Security Evaluation of Integrated eUICC

Version 1.0

25 March 2021

This Industry Specification 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 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.

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

Table of Contents

1 Introduction

1.1 Overview

The Integrated eUICC consists of:

- An Integrated TRE: hardware sub-system within a System-on-Chip (SoC) and its low-level kernel and software services
- The eUICC OS software: executed inside the Integrated TRE hardware, is stored securely in TRE internal memories and/or in remote memories, typically the hosting device Non Volatile Memory and/or RAM.

The Integrated TRE consists of three parts:

1. A kernel managing TRE hardware security functions.
2. The services for communication, application management, and memory management.
3. The hardware platform.

All the above mentioned parts of the Integrated eUICC have been taken into consideration in order to develop in this document the creation of the security certification framework for the Integrated eUICC.

1.2 Scope

This document covers the security certification framework for the Integrated eUICC and the process that SHALL be followed to perform the security evaluation of the Integrated eUICC that have been designed referencing GSMA PRD SGP.01 [1]. The associated Protection Profiles are described in GSMA PRD SGP.05 [2] and PP-0084 [6].

Integrated eUICCs assessed under these procedures are expected to be able to declare compliance to the eUICC security assurance requirements of the GSMA M2M and RSP compliance processes, SGP.16 [3].

This document describes a temporary certification methodology for Integrated eUICC awaiting an appropriately validated Protection Profile to be developed (i.e. certified as per Common Criteria process and referenced by GSMA).

The validity period of the temporary certification described in the present document is set up by the GSMA compliance programme [3].

NOTE: The Secure Subsystems in SoC (3S) Protection Profile, under development by Eurosmart, is a potential candidate for a definitive security certification methodology for the Integrated TRE used by the Integrated eUICC

1.3 Definitions

Term	Description
Certification Report	Evaluation Report issued by the Certification Body to attest the certification.
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".

Term	Description
Integrated eUICC	An eUICC implemented on a Tamper Resistant Element (TRE) that is integrated into a System-on-Chip (SoC), optionally making use of remote volatile/non-volatile memory (as per SGP.01 definition).
Integrated TRE	A TRE implemented inside a larger System-on-Chip (SoC)
GSMA Certification Body	Certification Body role, appointed by GSMA
Protection Profile	Implementation-independent statement of security needs for a TOE type (as per the Common Criteria methodology).
Security Target	Implementation-dependent statement of security needs for a specific identified TOE (as per the Common Criteria methodology).
Tamper Resistant Element	A security module consisting of hardware and low-level software providing resistance against software and hardware attacks, capable of securely hosting operating systems together with applications and their confidential and cryptographic data (as per SGP.01).

1.4 Abbreviations

Term	Description
eSA	GSMA eUICC Security Assurance
CB	Certification Body
IC	Integrated Circuit
ITSEF	Information Technology Security Evaluation Facility
NVM	Non Volatile Memory
OS	Operating System
RAM	Random Access Memory
SFR	Security Functional Requirement
SoC	System-on-Chip
SOG-IS	Senior Officials Group Information Systems Security
ST	Security Target
TOE	Target of Evaluation
TRE	Tamper Resistant Element
3S	Secure Subsystem in SoC

1.5 References

Ref	Doc Number	Title
[1]	[SGP.01]	Embedded SIM Remote Provisioning Architecture
[2]	[SGP.05]	Embedded UICC Protection Profile, also published by BSI as BSI-CC-PP-0089-2015
[3]	[SGP.16]	M2M Compliance Process v1.2
[4]	[GSMA PRD AA.35]	Procedures for Industry Specifications

Ref	Doc Number	Title
[5]	[RFC2119]	"Key words for use in RFCs to Indicate Requirement Levels," S. Bradner http://www.ietf.org/rfc/rfc2119.txt
[6]	PP-0084	BSI-CC-PP-0084-2014 Security IC Platform Protection Profile with Augmentation Packages, Version 1.0, Eurosmart 2014, certified by Bundesamt fur Sicherheit in der Informationstechnik (BSI)
[7]	PP-0089	BSI-CC-PP-0089-2015 Embedded UICC Protection Profile Version 1.1 / 25.08.2015, certified by Bundesamt fur Sicherheit in der Informationstechnik (BSI)
[8]	JIL-CCCE	Joint Interpretation Library Composite product evaluation for Smart Cards and similar devices Version 1.5.1 May 2018
[9]	[RFC8174]	Ambiguity of Uppercase vs Lowercase in RFC 2119 Key Words https://www.rfc-editor.org/info/rfc8174

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 [9], when, and only when, they appear in all capitals, as shown here."

2 Certification Process

2.1 Overview

In order to achieve the security certification of an Integrated eUICC, the process described in the following steps SHALL be executed:

1. Security certification of the Integrated TRE SHALL be obtained with a SOG-IS CB in the domain of '*smartcard and similar devices*' according to PP-0084 [6] and augmentation of the Security Target with additional Security Functional Requirements (SFRs)
to cover the security requirements defined in SGP.01 [1] Annex G.

2. Composite certification of the Integrated eUICC SHALL be done:

- Based on the Integrated TRE certified with the SOG-IS CB, and
- According to PP-0089 [7] using the assurance schemes authorised in SGP.16 [3]

The validation of the Integrated eUICC integration into the device is out of the scope of this document.

2.2 Security Certification for the Integrated eUICC

At the moment, there is no Protection Profile that covers the Integrated TRE isolation and optional use of remote memory as described in SGP.01 [1] Annex G. To bridge this gap, this document mandates to certify the Integrated TRE using Protection Profile BSI-CC-PP-0084-2014 [6] and to augment with the isolation and optional remote memory requirements described in SGP.01 [1] Annex G as part of the Security Target, as described below.

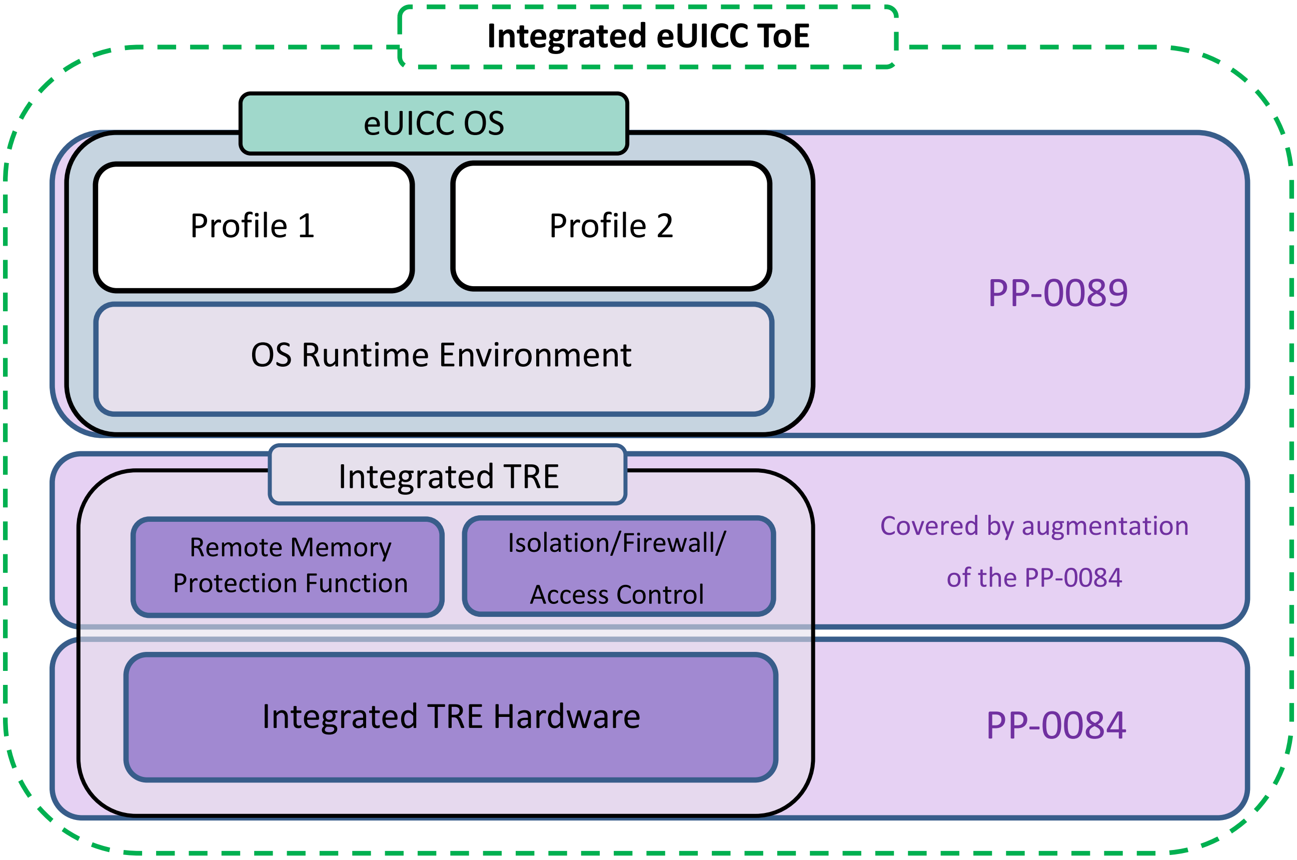

Figure 1 Composite Certification for the Integrated eUICC

A- Loader:

The BSI-CC-PP-0084-2014 [6] describes two possible optional loaders as augmentation packages:

1. The Package 1 loader for usage during the manufacturing stage. This loader is intended to be used in a secure environment.
2. The Package 2 loader for usage after the issuance of the TRE for operation on the field. This loader is intended to be used by authorised users of the TRE.

If a loader is present, it SHALL be included either within the Integrated TRE Security Target, or by composition, in the Integrated eUICC Security Target.

B- External Non-Volatile Memory:

The BSI-CC-PP-0084-2014 [6] mandates the inclusion of the internal Non Volatile Memory (e.g. Flash Memory) which is optional in the context of Integrated eUICC requirements in SGP.01 [1]. The Integrated TRE MAY use an external Non Volatile Memory.

In such case, SGP.01 [1] defines a Remote Memory Protection Function (RMPF) which SHALL be included within the Security Target of the Integrated TRE.

2.3 Integrated TRE certification

2.3.1 Security Target Augmentation

The Integrated TRE Security Target SHALL claim compliance to the BSI-CC-PP-0084-2014 [6] and additional Security Functional Requirements (SFRs) to cover the security requirements defined in Annex G of SGP.01 [1].

The Security Target SHOULD explicitly address SoC maker's technology choices such as the memory architecture.

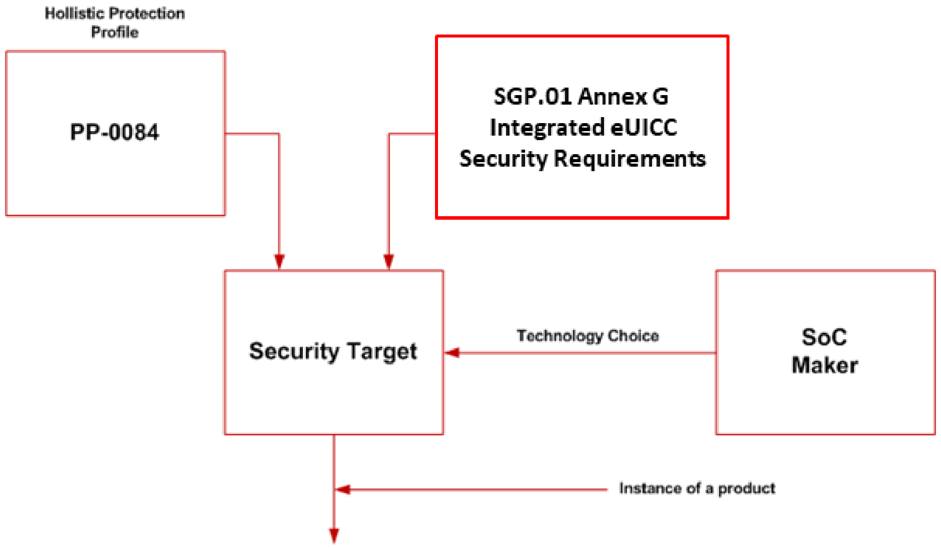
Hollistic Protection Profile
PP-0084
SGP.01 Annex G Integrated eUICC Security Requirements
Security Target
Technology Choice
SoC Maker
Instance of a product

Figure 2 Security Target for the Integrated eUICC TRE, initial phase

2.3.2 Certification Report

The Certification Report SHALL attest that the evaluation of the integrated eUICC has been performed in compliance to the BSI-CC-PP-0084-2014 [6] and the additional SFRs in the Security Target intended to cover the security requirements defined in Annex G.5 of SGP.01 [1].

2.3.3 Checklist to Support Compliance Verification

To simplify the process of reviewing the Certification Report, the ITSEF (Information Technology Security Evaluation Facility) evaluator, accredited by SOG-IS SHALL either produce a checklist or verify a checklist produced by the SoC maker.

This checklist provides evidence that all applicable requirements from SGP.01 [1] Annex G.5 'Security Functional Requirements' have been taken into account during the definition of the Security Target.

The checklist needs to be one of the deliverables to be analysed by the evaluator in whatever methodology chosen and reviewed by the CB in case the methodology followed is the GSMA eUICC Security Assurance (eSA).

2.4 Integrated eUICC Composite Certification

The Integrated eUICC Security Target SHALL comply with the security objectives and requirements as defined in Embedded UICC Protection Profile SGP.05 [2].

The evaluation of the eUICC running on the Integrated TRE SHALL be handled through the Composite Evaluation framework (see JIL-CCCE [8]).

Annex A Integrated eUICC Checklist (Informative)

The mandatory fields are SGP.01 version, Requirement and “Covered”. The Field “Security Target” is mandatory when the Security Target is public.

NOTE: The Security Target column needs to be filled with the reference of the Security Target Objective / Requirement or a rationale explaining why this requirement was considered out of scope.

Requirement	Description	Covered (Yes/No)	Security Target (see Note)	Comments
Example: ***GS01***	**Example:** *An Integrated TRE MAY use a remote memory within the Device, dedicated to the Integrated TRE, to store software and data. Remote memory can be volatile or non-volatile.*			
…	…			

Annex B Document Management

B.1 Document History

Version	Date	Brief Description of Change	Approval Authority	Editor / Company
V1.0	25/03/2021	First SGP.08 Version	ISAG	Gloria Trujillo, GSMA

B.2 Other Information

Type	Description
Document Owner	eSIMWG
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.