SAS for UICC Production (SAS-UP) Scope Definitions
Version 2.0
16 Sep 2021

Security Classification: Non-Confidential

Copyright Notice

Disclaimer

Antitrust Notice

The information contain herein is in full compliance with the GSM Association's antitrust compliance policy.

Table of Contents

1 Introduction

1.1 Overview

This document provides definitions of each of the following areas of scope in which a site participating in SAS for UICC Production (SAS-UP) may gain accreditation.

- Generation of data for personalisation;
- Personalisation;
- Management of PKI certificates, and
- Post-personalisation packaging.

These are current definitions and applicable scopes. Definitions will be updated and scopes extended as appropriate.

1.2 Abbreviations

Term	Description
2FF	2nd Form Factor ("Mini SIM")
3FF	3rd Form Factor ("Micro SIM")
4FF	4th Form Factor ("Nano SIM")
ECASD	Embedded UICC Controlling Authority Security Domain
eUICC	Embedded Universal Integrated Circuit Card
GSMA	GSM Association
ISD-R	Issuer Security Domain - Root
M2M	Machine-to-Machine
MFF	Machine-to-Machine Form Factor
OEM	Original Equipment Manufacturer
Perso_SC	Personalisation – security credentials (2-step personalisation – see below)
Perso_UICC	Personalisation – UICC OS credentials (2-step personalisation – see below)
PKI	Public Key Infrastructure
RSP	Remote SIM Provisioning
SD (Card)	Secure Digital (Card)
UICC	Universal Integrated Circuit Card
VQFN	Very-Thin Quad Flat-Pack, No-Leads
WLCSP	Wafer-Level Chip Scale Package

2   Generation of data for personalisation

Definition	Scope Options			
	UICC	**eUICC**	**2-step personalisation: Perso_SC**	**2-step personalisation: Perso_UICC**
Generation of personalisation data refers to the generation of any data that is to be encoded into a device intended to act as a UICC/eUICC to make it uniquely identifiable. This data may be: • Unique security keys that control future access to the device; • An Embedded UICC Controlling Authority Security Domain (ECASD) and Issuer Security Domain - Root (ISD-R), and/or • MNO profile data. The generated data may be used to personalise UICCs at the certified site, or at another site.	Generates data for conventional UICCs only. Will typically process customer-generated input files to produce personalisation data and customer response data.	Generates data for eUICCs, including the generation of individual eUICC certificates and data files for subscription management.	Generates unique hardware security credentials for the target device for use in the first step of a 2-step personalisation process. The two personalisation steps may be carried out at different times, in different environments, under the control of different entities. Perso_SC takes place under the direct logical and physical control of SAS-UP certified sites. The security credentials from Perso_SC are used to enable the Perso_UICC step to be carried out remotely under the logical control of an SAS-UP certified site.	Generates UICC OS credentials for use in the second step of a 2-step personalisation process,

3   Personalisation

Definition	Scope Options				
	Card	**Embedded**	**Wafer**	**Perso_SC**	**Perso_UICC**
Personalisation is the process of encoding each device intended to act as a UICC/eUICC with the information (personalisation data) generated during the data	Personalises card form-factor UICCs/eUICCs. Typically includes standard	Personalises embedded form factor UICCs/eUICCs. Typically includes	Personalises UICCs/eUICCs in parallel at wafer level, normally as part of wafer testing.	Personalises a target device with unique hardware security credentials as the first step of a 2-step	Personalises an authenticated hardware device as a UICC using UICC OS credentials. The

Definition	Scope Options				
	Card	**Embedded**	**Wafer**	**Perso_SC**	**Perso_UICC**
generation process. The table indicates the form factor(s) of the devices that are personalised. Personalisation may be carried out using data generated at the certified site, or at another site.	ID1/2FF/3FF/4FF cards/plug-ins/repluggable form-factors designed to be user-removable, but can be extended to non-standard user-removable form-factors such as SD cards.personalisation data and customer response data.	MFF2/VQFN8 silicon packages and similar small-form factors designed to be solder- or socket-mounted directly onto circuit boards and are not designed to be user-removable.	Dies from personalised wafers will typically be used to produce WLCSP packages that can be directly mounted onto circuit boards.	personalisation process.	authenticated hardware instance must have previously been personalised with security credentials in a Perso_SC process that has been SAS-UP certified.
				The two personalisation steps may be carried out at different times, potentially in different environments under the control of different entities. Perso_SC takes place under the direct logical and physical control of SAS-UP certified sites to enable a second Perso_UICC step to be carried out remotely under the logical control of an SAS-UP certified site.	

4   Management of PKI certificates

Definition	Scope Options	
	GSMA PKI Ready	**GSMA PKI LIve**
Management of PKI certificates is the process of: • Securely generating a key pair and certificate signing request and submitting this to a recognised certificate authority / issuer. • Securely storing the key pair and certificate and making them available under	✓ Has appropriate controls in place for issue of certificate(s) as part of the GSMA PKI from one of the Association's certificate issuers.	✓ As for GSMA PKI Ready, except that site has demonstrated compliant controls with GSMA PKI certificate(s) in use.

Definition	Scope Options	
	GSMA PKI Ready	**GSMA PKI LIve**
appropriate control for the generation of eUICC certificates. The scope statement refers only to the management of the key pair and certificate; the process of generating individual eUICC device certificates is included within the scope of "Generation of data for personalisation / eUICC".	Audit assessment was made based on use by the site of non-GSMA PKI certificates, either via (a) test/self-signed PKI certificates (controls audited 'dry', i.e. no live operations) or (b) certificates used in live operations issued by non-GSMA CAs. Where the key pair and certificate are used by a site SAS-UP certified for "Generation of data for personalisation / eUICC" then the resulting eUICC certificates will be accepted as part of the GSMA's PKI for M2M/RSP as appropriate.	

5 Post-personalisation packaging

Definition	Scope Options[1]	
	Card	**Wafer**
Post-personalisation packaging is the process of performing some value-added operation on personalised UICC/eUICC.	Machine wrapping or manual processing of personalised UICCs into retail or customer packages. May include standard or customer-specific wrapping or packaging design. Certified sites will have demonstrated appropriate controls for end-to-end asset management and reconciliation.	Processing of personalised wafers into individual dies and packaging into reel-tape or other medium for delivery to the customer or OEM integrator. May include additional processing steps for each wafer. Will include identification and separation of good and bad UICCs from the wafer, with a responsibility to reconcile and report on good UICCs included within the output medium.

---

[1] "Embedded" is not included as a scope option, as post-personalisation packaging of embedded form-factor UICCs does not normally occur as a separate production activity.

Annex A   Document Management

A.1   Document History

Version	Date	Brief Description of Change	Editor / Company
1.0	5 Sep 2018	First version	James Messham, FML
1.1	27 Apr 2021	PKI certificate management designations updated based on approved changes to FS.05.	David Maxwell, GSMA
2.0	14 Sep 2021	Added 2-step personalisation.	David Maxwell, GSMA & James Messham, FML

It is our intention to provide a quality product for your use. If you find any errors or omissions, please contact sas@gsma.com.