

Security Accreditation Scheme - Consolidated Security Requirements and Guidelines

Perso\_SC Clarification Change Request to Version 7.1 DRAFT v01

This 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 © 2022 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.

…

# Introduction



…

## Definitions

| Term | Description |
| --- | --- |
| … | |
| Discrete eUICC | An eUICC implemented on discrete standalone hardware, including its own dedicated volatile and non-volatile memory. |
| … | |
| eUICC | A 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 an Integrated TRE |
| Integrated TRE | A TRE implemented inside a larger System-on-Chip (SoC), optionally making use of remote volatile and/or non-volatile memory. |
| … | |
| Tamper Resistant Element (TRE) | 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. |
| … | |

…

| Requirement Statements | | |  | | Guidelines | |
| --- | --- | --- | --- | --- | --- | --- |
| 1. Two-Step Personalisation Process | | |  |  | |  |
|  | Personalisation may be carried out as a two-step process (Perso\_SC and Perso\_UICC). The process may involve a different entity in each step.  SAS-UP requirements apply to both Personalisation steps. SAS-UP certification must be applied to each step for UICC production flows requiring SAS-UP compliance (e.g. eUICC).  SAS-UP assessment of two-step Personalisation process can currently only be applied to the following product types:   * Integrated eUICC | |  |  | | Requirements for the two-step Personalisation process are not intended to apply where the full Personalisation process takes place in the same physically-secure EUM environment. Requirements in this section have been added to enable SAS-UP to support products, such as Integrated eUICC, where the two Personalisation steps may be carried out at different times, potentially in different environments under the control of different entities.  Both the Perso\_SC and Perso\_UICC processes should each always be carried out under the overall control of an SAS-UP certified entity. Each operation may be conducted:  At a physically certified SAS-UP location in all cases.  At a remote location only in cases where the requirements of 11.3.3 (for Perso\_SC) or 11.5.2 (for Perso\_UICC) are met.  Production processes for product types other than those listed in this requirement are not currently supported for SAS-UP certification, although this may change in the future.  Auditees involved in the eUICC production chain will be expected to demonstrate that the combined solution is secure. |
|  |  | Control of duplicate production |  |  | |  |
|  |  | Each Personalisation step shall incorporate controls to ensure that:   * Personalisation Data is only used once. * Creation of duplicate devices containing the same Personalisation Data is prevented. |  |  | | Auditees should demonstrate controls for preventing duplicate production. Personalisation Data for each eUICC should exist and be used in exactly one instance. A mechanism should be implemented to prevent the duplicate use of Personalisation Data. |
|  |  | Generation of hardware security credentials |  |  | |  |
|  |  | The generation of hardware security credentials, and their provisioning into the device hardware shall be considered a sensitive process, and be evaluated according to the requirements in section 7 of this document. |  |  | | Auditees must demonstrate that hardware credentials are generated and provisioned in a secure manner.  Credentials should be generated using security modules (HSM) that are FIPS 140-2 level 3 certified.  Where generation and provisioning to Integrated eUICC hardware occur in separate facilities, a secure exchange mechanism should be in place. |
|  |  | Generation of hardware security credentials shall be carried out by one of the following: |  |  | | Only credentials generated in accordance with SAS-UP requirements can be used for Perso\_UICC. |
|  | (i) | **Generation of all information, including sensitive information, outside the TRE.**  Generation shall always take place:   * At an SAS-UP certified location. * Under the control of an SAS-UP certified entity. |  |  | | Generation outside of the TRE must always be carried out at an SAS-UP certified location to ensure that the security of the data is assured during generation, storage and exchange of the data. |
|  |  | Or |  |  | |  |
|  | (ii) | **Generation of sensitive information inside the TRE and processing of non-sensitive information outside the TRE.**  Generation of sensitive information shall always take place:   * Within a TRE device that has a generation mechanism (i.e. RNG) which is FIPS 140-3 level 2 certified. * Under the control of an SAS-UP certified entity.   At an SAS-UP certified location in those cases where the process relies on security of either the physical or logical environment of the TRE at the time of generation. |  |  | | Generation inside the TRE may take place at a location that is not SAS-UP certified.  In this case the auditees are expected to demonstrate that:   * The process can only take place under the control of an SAS-UP certified entity (e.g. triggered by authenticated message from the SAS-UP certified entity). * Data that is exchanged with the TRE is protected during the personalisation of the hardware credentials according to the requirements of 11.3.3.   The process may be permitted to take place at a location that is not SAS-UP certified only if the entity controlling the process is able to demonstrate independence from the security of the physical or logical environments where the process takes place. If specific requirements apply to the solution that depend on security of the physical or logical environment, then that environment will be required to be SAS-UP certified.  Participants are encouraged to contact GSMA in advance of applying for SAS-UP certification to ensure that the correct audit approach is selected. |
|  |  | Personalisation of security credentials (Perso\_SC) |  |  | |  |
|  |  | The Personalisation of a hardware device with security credentials shall be considered a sensitive process, and be evaluated according to the requirements in section 7 of this document. |  |  | | Auditees should demonstrate that hardware credentials are provisioned in a secure manner. |
|  |  | Perso\_SC can occur only once within the device lifecycle. |  |  | | Auditees should demonstrate that hardware credentials can be used only once. |
|  |  | Personalisation of hardware security credentials shall be carried out: |  |  | | Only credentials personalised in accordance with SAS-UP requirements can be used later for Perso\_UICC. |
|  | (i) | **In cases where of all information, including sensitive information, is generated outside the TRE.**  Personalisation shall always take place:   * At an SAS-UP certified location. * Under the control of an SAS-UP certified entity. |  |  | | See 11.2.2(i). |
|  |  | Or |  |  | |  |
|  | (ii) | **In cases where sensitive information is generated inside the TRE and processing of non-sensitive information outside the TRE.**  Personalisation shall always take place:   * Under the control of an SAS-UP certified entity. * At an SAS-UP certified location in those cases where the process relies on security of either the physical or logical environment of the TRE at the time of generation. |  |  | | Where sensitive information is generated inside the TRE, the “personalisation” and “data generation” activities for Perso\_SC are considered to be conducted concurrently. In this context, “personalisation” considers the overall process, including the exchange of data with the TRE. “Data generation” is the process (or processes) by which data is generated inside the TRE.  See 11.2.2(ii). |
|  |  | In all cases, for personalisation of security credentials, communications between the entity controlling Perso\_SC and the TRE shall always be secured to ensure:   * Authenticity * Confidentiality * Replay protection |  |  | | Security controls may be defined and applied in different ways according to:   * How the process is conducted. * Inside or outside the TRE. * Where the process is conducted. * Under the direct control of SAS-UP certified entity performing the operation. * Remotely. * What data must be exchanged with the TRE during the process. * Auditees will be expected to demonstrate that the controls are appropriate. |
|  |  | Generation of UICC OS credentials |  |  | |  |
|  |  | The generation of UICC OS credentials shall be considered a sensitive process and be evaluated according to the requirements in section 7 of this document. |  |  | | Auditees should demonstrate that OS credentials are generated and in a secure manner.  Credentials should be generated using security modules (HSM) that are FIPS 140-2 level 3 certified. |
|  |  | Personalisation of UICC OS credentials (Perso\_UICC) |  |  | |  |
|  |  | Generated UICC OS credentials shall be provisioned to authenticated hardware instances that have previously been personalised with security credentials in a Perso\_SC process that has been SAS-UP certified. |  |  | | Auditees should demonstrate that OS credentials are to be provisioned only to authenticated Integrated eUICC hardware that has been personalised as part of an SAS-UP certified process.  Auditee may include in such demonstration mechanisms based on cryptographic means and legal obligations. |
|  |  | Personalisation of UICC OS credentials to a device shall be carried out by establishing a secure channel that: |  |  | | [11] 7.3.2, Package 2: Loader defines a set of security requirements for as part of a protection profile.  Auditees should demonstrate that:   * The OS credentials provisioning process, combined with capabilities provided by the Integrated eUICC hardware manufacturer satisfy requirements equivalent to those described in Package 2: Loader. * The means to establish a secure channel is rooted in a certified part of the target hardware. * The communication channel itself is secure. * The service it provides is secure. * The combined solution is secure. * The hardware includes the additional authentication requirements of [11] 7.2 Authentication of the Security IC. |
|  | (i) | Utilises unique security credentials personalised to the device in the Perso\_SC step. |  |  | |
|  | (ii) | Can only be initiated by an appropriately authorized entity in possession of the security credentials. |  |  | |
|  | (iii) | Enforces:   * Mutual authentication. * Confidentiality. * Replay protection. |  |  | |
|  |  | The Personalisation process shall ensure that: |  |  | |
|  | (i) | UICC OS credentials are provisioned only to pre-determined secure locations within the device. |  |  | |
|  | (ii) | UICC OS credentials are protected within the device after Personalisation to prevent disclosure and manipulation. |  |  | |

1. Document Management
   1. Document History

|  |  |  |  |
| --- | --- | --- | --- |
| Version | Date | Brief Description of Change | Editor / Company |
| 1.0 | 26 Jul 2016 | Created based on SAS-UP Guidelines document v5.0. Added Certificate Management requirements and PKI Certificate Policy security requirements. | James Messham, FML |
| 2.0 | 31 Mar 2017 | Incorporated SAS-SM requirements, including SM-DP+ and SM-DS. | RSPSAS subgroup |
| 2.1 | 2 Jan 2018 | Updated guidelines on external network connections (section 10.4.2) | SAS subgroup |
| 3.0 | 26 Jun 2019 | Added two-step personalisation process (Integrated eUICC) guidelines.  Added guidance on use of a single HSM platform for EUM and SM functions and network separation at such sites.  Added guidance on SM solution demonstration expectations. | Or Elnekaveh, Qualcomm James Messham, FML  Neil Shepherd, NCC Group |
| 4.0 | 25 Jul 2019 | Added guidelines for transfer of sensitive assets between sites. | SAS subgroup |
| 5.0 | 18 Jun 2020 | Development of remote user access guidelines | SAS subgroup |
| 6.0 | 20 Nov 2020 | Add specific guidelines for auditing of cloud service providers. | SAS subgroup |
| 7.0 | 2 Jul 2021 | Add guidelines for new requirement at 2.4.2 – clarify subcontractor responsibilities | James Messham, FML & Neil Shepherd, SRC |
| 7.1 | 22 Sep 2021 | Clarifications to HSM guidelines. Addition of SAS-UP definitions. | Saïd Gharout, Kigen |
| CR DRAFT v0.1 | 1 Feb 2022 | Terms alignment on implementation choices of Perso\_SC | Or Elnekaveh, Qualcomm,  James Messham, FML |

* 1. Other Information

|  |  |
| --- | --- |
| Type | Description |
| Document Owner | GSMA Fraud and Security Group |
| Editor / Company | David Maxwell, 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 [sas@gsma.com](mailto:sas@gsma.com).

Your comments or suggestions & questions are always welcome.