eUICC Security Assurance Principles

Version 1.0

07 July 2020

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

Security Classification: Non-confidential

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.

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.

Contents

1 Introduction

1.1 Overview

The GSMA eUICC Security Assurance Scheme is an independent security evaluation scheme for evaluating embedded UICCs (eUICCs) against the provisions of Protection Profiles for eUICCs (currently PP-0089 [1] and PP-0100 [2]). The scheme aims to establish trust for Service Providers and other risk-owners that their assets, including profiles for eUICC remote provisioning, are secure against state-of-the-art attackers. The scheme is based on the Common Criteria methodology ISO15408 [6], optimised for GSMA compliant eUICCs.

The scheme owner is the GSMA. The scheme is operated in accordance with the provisions and expectations of ISO17065 [7]. It includes a certification function with the Certification Body (CB) role, appointed by GSMA.

1.2 Scope

This document provides the GSMA eUICC Security Assurance principles for the GSMA eUICC Scheme including key details, contacts, and links.

1.3 Definitions

Term	Description
Certifier	Person acting on behalf of the GSMA Certification Body
Developer	Person acting on behalf of the EUM
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".
Evaluator	Person acting on behalf of the Licensed Laboratories
GSMA Certification Body	Certification Body role, appointed by GSMA
Licensed Laboratory	A security evaluation laboratory licensed by a GSMA CB to perform eUICC security evaluations for the GSMA eUICC Scheme
SOG-IS Authorising Scheme	As defined by https://www.sogis.eu/uk/status_participant_en.html and https://www.sogis.eu/uk/tech_domain_en.html (technical domain: smart cards and similar devices)

1.4 Abbreviations

Term	Description
CC	Common Criteria
CCRA	Common Criteria Recognition Agreement
EUM	eUICC Manufacturer
GSMA CB	GSMA Certification Body
IC	Integrated Circuit

Term	Description
ST	Security Target
TOE	Target of Evaluation

1.5 References

Ref	Doc Number	Title
[1]	[SGP.05]	Embedded UICC Protection Profile, also published by BSI as BSI-CC-PP-0089-2015
[2]	[SGP.25]	RSP eUICC for Consumer Device Protection Profile, also published by BSI as BSI-CC-PP-0100-2018
[3]	[SGP.07]	GSMA eUICC Security Assurance Methodology
[4]	[AA.35]	GSMA Procedures for Industry Specification
[5]	[RFC2119]	"Key words for use in RFCs to Indicate Requirement Levels", S. Bradner http://www.ietf.org/rfc/rfc2119.txt
[6]	[ISO15408]	The Common Criteria for Information technology — Security techniques — Evaluation criteria for IT security
[7]	[ISO17065]	Conformity assessment — Requirements for bodies certifying products, processes, and services
[8]	[CCRA]	Assurance Continuity: CCRA Guidelines
[9]	[GSMA PRD AA.35]	Procedures for Industry Specifications

1.6 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 TOE Overview and Scheme Contact Details

2.1 TOE-type overview

The scope for GSMA eUICC security evaluation is the combination of the hardware and software components implementing an eUICC (IC, JavaCard, etc.) holding profiles for remote provisioning, excluding the specific profiles themselves.

The details of the security certification scopes and requirements are provided in PP-89 [1] and PP-100 [2].

2.2 Contact details

The primary source of contact information on the scheme shall be published on the GSMA website. This includes details of the scheme Certification Body and Licensed Laboratories as well as links to scheme procedures and documents and the scheme owner contact address.

3 GSMA Certification Body (GSMA CB)

The scheme is expected to operate in accordance with the provisions and expectations of ISO17065 [7]. A GSMA appointed Certification Body is responsible for gaining and maintaining ISO17065 [7] accreditation for the scheme, including identifying necessary updates to the GSMA scheme documentation to align with ISO17065 [7] expectations.

The GSMA CB is responsible for, among other things, Certification activities, licensing laboratories for the scheme (according to the scheme defined criteria) and alignment of Licensed Laboratories to ensure a common approach to evaluations performed under the scheme.

The GSMA CB shall include the GSMA scheme within its scope of ISO17065 [7] accredited certification activities.

4 Laboratory Licensing

The GSMA CB(s) are required to manage the licensing of laboratories for the GSMA eUICC scheme. For a laboratory to become and stay licensed under the scheme, they need to:

1. Show and continue to show quality in performing evaluation considering state-of-the-art attackers.
2. Have and maintain a valid ISO-17025 [8] accreditation with Common Criteria (including performing at least EAL4+ALC_DVS.2+AVA_VAN.5 assurance requirements) in the technical domain of smart cards and similar devices.
3. Have and maintain a valid accreditation under a SOG-IS Authorising Scheme for the technical domain of smart cards and similar devices.[1]
4. Agree to the standard NDA with the GSMA CB.
5. Pay the relevant GSMA administration fee, this fee waived for laboratories who are GSMA members.

Laboratories wishing to be licensed should contact the GSMA CB and be prepared to provide evidence of fulfilling the above requirements. The result of a successful submission is listing by the GSMA CB as Licensed Laboratory.

5 Process

The scheme consists of the following phases:

1. Submission
2. Evaluation
3. Certification.

Prior to submission, the Developer shall have contracted with a Licensed Laboratory.to fill the application form together

[1] Under the SOG-IS rules at the time of issuance of this document, point 3 implies 1 and 2 are addressed.

The expected response time for all parties involved in each phase (submission, evaluation and certification) is 10 working days.

5.1 Submission Phase

A signed copy of the application form , together with a draft Security Target (ST), must be sent to the GSMA CB.

Note: the (draft) ST SHALL be in accordance with the scheme scope; compliance claims to PP-89 [1] and/or PP-110 [2].

The GSMA CB will respond with a quotation for certification for acceptance by the EUM. Upon agreement of quotation and schedule the evaluation phase shall commence.

A fixed price list will be published and updated annually for all types of certifications.

5.2 Evaluation Phase

By default, the three-stage evaluation phases defined by the GSMA eUICC Security Assurance Methodology [3] will be applied for eUICC evaluations under the scheme, following the GSMA accepted CB process. The first two evaluation stages may be combined resulting in a single meeting with the approval of the GSMA CB, if this is desired by the Developer, with a potentially increased project risk for the Evaluator and Developer.

Reporting for GSMA eUICC evaluations shall follow the GSMA eUICC Security Assurance Methodology [3].

5.3 Certification Phase

Certificates are published by the GSMA even after expiry.

The certificate validity period for GSMA eUICC certificates is five (5) years from last or more recent of the issuance date. If required, this period can be repeatedly extended through recertification.

Where certification relies on underlying composite product certificates these certificates shall have at least 12 months remaining validity at the time of certification issuance.

5.4 Certification Procedures and Assurance Continuity

The certification process supports new product certification and changed TOE certification based on the CCRA terminology supporting document “Assurance Continuity: CCRA Guidelines.”[8] Specifically, the GSMA eUICC scheme provides the following certification procedures.

5.4.1 New Certification

This procedure shall be used for new product evaluations.

5.4.2 Maintenance with Minor Changes

This procedure shall be used for changes of the TOE without security impact. Maintenance may not require involving a Licensed Laboratory. If it is not clear whether a security function has changed, the Developer shall assist the Certifier by providing an analysis from a Licensed Laboratory.

The maintained certificate will have the same validity as the original certificate.

5.4.3 Maintenance with Major Changes

This procedure shall be used for security relevant changes, where only the changed functionality will be assessed. It always requires the involvement of a Licensed Laboratory and the vulnerability analysis and testing are limited to the changes. The certificate validity from the original certificate will be kept.

5.4.4 Re-Certification

This procedure shall be used to extend the certificate validity with or without changing the TOE.

If major changes are present, then the evaluation focusses on the changes of the TOE using the current state-of-the-art attack techniques.

If the TOE is not changed, then the vulnerability analysis and testing is updated considering the current state-of-the-art attack techniques.

6 Scheme Oversight – Advisory Panel

Scheme oversight shall be performed by a GSMA Advisory Panel with participation representative of all participants in the scheme.

The roles of this panel shall include:

Periodic review of the scheme in order to:

- Review feedback on the scheme operation and ensure the scheme remains fit for purpose.
- Propose scheme improvements to ensure it remains optimised for GSMA eUICC scheme evaluations.

Risk management:

- Agree on potential waivers to the security requirements, as identified by the GSMA CB and other inputs
- Analyse potential security flaws not covered by the scheme and manage the evolution of the scheme, the GSMA Protection Profile [1] and [2], and the correspondinglist of attacks
- Analyse and mitigate security issues reported to the panel by the GSMA CB

7 Appeals

In the case of queries between any scheme participants the Appeal process described in AA.35 [4] section 10 shall apply.

8 Scheme Monitoring

Scheme monitoring shall be performed by GSMA. This monitoring shall include the following indicators:

1. Time monitoring:

    a) Time between the receipt of the application form including the draft Security Target from the Developer and the GSMA CB sending the appropriate quotation.

    b) Time between receipt of evaluation reporting from Licensed Laboratory and the approval of the ETR by the GSMA CB.
    c) Time between the approval of the ETR by the GSMA CB and the delivery of the final certificate.

2. Number of certified products per year to evaluate how the scheme is used.

These indicators shall be shared by GSMA on regular basis.

Annex A GSMA eUICC Security Assurance Application Form

This application form requests an eUICC Security Assessment under the GSMA scheme operated by GSMA CB.

This document shall be completed and submitted to the appropriate GSMA recipient. The signed form (in pdf format) shall be included along with the (draft) Security Target.

Application type	□ New Certification □ *Maintenance with Minor Changes: [Reference of the original certificate] [Latest issue date]* *□ Maintenance with Major Changes: [Reference of the original certificate] [Latest issue date]* □ Re-Certification: *[Reference of the original certificate] [Latest issue date]*
Publish certificate in the GSMA website	□ Yes □ No

A.1 General Product Information

Product Name	*[Product Name or Number as found on the device or packaging]*
Marketing Name	*[Product name as known by the customer]*
Software version	*[The initial SW version(s) used for RSP compliance for this declaration]*
TOE reference	*[Name] [Version]*
ST reference	*[Name] [Version] [Date]*
Product type	□ *Consumer: [SGPs versions]* □ *Machine-to-Machine: [SGPs versions]*
Certification type	□ *Consumer: [PP version]* □ *Machine-to-Machine: [PP version]*

A.2 Details of Submitter (Developer)

Company Name	*[Company name as registered for GSMA]*
Contact Name	*[Name of the person]*
Position	*[Position of the person]*
Address	*[Address of the person]*

Telephone	+
Email Address	*[Email of the person]*

A.3 Details of Evaluator

Company Name	*[Company name as registered for GSMA CB]*
Contact Name	*[Name of the person]*
Position	*[Position of the person]*
Address	*[Address of the person]*
Telephone	+
Email Address	*[Email of the person]*

A.4 Details of eUICC

TOE reference	*[Name] [Version]*
ST reference	*[Name] [Version] [Date]*

A.5 Schedule Dates

Intended Deliverable date of EM1	
Proposed EM1 date	
Intended Deliverable date of EM2	
Proposed EM2 date	
Intended Deliverable date of EM3	
Proposed EM3 date	

A.6 Signatures

A.6.1 Signature of Developer

Signature		
Name		
Position		
Company Name		

A.6.2 Signature of Evaluator

Signature		

Name		
Position		
Company Name		

Annex B Document Management

B.1 Document History

Version	Date	Brief Description of Change	Approval Authority	Editor / Company
1.0	07 July 2020	New Document for	ISAG	Gloria Trujillo

B.2 Other Information

Type	Description
Document Owner	Gloria Trujillo, GSMA
Editor / Company	Gloria Trujillo, 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.