May 2019	Updated to include the following CRs:	eSIM Group	Valerie Townsend, GSMA

		RSPCERT41 Doc 007r3 (adding permitted exception to Annex B) RSPCERT41 Doc 008r1 (General updates and editorials) RSPCERT42 Doc 008r1 (additional (interim) methodology option for eUICC assurance) RSPCERT43 Doc 007r1 (Annex B update for (interim) method option for eUICC assurance) RSPCERT43 Doc 016r0 (Annex A.1: identifying PKI certificate holder) RSPCERT43 Doc 017r1 (Annex A.2: adding details of PKI certificate reuse) RSPCERT43 Doc 018r3 (section 1 editorials, sections 3.1 and 5 added. RSPCERT43 Doc 9r2 editorials RSPCERT43bis Doc 2r1: updates following working group review.		

		eSIMWG4#1 Doc 017: updates to Section 3.1 and A.2.5.2 (option 2)		
V.1.2		CR001R000 Changes to certification and OS update CR003R001 SGP.16 Annex B - expiry dates for the interim process transition period CR004R001 Addition of eUICC Assurance Scheme Annex A.3 CR005R001 Section 3.5: refer to the definition of eUICC OS update in SGP.01 CR006R001 Annex A.2: Addition of a field to refer to a previous declaration in case of an update of a declaration CR007R004 Addition of Annex A.5 for urgent update notification CR008R000 SGP.16 annex A.2 Java Card CR009R001 Additional Changes to Annex B	eSIM Group	Gloria Trujillo, GSMA
V1.3	25th March 2021	CR0010R04 - SGP.16 annex A.2 Integrated eUICC CR0017R00 - Addition of integrated eUICC to SGP.16 CR0018R01 - Deadline to commence interim solution evaluations	ISAG	Gloria Trujillo, GSMA

		CR0019R00 - Evaluation project start and finalisation		

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.