eUICC Security Assurance Principles
Version 2.1
22 March 2024

Security Classification: Non-Confidential

Copyright Notice

Disclaimer

Compliance Notice

The information contain herein is in full compliance with the GSMA 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 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 SGP.05 [1] and SGP.25 [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 Bodies (CB), 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
eSA Appeals Board	Group in charge of ruling on appealed Evaluation and Certification Results, deciding to uphold the Evaluation and Certification Results or decide on the interpretation of the eSA scheme.
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
CB	Certification Body
CC	Common Criteria
CCRA	Common Criteria Recognition Agreement

Term	Description
eSA	eUICC Security Assurance
EUM	eUICC Manufacturer
GSMA CB	GSMA Certification Body
IC	Integrated Circuit
ST	Security Target
TOE	Target of Evaluation

1.5 References

Ref	Doc Number	Title
[1]	[SGP.05]	Embedded UICC Protection Profile, version • 1.0, GSM Association, September 2014 • 1.1, GSM Association, August 2015 also published by BSI as BSI-CC-PP-0089-2015 • 4.0, GSM Association, October 2022 • 4.1, GSM Association, March 2023
[2]	[SGP.25]	RSP eUICC for Consumer Device Protection Profile, version: • 1.0, GSM Association, June 2018 also published by BSI as BSI-CC-PP-0100-2018 • 2.0 GSM Association, December 2023
[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]	Void	Void
[10]	[RFC8174]	Ambiguity of Uppercase vs Lowercase in RFC 2119 Key Words https://www.rfc-editor.org/info/rfc8174
[11]	[JIL AM]	JIL Attack Methods for Smartcards and Similar Devices
[12]	[JIL AP]	JIL Application of Attack Potential to Smartcards

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] and clarified by RFC8174 [10], when, and only when, they appear in all capitals, as shown here.

“FFS” or “For Further Study” means that it will be covered in the next version of SGP.06.

2 TOE Overview and Scheme Contact Details

2.1 TOE-type overview

The scope for GSMA eUICC Security Assurance (eSA) 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 SGP.05 [1] and SGP.25 [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)

For a Certification Body to become a GSMA appointed Certification Body and stay appointed under the eSA Scheme, they need to:

- Respond to the GSMA eSA CB Request for Proposal.
- Satisfy the requirememts stated in the GSMA eSA CB Request for Proposal.
- Sign the GSMA eSA Scheme Standards Terms and Conditions.
- Sign the Letter of Agreement on GSMA eSA Scheme.

A GSMA appointed Certification Body SHALL be responsible for:

1. **ISO17065 [7] accreditation:**

    a. Gaining and maintaining ISO17065 [7] accreditation for the scheme, including identifying necessary updates to the GSMA scheme documentation to align with ISO17065 [7] expectations.

    b. Including the GSMA eSA scheme within its scope of ISO17065 [7] accredited certification activities.

2. **Laboratory Licensing:**

    a. Licensing their laboratories for the scheme (according to the scheme defined criteria).

    b. Alignment of Licensed Laboratories to ensure a common approach to evaluations performed under the scheme methodology. In case of the Vulnerability Analysis, the alignment SHALL be based on the latest JIL guidance documentation [11] and [12].

3. Certification Consistency:

In order to assist the consistent application of the criteria and methods between Evaluation and Certification processes, each GSMA Certification Bodies SHALL ensure and work towards a uniform interpretation of the currently applicable eSA Scheme Principles and Methodology [3] and in case of Vulnerability Analysis, it will base its final judgment on current JIL guidance [11] and [12].

4 Laboratory Licensing

For a laboratory to become and stay licensed under the eSA Scheme, they need to:

- Show and continue to show quality in performing evaluation considering state-of-the-art attackers.
- 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.
- Have and maintain a valid accreditation under a SOG-IS Authorising Scheme for the technical domain of smart cards and similar devices.[1]
- Agree to the standard NDA with the GSMA CB.
- Pay the relevant GSMA administration fee, this fee waived for laboratories who are GSMA members.
- Sign the GSMA eSA Standards Terms and Conditions.

A GSMA Licensed Laboratory SHALL be responsible for:

1. Reporting its analysis, describing the evaluation activities according to the evaluation methodology and provide a clear conclusion whether the product meet the requirements or not.
2. Performing the vulnerability analysis and testing, needed to ensure that the product is protected against state of the art attacks as they are defined in the applicable documents, including the current JIL guidance [11] and [12].

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

5 Process

The scheme consists of the following phases:

1. Submission
2. Evaluation
3. Certification.

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

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

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), SHALL be sent to the GSMA CB.

Note: the (draft) ST SHALL be in accordance with the scheme scope; compliance claims to SGP.05 [1] and/or SGP.25 [2].

The GSMA CB SHALL 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 SHALL be published by the GSMA CBs, 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 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 SHALL be 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

Scheme oversight SHALL be performed by committee comprised of GSMA staff and GSMA members representatives of all participants in the scheme.

It is responsible for maintenance of the eSA Scheme documentation.

The roles of this panel SHALL include:

The periodic review of the eSA scheme documentation SHOULD focus on:

- 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.
- Contributes to the development of Certification Body and Licensed Laboratory selection criteria.

The eSIMWG5 Subgroup is also responsible for risk management of the eSA Scheme such as:

- 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 eSIMWG5 Subgroupby the GSMA CB

The eSIMWG5 Subgroup is also responsible for ensuring alignment between performance and assurance of the GSMA eSA Certification Bodies.

Updates will normally arise from a regular review meeting of the eSIMWG5 Subgroup. Where acute issues are identified ad hoc meetings MAY be convened to discuss updates to the eSA Scheme documentation.

7 Appeals

Appeals SHOULD first be brought to the GSMA CB that SHALL apply their appeal process as described in ISO17065[7] and that SHALL take precedent to the appeal process by the eSA Appeal Board.

In the event that the GSMA CB appeal process as described in ISO17065[7] does not resolve the dispute, the Developer MAY lodge an appeal with the GSMA within twenty (20) business days of completion of the Evaluation/Certification. The GSMA will refer the appeal to the eSA Appeals Board.

In case of an appeal, the evaluation report will also be provided to the eSA Appeals Board.

The eSA Appeals Board is comprised of one Licensed Laboratory and one GSMA CB (if it exist) separate from the Licensed Laboratory and GSMA CB companies that performed the Evaluation/Certification that is the subject of the appeal.

The eSA Appeals Board will consider and rule on appealed Evaluation and Certification Results, deciding to uphold the Evaluation and Certification Results or decide on the interpretation of the eSA scheme. The process to be followed by the eSA Appeals Board will include:

- Review of the Evaluation Report, focussing on the appealed assessment(s)

- Discussion with the Licensed Laboratory and GSMA CB that perfomed the Evaluation/Certification

The Developer MAY request the members of the eSA Appeals Board to sign an NDA prior to receiving a copy of the Evaluation Report and other information about the product in question.

The eSA Appeals Board will seek to rule on appeals within twenty (20) business days of lodgement of the appeal, subject to the availability of the Licensed Laboratory, GSMA CB and the Developer and the prompt provision of any information requested from either party.

The Developer and the Licensed Laboratory and GSMA CB companies that performed the Evaluation/Certification that is the subject of the appeal, agree to accept the decision of the eSA Appeals Board as final.

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.

Certificate 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

TOE reference	*[Name] [Version]*
ST reference	*[Name] [Version] [Date]*
Protection Profile	*[Depending on the 'Product type' above, indicate the PP document and version. Please mark only one]* ☐ **SGP.25** ☐ **SGP.05**
Version	*[add the PP version here]*

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 Final Evaluation Meeting Schedule Date

Proposed Final Evaluation Meeting date	

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, GSMA
1.1	05 July 2023	CR0030R01 - Introduce multiple CBs CR0031R04 – CR Advisory Panel Changes CR0032R01 - SGP.06 Annex A modifications CR0033R03 - SGP.06 Annex A further modifications	ISAG	Gloria Trujillo, GSMA
2.0	19 December 2023	CR0035R02 - Add latest versions of SGP.05 and SGP.25 to the scope	ISAG	Gloria Trujillo, GSMA
2.1	22 March 2024	CR0036R01 – Add JIL document into reference section and add correspondent sentences	ISAG	Gloria Trujillo, GSMA

B.2 Other Information

Type	Description
Document Owner	eSIMG
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.