M2M Compliance Process
Version 1.0
25 July 2018

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 3
1.1 Overview 3
1.2 Transition between M2M early adopters products and SGP.16 3
1.3 Scope 3
1.4 Intended Audience 3
1.5 Definition of Terms 3
1.6 Abbreviations 4
1.7 References 4
1.8 Conventions 4
2 Compliance Overview 4
3 Compliance Declarations 5
4 Compliance Requirements 5
4.1 Site Security Requirements 5
4.2 Product Security Requirements (eUICCs only) 6
4.3 Functional Compliance Requirements 7
4.3.1 Functional Compliance via Industry Partner Certification Schemes 7
4.3.2 Functional Compliance via Vendor or Third Party Implemented Test Plan 7
Annex A M2M Declaration Templates 9
Annex B M2M Certification Applicability Table (Normative) 9
Annex C Document Management 10
C.1 Document History 10
Other Information 10

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 Architecture and Technical PRDs, SGP.01 [1] and SGP.02 [2].

This version of SGP.16, including its associated annexes, is the initial version applicable from the date of publication, but references pre-existing industry certification processes, as detailed in Annex B.

Vendors who released M2M Products before the publication of SGP.16 had the opportunity to declare their products to the GSMA on the GSMA infocentre site as M2M early adopters products. These M2M early adopters products are therefore not bound to the rules stated in SGP.16.

Only after the information in the forms are validated by GSMA, can the M2M Product Vendor then request the issuance of a certificate from the GSMA certificate issuer.

1.2 Transition between M2M early adopters products and SGP.16

The allowed period for products to continue declare M2M early adopters products instead of SGP.16 compliant products is 12 months after the publication of the SGP.16 initial version. After these 12 months, compliance of new M2M Products can only be declared against SGP.16. See detailed in Annex B.

1.3 Scope

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

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

1.4 Intended Audience

M2M Product Vendors, telecom service providers, test and certification bodies, and other industry organisations working in the area of M2M/IoT.

1.5 Definition of Terms

Term	Description
M2M Product	eUICC, SM-SR (Subscription Manager Secured 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.

1.6 Abbreviations

Abbreviation	Description
eUICC	Embedded UICC
EUM	eUICC Manufacturer
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 Secured Routing

1.7 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]	RFC2119	“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

1.8 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 [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 compliancy requirements, split into “Site Security Requirements”, “Product Security Requirements” and “Functional Compliance Requirements” can be found in Annex B.

Annex B of this document 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 the M2M requirements.

Details are provided on the expected means to demonstrate compliance, together with 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 as follows:

- A completed template Annex A.1, the M2M Product declaration, which also provides details of the organisation responsible for the declaration,

Plus:

- 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

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 used 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's 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)

The security compliance requirement in IC platform protection profile PP-0084 or PP-0035, certified by Common Criteria, and listed on the common criteria portal (www.commoncriteriaportal.org/products) is mandatory.

An eUICC specific protection profile, defined by PRD SGP.05 [4], is available and mandatory for M2M Products.

Note: A GSMA-owned Security Evaluation Scheme certificate will be considered as an alternative, when available.

In all cases, the security evaluation scheme certificate references shall be included in the Annex A.2 details for the declared eUICC.

Product type	Product Security Requirement	Compliance requirement
eUICC	Security IC platform protection profile with augmentation package certification (PP-0035 or PP-0084)	Certified and listed
	SGP.05 GSMA PP eUICC for M2M (PP-0089) Or GSMA-owned Security Evaluation Scheme, when available (see Note1)	Certified and listed

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 provides the required means of test for eUICCs, referencing the SGP.11 [3] test 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]. Annex 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

Annex A M2M Declaration Templates

An M2M Product declaration consists of Annex A.1 plus 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 recommended to reference this table when planning product compliance.

Annex C Document Management

C.1 Document History

Version	Date	Brief Description of Change	Approval Authority	Editor / Company
V1.0	XXth Jul 2018	Initial version of SGP.16 V1.0 M2M Compliance Products	SIM Group/TG	Gloria Trujillo, GSMA

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.

5