M2M Compliance Process
Version 1.1
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 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

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].

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

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 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

3.1 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 M2M features.

A new declaration (i.e. latest SGP.16 template) is to be submitted for any changes to M2M remote provisioning features.

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.

In either case, 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.

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

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, 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
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, 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 3: M2M Product Security Compliance requirements

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 4: 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. 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*

Annex B M2M Certification Applicability Table (Normative)

This Annex, found in the SGP.16 zip file, 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.

Annex C Document Management

C.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) 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)	eSIM Group	Valerie Townsend, GSMA

C.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.