SGP.16 M2M Compliance Process
Version 1.5
27 January 2025

Security Classification: Non-confidential

Copyright Notice

Disclaimer

Compliance Notice

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

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

Contents

1.1 Overview 3
1.2 Scope 3
1.3 Intended Audience 3
1.4 Definition of Terms 3
1.5 Abbreviations 3
1.6 References 4
1.7 Conventions 4
2 Compliance Overview 5
3 Compliance Declarations Types 5
3.1 Compliance Maintenance 6
3.1.1 New Declaration or Major Update Declarations 6
3.1.2 Minor Update Declarations 7
3.1.3 Self-Assessment of eUICC Certified Products Update Declarations 8
3.1.4 Product Withdrawal 8
3.1.5 eUICC Fast Track Update Declaration 8
3.1.6 eUICC Compliance Expiration 10
4 Compliance Requirements 10
4.1 Site Security Requirements 10
4.1.1 Lapse of Compliance 11
4.1.2 Specific Considerations for eUICC 11
4.1.3 Security Recertification 11
4.2 Product Security Requirements (eUICCs only) 12
4.3 Functional Compliance Requirements 13
4.3.1 Functional Compliance via Industry Partner Certification Schemes 13
4.3.2 Functional Compliance via Vendor/ Third Party Implemented Test Plan or Third Party Test Tool Permitted 14
4.3.3 Functional Compliance Re-testing 14
5 M2M Digital Certificates (PKI) 15
5.1 Specific considerations for eUICC certificates 15
Annex A M2M Declaration Templates 16
Annex B M2M Certification Applicability (Normative) 16
Annex C Process for declaration updates (informative) 17
Annex D Document Management 17
D.1 Document History 17
D.2 Other Information 21

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.
Field-Test eUICC	A pre-production eUICC whose functional or security certifications are not yet completed by the EUM.

1.5 Abbreviations

Abbreviation	Description
eUICC	Embedded UICC
EUM	eUICC Manufacturer

Abbreviation	Description
M2M	Machine to machine
PRD	Permanent Reference Document
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 based on PP-0084
[14]	RFC 8174	Ambiguity of Uppercase vs Lowercase in RFC 2119 Key Words https://www.rfc-editor.org/info/rfc8174
[15]	GSMA PRD SGP.18	Security Evaluation of Integrated eUICC based on PP-0117

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 ecosystem. 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.

Field-Test eUICC requiring PKI certificates chaining to GSMA CI are exempt from compliance declaration and SHALL be operated according to requirements stated in SGP.01 [1] (Version 4.3 or higher). Compliance requirements applicable to these Field-Test eUICCs are described in this document in section 4.2 table 5.

3 Compliance Declarations Types

To declare compliance with SGP.16, the product SHALL:

- Be compliant with the technical requirements defined in the GSMA PRD SGP.01 [1] and GSMA PRD SGP.02 [2].
- Have demonstrated its compliance using the means described in SGP.16, and its Annex A.

The compliance declaration templates for M2M Products are detailed in Annex A of this document and SHALL be submitted to M2MCompliance@gsma.com for verification once all compliance requirements have been met. The compliance declaration comprised:

- Completed template Annex A.1, the M2M 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 (as applicable) : the compliance details of the declared eSIM M2M 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
eUICC	Annex A.1	Annex A.2
SM-DP	Annex A.1	Annex A.3
SM-SR	Annex A.1	Annex A.4
eUICC Fast Track Update	Annex A.1	Annex A.5

Self-Assessment of eUICC Certified products	NA	Annex A.6

Table 1 M2M 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 remote provisioning features.

3.1.1 New Declaration 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 (M2M) Products

- IC Platform Changes
- Major version update (e.g: v1.0 to v2.0)
- Software Security Changes (part of the security TOE)
- Addition of optional features of SGP.02

The process to follow for new or major update eUICC declarations is to fill and send the latest SGP.16 template (A.1 plus A.2) 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 M2M reference (if listed on GSMA Compliance data base) for the new declaration.

SM-DP or SM-SR Products:

- Major version update (e.g: v1.0 to v2.0)
- Addition of optional features of SGP.02

The process to follow for new or major update SM-DP or SM-SR declarations is to fill and send the latest SGP.16 template (A.1 plus A.3 or A.4) 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 M2M 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 M2M product that impact M2M functionality such as:

eUICC (M2M) 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.02

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.16 template (A.1 plus A.2) 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.16 (i.e. the initial or latest version) according to the reason for compliance maintenance.

SM-DP or SM-SR Products:

- Minor Version support update (e.g: v2.1 to v2.2).
- Removal of optional feature of SGP.02.

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-SR declarations is to fill and send the latest SGP.16 template (A.1 plus A.3 or A.4) 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.16 (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 (M2M) product that do not impact the M2M 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.16 template A.6 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 M2MCompliance@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 the 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 M2M 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 M2M eUICC;
- or to correct functional issues preventing the expected use of the M2M 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 M2M 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 M2M eUICC product maintains compliances to the same versions of SGP.01 [1] and SGP.02 [2] in the updated compliance declaration;
- The updated M2M eUICC support the same features (optional and mandatory) as the original M2M 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 M2M 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 indicating Fast Track (Annex A.5) SHALL:

- Be initiated from the EUM by sending the Fast Track Update (Annex A.5) 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.2 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 eUICC product.

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

4 Compliance Requirements

The compliance requirements are derived from the GSMA SGP.01 [1] eSIM Architecture specification. This section details these requirements and their applicability to M2M Products as:

- Site security requirements for M2M eUICC production sites and Subscription Management service sites,
- Product security requirements (M2M eUICC only),
- Functional requirements, including interoperability.

4.1 Site Security Requirements

All eUICC production sites and all SM-DP and SM-SR hosting sites used in the GSMA M2M ecosystem must hold a valid site security accreditation for the entire time they are being used for eUICC production or Subscription Management 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 (Annex A.2), SM-DP and SM-SR as appropriate (Annexes A.3 and A.4).

Product type	SAS requirement		Compliance requirement
	Scheme	Required Scope	
eUICC	SAS-UP	• Management of PKI certificates • Generation of data for 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

4.1.1 Lapse of Compliance

In case of any lapses of M2M compliance as a consequence of a lapse in any individual SAS-UP or SAS-SM certification at eUICC production sites, SM-DP or SM-SR services sites used in GSMA eSIM, the following provisions SHALL apply:

1. The GSMA M2M Compliance Team SHALL notify the above loss of SAS certification to all the stakeholders using the listed sites in their M2M Product declarations (see. Annexes A.2, A.3 and A.4).
2. If all the SAS certifications used by a declared M2M Product lapse, the GSMA M2M Compliance Team SHALL notify this loss of compliance to relevant stakeholders (primarily participants in the eSIM PKI ecosystem) via the GSMA M2M 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 M2M Compliance Team in order to regain M2M compliant status. Resubmission of other declaration templates required by this PRD to gain initial M2M compliance is normally not needed unless the information in those declarations has changed.

4.1.2 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.2 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

4.1.3 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.

4.2 Product Security Requirements (eUICCs only)

A protection profile has been developed for eUICC software implementing the GSMA Embedded SIM Remote Provisioning architecture for M2M

Note: SGP.05 [4] v1.1 covers GSMA eSIM architecture for M2M [1] and is 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)

A discrete M2M eUICC SHALL use a certified IC platform according to table 3.

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 of 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

An integrated M2M eUICC SHALL use a certified TRE according to table 4.

Product type	Product Security Requirement	Compliance requirement
Integrated eUICC	Integrated TRE certified following SGP.08 [13] methodology or SGP.18 [15] methodology. Note: the applicability period of SGP.08 [13] and SGP.18 are defined in Annex B.	Certification Report
	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

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

Product type	Product Security Requirement	Compliance requirement
Discrete Field-Test eUICC	Security IC Platform Protection Profile with Augmentation Package Certification (PP-0084) or Security IC Platform Protection Profile, Version 1.0 (PP-0035)	Common Criteria certified and listed, or scan of certificate attached.
Integrated Field-Test eUICC	Integrated TRE certified following SGP.08 [13] methodology or SGP.18 [15] methodology. NOTE: the applicability period of SGP.08 [13] and SGP.18[15] are defined in Annex B.	Certification Report

Table 5: Secure IC Platform requirements for Field-Test 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 tests.

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], the permitted test methodologies are:

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

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 referencing the SGP.11 [3] test requirements.

eUICCs (Annex A.2) are judged to have met the M2M functional compliance requirement if they have a valid, M2M eUICC certification reference from GlobalPlatform.

Product	Functional test organisation	Compliance requirement (see Annex B for details)	Link to industry certification scheme
eUICC	GlobalPlatform	GP Product Functional Certification to: • 'GSMA eUICC M2M' functional test suite • 'TCA Interoperable Profile' test suite	GlobalPlatform

Table 6: M2M 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 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/Third Party Implemented Test Plan	Third Party Test Tool Permitted	Reference
SM-DP	Yes	Yes	SGP.11
SM-SR	Yes	Yes	SGP.11

Table 7: M2M 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 SM-DP and SM-SR. 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.
- SM-DP, SM-SR
  - For all SM-DP and SM-SR 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-SR 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 M2M Digital Certificates (PKI)

The GSMA eSIM 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 eUICC
- SM-DP
- SM-SR

The EUM CA Certificate from the GSMA CI MAY also be used for a Field-Test eUICC which is considered as SGP.16 compliant for the purpose of certificate use if it is operated according to the requirements set for Field-Test eUICCs in SGP.01 [1] (version 4.3 or higher) and SGP.02 [2] (version 4.3 or higher).

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 Authority Certificate* from the GSMA CI. The issued EUM CA certificate can be used by the eUICC manufacturer to generate eUICC certificates, as needed.

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

- A new SGP.16 declaration SHALL be submitted for each additional eUICC product intending to re-use an existing EUM CA Certificate,
- The additional product reusing An existing EUM CA Certificate SHALL:
    - Have its own evidence of GlobalPlatform 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.16 Annex B),
    - Be manufactured at a SAS accredited site,

Different EUM CA Certificates MAY be requested for the same eUICC product. 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.

An issued EUM (PKI) certificate for the initially declared eUICC product is also allowed to be used with additional Field-Test eUICC product(s). In this case the provisions set in SGP.01 [1] (version 4.3 or higher) and SGP.02 [2] (version 4.3 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 M2M Declaration Templates

An M2M eSIM Product declaration consists of Annex A.1 plus either Annex A.2, A.3, A.4 or A.5, or A.6 according to the product type.

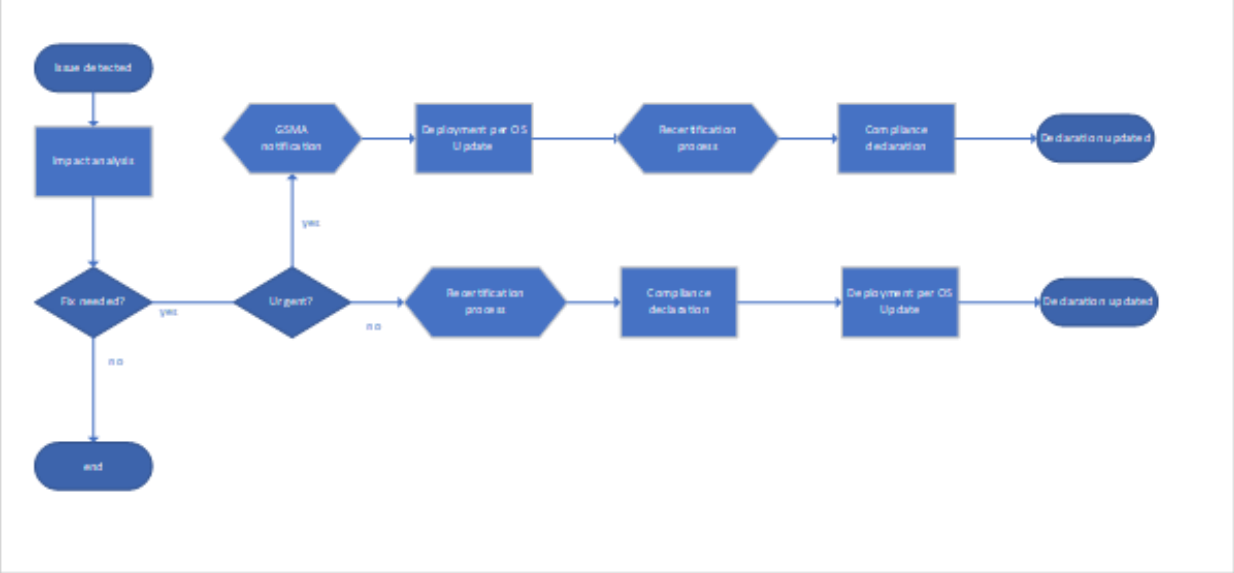
Refer to the SGP.16 zip file for the following Annex A templates:

- *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 Details of Declared eUICC Fast Track Update*
- *A.6 Self-assessment of eUICC Certified Product 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). *Refer to the SGP.24 Annex B file for this information.*

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: 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)	eSIM Group	Valerie Townsend, GSMA

		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	24th 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		
V1.3.1	28th January 2022	CR0020R00 - Editorial change section 4.2 table 4 CR0021R02 - Interim security certification extension CR0022R00 - Removing self-reference in Table B.1	eSIMWG4	Gloria Trujillo, GSMA
V1.3.2 Draft 1	7th March 2022	CR0024R02 – Add flexibility on EUM PKI Certificate use	eSIMWG4	Gloria Trujillo, GSMA
V1.3.2 Draft 2	1st April 2022	CR0023R05 – Lapse of Compliance	eSIMWG4	Gloria Trujillo, GSMA
V1.3.3	8 August 2022	CR0025R00 – SGP.16 annex A.3 include Updates for SM-DP CR0026R00 – SGP.16 annex A.4 include Updates for SM-SR CR0028R01 - Bug fixing related to dates CR0029R01 – SAS-UP subsequent update v1.3.3 CR0030R01 – SAS-SM subsequent update v1.3.3- SM-DP CR0031R01 - SAS-SM subsequent update v1.3.3- SM-SR CR0032R01 – Removal of interim methodology in Annex A.2 CR0033R01 – Update SGP.08 reference	ISAG	Gloria Trujillo, GSMA

SGP.16 v1.4	04 April 2023	CR0034R01 – Add reference to SGP.09 CR0035R01 – Add SGP.09 in Annex A.2 CR0036R01 - Update SGP.05 V4.0 CR0037R02 – Add SGP.18 V1.0 reference CR0038R02 – Add SGP.18 V1.0 reference in Annex A.2 CR0040R01 - Add SGP.01 V4.3 reference CR0041R03 - Product declaration type definiton CR0042 - Add SGP.02 V4.3 reference CR0043 - Add certification expiration CR0044 - Remove term infocentre from Annex A.2 CR0045 - Remove term infocentre from Annex A.3 CR0046 - Remove term infocentre from Annex A.4 CR0047 - Remove term infocentre from Annex A.5	ISAG	Gloria Trujillo, GSMA
SGP.16 v1.5	27 January 2025	CR0048R01 - GlobalPlatform Terminology Changes CR0049R02 - Product Variant clarifications on Core Spec CR0051R03 - Compliance Maintenance Clarification v1.5 CR0052R03 - Annex A.1 GSMA Database Visibility CR0054R02 - New Annex A.6 – Self-Assessment CR0058R01 - Section 4.2 alignment with SGP.24 CR0160R01 - Add newest version of SGP.08 and SGP.18 into applicability table CR0055R00 - Annex A.2 changes for aligment with SGP.24	ISAG	Gloria Trujillo, GSMA

		CR0056R01 - Annex A.3 changes for aligment with SGP.24 CR0057R01 - Annex A.4 changes for aligment with SGP.24 CR0059R01 - New Security Recertification section CR0061R01 - Add self-assesment in Annex A list at end of document CR0062R01 - Update Applicability Table CR0063R01 - Add Functional testing using third party test tool referencing in section 4.3 CR0064R01 - Addition of Field-Test eUICC CR0065R01 - Further changes to Functional Compliance re-testing CR0066R01 - Update of Applicability table for integrated Euicc CR0067R01 - Remove GSMA turnaround time CR0068R01 - Final Alignments between SGP.24 and SGP.16 CR0069R02 - Modification to Annex A.5 CR0070R01 - Add eUICC Fast Track in Annex A.1 CR0071R00 Extract Applicability table from SGP.16 V1.5 core CR0072R01 Deletion of Annex C from SGP.16 V1.5		

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.