

Security Evaluation of Integrated eUICC based on PP-0084

Version 1.2

07 October 2022

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

Copyright © 2023 GSM Association

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.

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 3](#_Toc116035818)

[1.1 Overview 3](#_Toc116035819)

[1.2 Scope 3](#_Toc116035820)

[1.3 Definitions 4](#_Toc116035821)

[1.4 Abbreviations 4](#_Toc116035822)

[1.5 References 5](#_Toc116035823)

[1.6 Conventions 6](#_Toc116035824)

[2 Certification Process 6](#_Toc116035825)

[2.1 Overview 6](#_Toc116035826)

[2.2 Security Certification for the Integrated eUICC 6](#_Toc116035827)

[2.3 Integrated TRE certification 8](#_Toc116035828)

[2.3.1 Security Target Augmentation 8](#_Toc116035829)

[2.3.2 Certification Report 8](#_Toc116035830)

[2.3.3 Checklist to Support Compliance Verification 8](#_Toc116035831)

[2.4 Integrated eUICC Composite Certification 9](#_Toc116035832)

[Annex A Integrated eUICC Checklist (Informative) 10](#_Toc116035833)

[Annex B Integrated eUICC Security Requirements (Normative) 11](#_Toc116035834)

[B.1 General Security Requirements 11](#_Toc116035835)

[B.2 Security Certification Requirements 13](#_Toc116035836)

[B.3 Conformance Claims 13](#_Toc116035837)

[B.4 Security Objectives 13](#_Toc116035838)

[B.5 Security Functional Requirements 14](#_Toc116035839)

[Annex C Document Management 15](#_Toc116035840)

[C.1 Document History 15](#_Toc116035841)

[C.2 Other Information 16](#_Toc116035842)

# Introduction

## 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.

## Scope

This document describes the certification methodology for Integrated eUICC based on Protection Profile PP-0084[6].

The certification methodology for Integrated eUICC based on the the Protection Profile PP-0117 [20] is defined by SGP.18 [21].

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

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 programmes specified in [3] and [11].

## 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) |
| 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). |

## 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 |

## References

| Ref | Doc Number | Title |
| --- | --- | --- |
|  | [SGP.01] | Embedded SIM Remote Provisioning Architecture |
|  | [SGP.05] | Embedded UICC Protection Profile, also published by BSI as BSI-CC-PP-0089-2015 |
|  | [SGP.16] | M2M Compliance Process |
|  | [GSMA PRD AA.35] | Procedures for Industry Specifications |
|  | [RFC2119] | “Key words for use in RFCs to Indicate Requirement Levels,” S. Bradner  <http://www.ietf.org/rfc/rfc2119.txt> |
|  | 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) |
|  | 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) |
|  | JIL-CCCE | Joint Interpretation Library Composite product evaluation for Smart Cards and similar devices Version 1.5.1 May 2018 |
|  | [SGP.21] | RSP Architecture |
|  | [SGP.25] | GSMA Embedded UICC for Consumer Devices Protection Profile |
|  | [SGP.24] | RSP Compliance Process |
|  | PP-0100 | BSI-CC-PP-0100-2018 |
|  | NIST SP 800-108 | Recommendation for Key Derivation Using Pseudorandom Functions |
|  | BSI TR-02102-1 | Cryptographic Mechanisms: Recommendations and Key Lengths |
|  | ANSSI RGS v2 B1 | Référentiel Général de Sécurité version 2.0 Annexe B1 |
|  | NIST SP 800-175B | Guideline for Using Cryptographic Standards in the Federal Government: Cryptographic Mechanisms |
|  | NIST SP 800-53r4 | Security and Privacy Controls for Federal Information Systems and Organisations – Revision 4 |
|  | JIL-Application-of-Attack-Potential-to-Smartcards-v3-1 | Application of Attack Potential to Smartcards and Similar Devices  Version 3.1, Jun 2020 |
|  | SOG-IS | SOG-IS Smartcards and similar devices CC supporting documents at this link: https://www.sogis.eu/uk/supporting\_doc\_en.html |
|  | PP-0117 | BSI-CC-PP-0117-2022 Secure Sub-System in System-on-Chip (3S in SoC) Protection Profile |
|  | [SGP.18] | Security Evaluation of Integrated eUICC based on PP-0117 |

## 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].”

# Certification Process

## 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 Annex B.

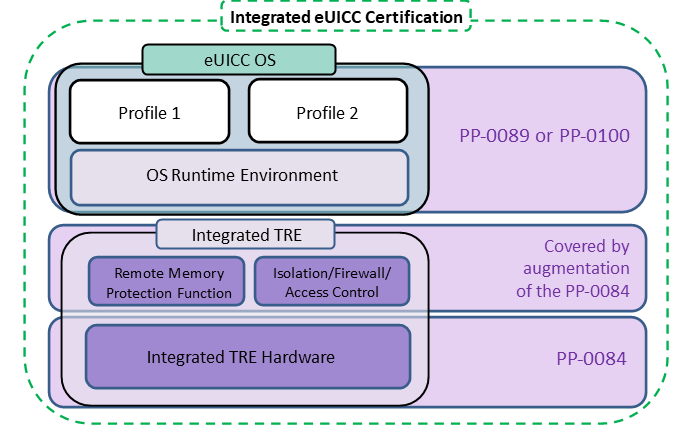
2. Composite certification of the Integrated eUICC SHALL be done:

* 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.

## 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 Annex B. 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 Annex B as part of the Security Target, as described below.



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 Annex B. The Integrated TRE MAY use an external Non Volatile Memory.

In such case, Annex B defines a Remote Memory Protection Function (RMPF) which SHALL be included within the Security Target of the Integrated TRE.

## Integrated TRE certification

### 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 B.

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



1. Security Target for the Integrated eUICC TRE, initial phase

### 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] or Annex J.5 of SGP.21 [9].

### 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 Annex B 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).

## 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]).

1. 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:**  ***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.* |  |  |  |
| … | … |  |  |  |

1. Integrated eUICC Security Requirements (Normative)

* 1. General Security Requirements

| Req no. | Description |
| --- | --- |
| **GS01** | An Integrated TRE MAY use a Remote Memory within the Device, dedicated to the Integrated TRE, to store software and data. |
| **GS02** | All Integrated eUICC software and data which are stored outside the Integrated TRE SHALL be protected by the Integrated TRE in order to ensure their confidentiality, their integrity, and software side channel protection.  This includes protection against side-channel attacks such as cache-timing attacks. |
| **GS03** | All Integrated TRE software and data, including context, SHALL only be stored in protected memory as requested in paragraph 36 in BSI-CC-PP-0084 [6]. |
| **GS04** | All Integrated TRE software and data stored outside an Integrated TRE SHALL be protected against replay attacks. |
| **GS05** | The Integrated TRE internal instruction and data buses SHALL be isolated from the rest of the SoC. |
| **GS06** | The other SoC components SHALL have no access to the Integrated TRE internal buses. |
| **GS07** | The Integrated TRE SHALL be the only entity to expose TRE data outside the Integrated TRE. |
| **GS08a** | All the credentials used to protect the data stored in the Remote Memory, dedicated to the Integrated TRE as per requirements GS02 and GS03**GS03**, SHALL only be stored and used in the Integrated TRE. |
| **GS09** | The Integrated TRE SHALL be isolated from all other SoC components such that no other SoC components can have access to assets inside the Integrated TRE. |
| **GS10** | The Integrated TRE SHALL have a hardware and software protection means that controls the access to every function of the Integrated TRE (e.g. cryptographic unit). |
| **GS11** | The Integrated TRE SHALL process/execute its data/software in a dedicated secure CPU contained within the Integrated TRE. |
| **GS12** | The Integrated TRE SHALL be resistant against hardware and software side-channel attacks (e.g. DPA, cache-timing attacks, EMA etc.). |
| **GS13** | All Integrated TRE software and data SHALL be exclusively processed within the Integrated TRE. |
| **GS14** | The Integrated TRE SHALL include in its security target the following threats for software and data managed by the TRE, but stored outside the TRE:   * leakage * probing * manipulation |
| **GS15** | The protection of software and data stored in Remote Memory as defined in GS02 SHALL be managed by the Integrated TRE using means which are independent of the Remote Memory implementation. |
| **GS16** | All cryptographic processing used by the Integrated TRE SHALL be contained within the Integrated TRE. |
| **GS17** | All security mechanisms within the Integrated TRE SHALL withstand state of the art attacks. |
| **GS18** | If Remote Memory outside the SoC is used, the combination of Integrated TRE and Remote Memory SHALL implement mechanisms protecting access to Remote Memory. |
| **GS19** | Integrated TRE implementations using Remote Memory outside the SoC SHALL implement mechanisms protecting the integrity of Remote Memory contents as defined in GS02. |

1. : General Security Requirements



1. : Example of Optional Remote Memory Usage

Note: IC Dedicated Software including its authentication by the TRE, is covered by BSI-CC-PP-0084 [6] and is not required to be augmented by this annex.

* 1. Security Certification Requirements

| Req no. | Description |
| --- | --- |
| **SC01** | An Integrated TRE together with the RMPF SHALL be evaluated according to BSI-CC-PP-0084 [6] augmented with the requirements defined in this annex.  Note: The requirements relating to Remote Memory and to RMPF are only applicable when that type of memory is used by the Integrated TRE. |
| **SC02** | Evidence of Isolation (for example GS05, GS06, GS07, GS09) SHALL be assessed during evaluation. |
| **SC03** | Evidence of proper Life Cycle management of the Integrated TRE SHALL be assessed during evaluation. |

1. : Security Certification Requirements
   1. Conformance Claims

| Req no. | Description |
| --- | --- |
| **CC01** | The Integrated TRE SHALL claim in its security target, that it comprises of Security IC and IC Dedicated Software regarded as a Security Integrated Circuit which implements all functional aspects specified by the BSI-CC-PP-0084 [6] Protection Profile augmented with the requirements defined in this Annex. |
| **CC02** | The Integrated TRE SHALL provide resistance to attackers with “high” attack potential as defined by AVA\_VAN.5 and ALC\_DVS.2 in [18]. |
| **CC03** | The Integrated TRE SHALL be evaluated against the requirements, methods of attacks and evaluation documents for smartcards and similar devices published by SOG-IS [19]. |

1. : Conformance Claims
   1. Security Objectives

BSI-CC-PP-0084 [6] defines security problems related to the Security IC being evaluated and corresponding security objectives. Within BSI-CC-PP-0084 [6], the definitions do not take into account the implementation of the TRE within a SoC and the use of Remote Memory. In particular, Integrated TRE has to include additional security problems and objectives in its security target. The security target shall include the following in its security objectives:

| Req no. | Description |
| --- | --- |
| **SO01** | The Integrated TRE SHALL define, in its security target, a security objective to protect software and data managed by the TRE and stored outside the TRE against:   * leakage * probing * manipulation |

1. : Security Objectives
   1. Security Functional Requirements

| Req no. | Description |
| --- | --- |
| **IESFR01** | An Integrated TRE that uses Remote Memory SHALL implement a Remote Memory Protection Function (RMPF) to protect software and data to be stored in Remote Memory, outside the TRE. |
| **IESFR02** | The RMPF SHALL reside in the Integrated TRE. |
| **IESFR03** | The RMPF SHALL ensure the following security properties: (1) confidentiality (2) integrity and (3) replay-protection.  Note: these properties are intended to cover a range of possible attacks, including replay of commands on the Remote Memory, rollback of data stored in the Remote Memory, cloning the content of a Remote Memory from another device, swapping or corrupting data within the Remote Memory, etc. |
| **IESFR04** | The RMPF SHALL use keys that are either:   * derived from a secret TRE-unique seed(s), or; * randomly generated within the Integrated TRE |
| **IESFR05** | TRE-unique seed(s) used by RMPF SHALL be generated using a certified random number generator as required by BSI-CC-PP-0084 [6]. |
| **IESFR06** | TRE-unique seed(s) used by the RMPF SHALL be generated inside the TRE. |
| **IESFR07** | The entropy of the TRE-unique seed(s) used by the RMPF SHALL be at least 256 bits. |
| **IESFR08** | Randomly generated keys used by the RMPF shall be at least 256 bits. |
| **IESFR09** | The key derivation mechanism used by the RMPF SHALL be compliant with NIST SP 800-108 [13] 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, |
| **IESFR10** | The keys used by the RMPF SHALL be protected by the TRE. |
| **IESFR11** | Seed(s) used by the RMPF SHALL be restricted to the RMPF. |
| **Confidentiality Requirements** | |
| **IESFR12** | 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 [16] or recommended by BSI in BSI TR-02102-1 [14] or recommended by ANSSI RGS v2 B1 [15]. |
| **Integrity and Authenticity** | |
| **IESFR13** | The RMPF SHALL use a cryptographic integrity mechanism with security strength equivalent to, or greater than SHA-256. |
| **IESFR14** | 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 [16] or recommended by BSI in BSI TR-02102-1 [14] or recommended by ANSSI RGS v2 B1 [15]. |
| **IESFR15** | IESFR12 and IESFR14 MAY also be provided in combination by an authenticated encryption mode fulfilling both requirements. |
| **Replay protection** | |
| **IESFR16** | The RMPF SHALL detect any replay attack on the Integrated TRE. |
| **IESFR17** | The Integrated eUICC SHALL be resistant to replay attacks on the data stored in Remote Memory. |
| **IESFR18** | The Integrated eUICC SHALL be able to verify that the data received from the Remote Memory is not unsolicited.  Note: Solicited data received from the Remote Memory is data that the Integrated eUICC did intend to retrieve at runtime from Remote Memory and/or retrieved data that the Integrated eUICC was able to verify according to the requirements set in this Annex. |
| **IESFR19** | The RMPF SHALL NOT process data if it is unable to detect a replay attack.  Note: Such a situation may arise e.g. if the RMPF uses a counter to detect replay attacks and the counter expired or became unreliable for any other reason. |
| **Test Interface** | |
| **IESFR20** | The Integrated eUICC Test Interface SHALL NOT affect the security requirements defined in this annex. |

1. : Security Functional Requirements
2. Document Management
   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 |
| V1.1 | 30/06/2021 | CR008R00 - Make SGP.08 applicable to GSMA RSP (Consumer) products | ISAG | Gloria Trujillo, GSMA |
| V1.2 | 19/09/2022 | CR0010R01 - Streamlining Annex J and G | ISAG | Gloria Trujillo, GSMA |

* 1. 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](mailto:prd@gsma.com)

Your comments or suggestions & questions are always welcome.