Security Evaluation of Integrated eUICC based on PP-0117

Version 1.0

07 October 2022

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

Security Classification: Non-confidential

Copyright Notice

Disclaimer

Compliance Notice

The information contain herein is in full compliance with the GSM Association's 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 in 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 describes the certification methodology for Integrated eUICC based on the Protection Profile PP-0117 [6] developed by Eurosmart and certified by BSI.

The certification methodology for Integrated eUICC based on the Protection Profile PP-0084 [18] is defined by SGP.08 [19].

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] and SGP.21 [9]. The associated Protection Profiles are described in GSMA PRD SGP.05 [2], and SGP.25 [10].

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, respectively SGP.16 [3] and SGP.24 [11].

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".
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 /SGP.21).
Integrated TRE	A TRE implemented inside a larger System-on-Chip (SoC)

Term	Description
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 /SGP.21).

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
RMPF	Remote Memory Protection Function
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
[3]	SGP.16	M2M Compliance Process
[4]	GSMA PRD AA.35	Procedures for Industry Specifications
[5]	RFC2119	"Key words for use in RFCs to Indicate Requirement Levels," S. Bradner http://www.ietf.org/rfc/rfc2119.txt
[6]	PP-0117	BSI-CC-PP-0117-2022 Secure Sub-System in System-on-Chip (3S in SoC) Protection Profile
[7]	PP-0089	BSI-CC-PP-0089-2015

Ref	Doc Number	Title
		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]	SGP.21	RSP Architecture
[10]	SGP.25	GSMA Embedded UICC for Consumer Devices Protection Profile
[11]	SGP.24	RSP Compliance Process
[12]	PP-0100	BSI-CC-PP-0100-2018
[13]	NIST SP 800-108	Recommendation for Key Derivation Using Pseudorandom Functions
[14]	BSI TR-02102-1	Cryptographic Mechanisms: Recommendations and Key Lengths
[15]	ANSSI RGS v2 B1	Référentiel Général de Sécurité version 2.0 Annexe B1
[16]	NIST SP 800-175B	Guideline for Using Cryptographic Standards in the Federal Government: Cryptographic Mechanisms
[17]	NIST SP 800-53r4	Security and Privacy Controls for Federal Information Systems and Organisations – Revision 4
[18]	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)
[19]	SGP.08	Security Evaluation of Integrated eUICC based on PP-0084

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 Certification Process

2.1 Security Certification for the Integrated eUICC

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-0117 [6] and a Security Target with the additional security requirements defined in Annex B.

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

- Based on the Integrated TRE certified with the SOG-IS CB, and
- According to either:

- PP-0089 [7] or SGP.05 [2] using the assurance schemes authorised in SGP.16 [3]
- PP-0100 [12] or SGP.25 [10] using the assurance schemes authorised in SGP.24 [11]

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

2.2 Integrated TRE certification

2.2.1 Security Target Augmentation

The Integrated TRE Security Target SHALL claim compliance to the BSI-CC-PP-0117-2022 [6] and the additional security requirements defined in Annex B.

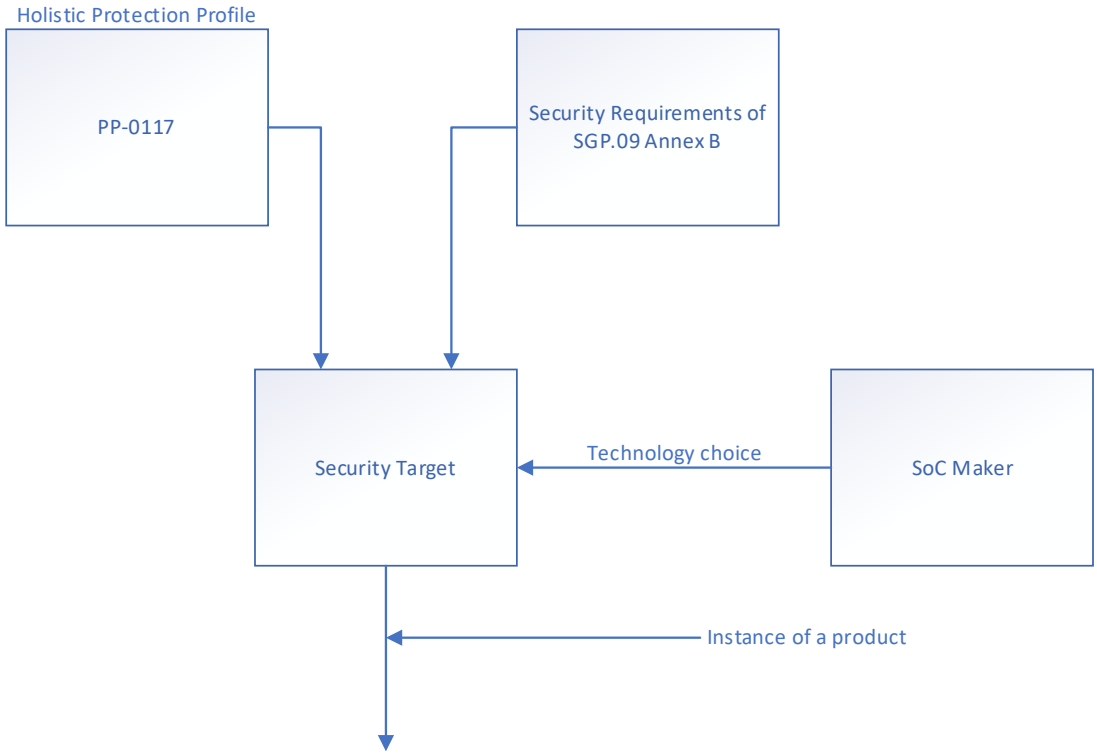

Figure 1 Security Target for the Integrated eUICC TRE

2.2.2 Certification Report

The Certification Report SHALL attest that the evaluation of the integrated eUICC has been performed in compliance to the BSI-CC-PP-0117-2022 [6] .

2.2.3 Checklist to Support Compliance Verification

The SoC maker SHALL produce a checklist, as detailed in Annex A, that provides evidence that all requirements from Annex B have been taken into account during the definition of the Security Target.
This checklist SHALL be used during the Integrated eUICC security evaluation.

2.3 Integrated eUICC Composite Certification

The Integrated eUICC Security Target SHALL comply with the security objectives and requirements as defined in the Protection Profile SGP.05 [2] or SGP.25 [10].

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 Requirement from Annex B 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: **SEC1**	**Example:** *TRE-unique seed(s) used by the RMPF SHALL be generated inside the TRE..*			

Annex B Integrated eUICC Security Requirements (Normative)

Req no.	Description
	Cryptographic Keys Requirements
SEC1	TRE-unique seed(s) used by the RMPF SHALL be generated inside the TRE.
SEC2	The entropy of the TRE-unique seed(s) used by the RMPF SHALL be at least 256 bits.
SEC3	Randomly generated keys used by the RMPF shall be at least 256 bits.
SEC4	The key derivation mechanism used by the RMPF SHALL be compliant with NIST SP 800-108 **Error! Reference source not found.**] and SHALL use: • a block cipher with security strength equivalent to or greater than AES-256, or • a hash function with security strength equivalent to or greater than SHA-256,
	Confidentiality Requirements
SEC5	The RMPF SHALL provide confidentiality based on encryption using a cipher with security strength equivalent to, or greater than AES-256 and using a suitable mode of operation approved by NIST in NIST SP 800-175B **Error! Reference source not found.Error! Reference source not found.** or recommended by BSI in BSI TR-02102-1 **Error! Reference source not found.** or recommended by ANSSI RGS v2 B1 **Error! Reference source not found.**.
	Integrity and Authenticity
SEC6	The RMPF SHALL use a cryptographic integrity mechanism with security strength equivalent to, or greater than SHA-256.

Req no.	Description
SEC7	The RMPF SHALL provide authentication using a MAC of at least 128 bits based • on a block cipher using a cipher with security strength equivalent to or greater than AES-256, or • on a hash function with security strength equivalent to or greater than SHA-256, and using a mode of operation approved by NIST in NIST SP 800-175B **Error! Reference source not found.** or recommended by BSI in BSI TR-0 2102-1 **Error! Reference source not found.** or recommended by ANSSI RGS v2 B1 **Error! Reference source not found.**.
SEC8	SEC5 and SEC7 MAY also be provided in combination by an authenticated encryption mode fulfilling both requirements.

Annex C Document Management

C.1 Document History

Version	Date	Brief Description of Change	Approval Authority	Editor / Company
V1.0	19/09/2022	CR0001R01 – SGP.18 v1.0 Adoption of PP-0117 (3S PP)	ISAG	Gloria Trujillo, GSMA

C.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.