eSIM CI Registration Criteria

Version 1.0

24 October 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

The digital public key Certificate plays an essential role to identify and authenticate the entities within the GSMA eSIM ecosystem.

The specific requirements for mutual authentication within the eSIM solution make the use of frequently used internet Certificates unsuitable and hence the GSMA solution defines a specific PKI for eSIM.

This PKI is critical for the security of eSIM and consequently, the rigour and security of the GSMA eSIM Certificate Issuer (GSMA CI) keys are critical to the security of the ecosystem.

In addition, the stability, longevity, and distribution reach of a GSMA CI's Certificates are factors that affect the consumer's interoperability with their choice of mobile network providers.

1.1 Purpose

This document serves as a guidance for companies who are interested in applying to become a GSMA CI.

1.2 Overview

This section describes the role of Certificate Authority (CA) in a general PKI, the GSMA CI and what is termed as an Independent eSIM CA.

Any PKI depends on digital Certificates for signatures, authentication and key-agreement. The trust in such Certificates is crucial and this trust is placed in what is known as the Certificate Authority (CA).

1.3 Certificate Authority

A Certificate Authority is an organisation which is accredited by a Policy Authority (PA) to issue manage, revoke, and renew digital Certificates. GSMA is the eUICC PKI Policy Authority (PKI-PA) in this document.

If two CAs belong to different PKIs, there is not a trust path between the CAs. Therefore, their Certificates are not trusted across the two CAs.

1.4 GSMA CIs

GSMA acts as a Policy Authority for the eUICC PKI. A CA accredited by the Policy Authority becomes a GSMA CI

This document describes the eligibility criteria to become a GSMA CI.

1.5 Independent eSIM CAs

A CA accredited by a different Policy Authority and issuing Certificates to eSIM actors (EUMs, SM-DP+ providers, etc.) is called an *Independent eSIM CA*.

Note: this only affects eSIM (Remote SIM Provisioning) operations, not mobile network services.

1.6 Relevant Documents

The following documents should be read in conjunction with this document:

[1] SGP.01 Embedded SIM Remote Provisioning Architecture
[2] SGP.02 Remote Provisioning Architecture for Embedded UICC Technical Specification
[3] SGP.14 GSMA eUICC PKI Certificate Policy
[4] SGP.16 M2M Compliance Process
[5] SGP.21 Remote SIM Provisioning Architecture
[6] SGP.22 RSP Technical Specification
[7] SGP.24 RSP Compliance Process
[8] Recognised CI Term Sheet

1.7 Scope

This document covers all variants of the GSMA eSIM specifications, including Consumer and M2M versions.

1.8 Definitions of Terms

Term	Description
Certificate	A digital representation of information which at least: • Identifies its issuing Certificate Authority • Names or identifies the Subscriber of the Certificate • Contains the Subscriber’s public key • Identifies its operational period Is digitally signed by the issuing Certificate Authority
Certificate Authority (CA)	An entity accredited to issue, manage, revoke, and renew Certificate.
Certificate Issuer (CI)	An entity that is accredited by the Policy Authority to issue digital Certificates.
GSMA Certificate Issuer (GSMA CI)	A Certificate Authority accredited by the GSMA to enable global interoperability within the GSMA eSIM ecosystem.
Device	User equipment used in conjunction with an eUICC to connect to a mobile network e.g. a tablet, wearable, smartphone or handset.
eSIM	eSIM is the top level generic descriptor applied to the Devices and eUICCs that support Remote SIM Provisioning.
eUICC	A removable or non-removable UICC which enables the remote and/or local management of profiles in a secure way. NOTE: The term originates from "embedded UICC".
Independent eSIM CA	A non-GSMA CI that issues digital public key Certificates for a specific region, company or group of companies for eSIM purposes.

Operator	A Mobile Network Operator or Mobile Virtual Network Operator; a company providing wireless cellular network services.
Public Key Infrastructure (PKI)	A set of policies, processes, server platforms, software and workstations used for the purpose of administering Certificates and public-private key pairs, including the ability to issue, maintain, and revoke public key Certificates.

1.8 Abbreviations

Term	Description
CA	Certificate Authority
CI	Certificate Issuer
CP	Certificate Policy
CRL	Certificate Revocation List
PA	Policy Authority
PKI-PA	PKI Policy Authority

1.9 References

Ref	Document Number	Title
[1]	SGP.01	Embedded SIM Remote Provisioning Architecture
[2]	SGP.02	Remote Provisioning Architecture for Embedded UICC Technical Specification
[3]	SGP.14	GSMA eUICC PKI Certificate Policy
[4]	SGP.16	M2M Compliance Process
[5]	SGP.21	Remote SIM Provisioning Architecture
[6]	SGP.22	eSIM RSP Technical Specification
[7]	SGP.24	RSP Compliance Process
[8]		Recognised CI Term Sheet

2 Role of CIs in eSIM

2.1 GSMA CI

GSMA CIs are gatekeepers for the PKI infrastructure used in all GSMA eSIM solutions.

GSMA CIs will be expected to fully comply with and where applicable, enforce the GSMA eUICC PKI Certificate Policies [3].

GSMA CIs will be required to sign and agree with the legal terms and conditions for the use of ‘GSMA CI’ [8].

2.2 Independent eSIM CA

Any organisation is able to establish their own eSIM Certificates using the GSMA's published specifications.

All CAs should recognise that Devices using their Certificates are limited to capabilities offered by only those Operators and Service Providers who have also chosen to use the same CA's Certificates. The use of Certificates offered by an Independent eSIM CA is based on consensus from all the actors of the ecosystem. Entities that have chosen to use only Independent eSIM CAs will not be able to operate within the GSMA ecosystem.

Any Devices/LPAs choosing to use Certificates from multiple CAs, SHALL ensure they have implemented a robust method of selecting the correct Certificate for the service the consumer wishes to engage with.

An Independent eSIM CA wishing to be recognised as a GSMA CI SHALL follow the registration process for GSMA Recognised CIs. Responses to the criteria in Section 3 will be part of the GSMA CI registration process.

CAs interested in providing this service should contact GSMA (RootCAs@gsma.com).

2.3 All CAs

Any CA should consider the following requirements:

- Ensure continuity of services in the case where Certificates are no longer provided.
- Protection for systems used in the generation and management of Certificates.
- Complete logging, monitoring and alerting of security-related changes.
- Compliance with Auditing Requirements as needed.

3 Criteria to become a GSMA CI

3.1 Criterion 1: Compliance

- Description: Compliance is required to the specifications in SGP.21 [5], SGP.22 [6], SGP.01 [1], SGP.02 [2], SGP.16 [4], and SGP.24 [7].
- Key sections in these specifications are:
    - SGP.21 section 3.5 "Certificate Issuer" [5]
    - SGP.22 section 4.5 "Keys and Certificates" [6]
    - SGP.01 section 2.3 "The eUICC ecosystem" [1]
    - SGP.02 section 2.3 "Security overview" [2]
    - SGP.16 (whole specification)
    - SGP.24 (whole specification)
- Proof: Statement in application as part of terms and conditions defined in [8].

3.2 Criterion 2: International coverage

- Description: Ability to distribute and support Certificate issuance in different countries on a non-discriminatory basis.
- Proof: Evidence of market coverage.

3.3 Criterion 3: Quality assurance

- Description: Suitable QA procedures with supporting audits.
- Proof:

  Either:

  - Webtrust Certificate, and/or
  - Equivalent from government certification body

3.4 Criterion 4: Agreement to commit to a Business Continuity Plan

- Description: Devices attached to the GSMA CI could become stranded and unable to download new profiles from operators. A GSMA CI leaving the GSMA ecosystem without a proper business continuity plan could potentially harm current and future product deployments and thus damage eSIM's reputation as a viable Remote SIM Provisioning solution. Therefore, the GSMA CI needs to demonstrate its on-going commitment to devices already attached to this GSMA CI. In the case where a GSMA CI wishes to discontinue their service, there shall be a commitment to the following:
  - Maintaining the CRL for the entities to verify the validity of existing Certificates.
  - Ensure a mechanism is in place for the ongoing provisioning of valid Certificates to any impacted entities (e.g. SM-DP+s)
- Proof: Statement from CA and a summary of the Business Continuity Plan.

3.5 Criterion 5: Coverage

- Description: Interoperability is improved when the GSMA CI covers a large number of Operators. However, a concentration of a high number of CAs in a region will not provide a more robust ecosystem, but more likely, give rise to interoperability issues.
- Proof: To provide a list of the countries where the GSMA CI is going to provide service.

3.6 Criterion 6: Ability to control quality

- Description: Due diligence of supply procedures.
- Proof: The GSMA CI should demonstrate that they have a robust process to undertake appropriate due diligence against prospective customers in order to maintain a high quality and trusted ecosystem. As an example, declaration such as:
  - Due diligence to prove legal title of the respective companies.
  - Declare they will only issue Certificates to GSMA compliant entities according to SGP.24 [7] and SGP.16 [4].
  - Declare audit procedures and results.

3.7 Criterion 7: Ability to protect the ecosystem.

- Description: Detect, revoke and remove Certificates that damage Operator networks or do not comply.

- Proof: A declaration stating that, the GSMA CI will revoke the Certificate upon request, and a description of how this process will be executed.

3.8 Criterion 8: Non-discrimination

- Description: The GSMA CI shall ensure that issuance and management of its Certificates is done in a non-discriminatory way.
- Proof: A declaration stating that the GSMA CI will issue Certificates in a non-discriminatory way.

Annex A Document Management

A.1 Document History

Version	Date	Brief Description of Change	Approval Authority	Editor / Company
1.0	15/07/2019	First version of SGP.28	eSIM	Yolanda Sanz/GSMA

Other Information

Type	Description
Document Owner	Yolanda Sanz
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 or suggestions & questions are always welcome.