Security Accreditation Scheme for UICC Production - Standard

Version 9.3

19 July 2024

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 4
1.1 Overview 4
1.2 Background 4
1.3 Scope 4
1.4 Intended Audience 5
1.5 Related Documents 5
1.6 Definitions 6
1.7 Abbreviations 6
1.8 References 7
1.9 Conventions 8
2 Process and Scope Definitions 9
2.1 Product Lifecycles 9
2.1.1 UICC 9
2.1.2 eUICC 10
2.2 Scope of Certification 10
2.2.1 Generation of Data for Personalisation 11
2.2.2 Personalisation 11
2.2.3 Management of PKI Certificates 12
2.2.4 Post-Personalisation Packaging 13
3 The Process Models 14
3.1 The Actors 15
4 The Assets 15
4.1 Introduction 15
4.2 Assets Classification 16
4.3 Asset Characteristics 16
4.4 Incoming Sensitive Components (ISC) 16
4.5 Partly Finished Products (PFP) 16
4.6 Finished Products (FIN) 16
4.7 Personalisation Rejects (PRJ) 17
4.8 Sensitive information (SEN) 17
4.9 Cryptographic Keys (KEY) 18
5 The Threats 18
5.1 Introduction 18
5.2 Direct Threats Description 18
5.3 Indirect Threats Description 19
5.4 Application of Threats in the Process 19
6 Security Objectives 20
6.1 Introduction 20
6.2 Security Objectives for the Sensitive Process 20
6.3 Security Objectives for the Environment 20
7 Security Requirements 21
Annex A Assets 22

Annex B Document Management 24
B.1 Document History 24
B.2 Other Information 25

1 Introduction

1.1 Overview

The GSMA Security Accreditation Scheme for UICC Production (SAS-UP) is a voluntary scheme through which UICC suppliers (including eUICC and Integrated eUICC suppliers) subject their operational sites to a comprehensive security audit to ensure that adequate security measures to protect the interests of mobile network operators (MNO) have been implemented.

MNOs are dependent on suppliers to control risks; to ensure that adequate security is in place. Confidence is improved by the introduction of an auditable SAS Standard, which can be applied consistently to UICC suppliers. The purpose of the SAS-UP Standard is to:

- Minimise risks to MNOs introduced by UICC production (including eUICC and Integrated eUICC production).
- Provide a set of auditable requirements, together with the SAS Consolidated Security Requirements and Guidelines [2] and the SAS-UP Methodology [1], to allow UICC suppliers to provide assurance to their customers that risks are controlled.
- Support SAS for Subscription Management (SAS-SM) by facilitating the accreditation of UICC suppliers producing eUICCs or Integrated eUICCs and maintaining associated interfaces to entities performing subscription management roles.

Security objectives applicable to UICC suppliers are herein outlined.

NOTE: All references to UICCs and UICC suppliers in this document apply equally to Discrete eUICCs or Integrated eUICC and eUICC or Integrated eUICC suppliers unless specifically stated otherwise.

1.2 Background

This SAS-UP Standard and related documents have been created and developed within GSMA through collaboration between representatives from MNOs, UICC suppliers and the GSMA-appointed auditing companies. The GSMA is responsible for updating the SAS Standard. A review of the scheme and its documentation takes place with MNOs, UICC suppliers and the appointed auditors annually.

1.3 Scope

Sites eligible for auditing include only those carrying out activities within the scope of this document, as follows:

- Generation of personalisation data for UICCs
- UICC personalisation
- Value-added fulfilment of UICCs
- Processing of data for subscription management

The security objectives have been achieved by defining:

- UICC production life cycle and processes
- Assets to be protected

- Risk and threats
- Security requirements.

This document is not intended to be a UICC production protection profile.

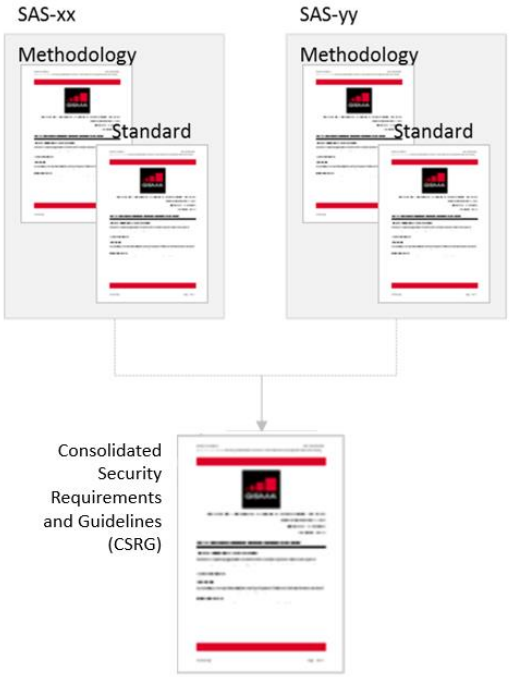
To further reduce the risks for MNOs, it is acknowledged that the security objectives must continue to be met after the personalisation phases where the supplier is responsible for delivery.

1.4 Intended Audience

- Security professionals and others within UICC supplier organisations seeking to obtain accreditation under SAS-UP.
- Security professionals and others within organisations seeking to procure UICCs
- SAS Certification Body members
- SAS-UP auditors

1.5 Related Documents

This document is part of the Security Accreditation Scheme documentation published by the GSMA. Documentation is structured as follows:



Each SAS scheme comprises a **Methodology** and **Standard** relevant to Sensitive Processes (SPs) that should be protected**.**

The **Methodology** describes the purpose of the scheme and how it is administered.

The **Standard** describes the security objectives related to the relevant SPs.

The **Consolidated Security Requirements and Guidelines (CSRG)** describe all of the security requirements that may apply to SPs in the different SAS schemes, and provides examples of how the security requirements may be achieved.

Figure 1 - SAS Documentation Structure

The accreditation schemes and documents are designed such that multiple schemes may utilise the same Consolidated Security Requirements and Guidelines.

The security objectives described in this document are supported by the GSMA SAS Methodology for UICC Production [1] and the GSMA SAS Consolidated Security Requirements and Guidelines [2].

1.6 Definitions

Term	Description
Actor	Person who is involved in, or can affect, the Sensitive Process
Business Continuity	Capability of a UICC supplier to continue production at acceptable predefined levels (as determined by customer requirements) following a failure incident.
Common Criteria	Criteria used as the basis for evaluation of security properties. The evaluation results help in determining whether or not the product is secure
Duplicate	Two or more assets of the same nature showing a set of information that should be individual according to the correct process
Employee	An individual who works part-time or full-time under a contract of employment, whether oral or written, express or implied, and has recognized rights and duties. Also called worker.
Environment	Environment of use of the sensitive process limited to the security aspects
eUICC	A UICC which is not easily accessible or replaceable, is not intended to be removed or replaced in a device, and enables the secure changing of profiles. Note: The term originates from "embedded UICC".
Integrated eUICC	An eUICC managing Operator credentials, that is integrated into a larger chip, such as a System-on-Chip (SoC). It is implemented on an integrated Tamper Resistant Element (TRE); a certified secure element using the Common Criteria PP-0084 Protection Profile, augmented to support remote memory. It operates as an eUICC conforming to GSMA SGP.01/02/21/22 eSIM specifications.
Key	Refers to any logical key (e.g. cryptographic key)
Physical key	Any key and/or combination used for opening a physical lock (e.g. a door, vault, safe or secure cabinet)
Reject	Finished or partially finished product containing sensitive information which has been ejected from the process.
Sensitive Process	The security evaluation field, covering the processes and the assets within those processes
UICC	A smart card that conform to the specification written and maintained by the ETSI Smart Card Platform.

1.7 Abbreviations

Term	Description
2FF	2nd Form Factor (“Mini SIM”)
3FF	3rd Form Factor (“Micro SIM”)
4FF	4th Form Factor (“Nano SIM”)
ASI	Additional Sensitive Information
CSR	Consolidated Security Requirements and Guidelines
ECASD	eUICC Controlling Authority Security Domain
EIS	eUICC Information Set
FIN	Finished Products
FS.nn	Prefix identifier for official documents belonging to GSMA Fraud and Security Group

Term	Description
GSMA	GSM Association
ISD-R	Issuer Security Domain - Root
ISC	Incoming Sensitive Components characterise the process sensitive inputs such as information, products, files, keys, etc.
ISI	Incoming Sensitive Information characterise the process sensitive inputs such as requests, files and keys.
IT	Information Technology
M2M	Machine-to-Machine
MFF	Machine-to-Machine Form Factor
MNO	Mobile Network Operator
OEM	Original Equipment Manufacturer
OSI	Outgoing Sensitive Information characterise the process sensitive outputs such as responses, files and keys.
Perso_SC	Personalisation – security credentials (2-step personalisation – see below)
Perso_UICC	Personalisation – UICC OS credentials (2-step personalisation – see below)
PFP	Party Finished Products
PKI	Public Key Infrastructure
PRJ	Personalisation Rejects
RSP	Remote SIM Provisioning
SEN	Sensitive Information
SAS	Security Accreditation Scheme
SAS-SM	Security Accreditation Scheme for Subscription Management Roles
SAS-UP	Security Accreditation Scheme for UICC Production
SD (Card)	Secure Digital (Card)
SGP.nn	Prefix identifier for official documents belonging to GSMA SIM Group
SM-DP	Subscription Manager – Data Preparation
SM-DP+	Subscription Manager – Data Preparation (Enhanced compared to the SM-DP in SGP.02 [6])
SM-SR	Subscription Manager – Secure Routing
SP	Sensitive Process
VQFN	Very-Thin Quad Flat-Pack, No-Leads
WLCSP	Wafer-Level Chip Scale Package

1.8 References

Ref	Doc Number	Title
[1]	PRD FS.05	GSMA SAS Methodology for UICC Production, latest version available at www.gsma.com/sas
[2]	PRD FS.18	GSMA SAS Consolidated Security Requirements and Guidelines, available at www.gsma.com/sas
[3]	RFC 2119	“Key words for use in RFCs to Indicate Requirement Levels”, S.

Ref	Doc Number	Title
		Bradner, March 1997. Available at http://www.ietf.org/rfc/rfc2119.txt

The following additional references apply only in the context of the eUICC.

Ref	Doc Number	Title
[4]	PRD SGP.01	Embedded SIM Remote Provisioning Architecture
[5]	PRD SGP.02	Remote Provisioning Architecture for Embedded UICC Technical Specification
[6]	PRD SGP.21	RSP Architecture
[7]	PRD SGP.22	Remote SIM Provisioning (RSP) Architecture for consumer Devices

1.9 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 [3].”

2 Process and Scope Definitions

The UICC and eUICC product life-cycles can be broken down into a number of phases as shown below.

In each case the SAS-UP Standard is defined only for activities within the phases marked for each product lifecycle. Remote provisioning and management of the eUICC is out of the scope of this Standard.

2.1 Product Lifecycles

2.1.1 UICC

	#	Title	Description
	1.	Software development	Basic software and operating system development; application software development, integration and validation
	2.	IC design	IC development; hardware development, initialisation and test program development, integration and validation, initialisation of identification information and delivery keys
	3.	Production	Manufacture, assembly and testing of the device to be personalised.
Scope of SAS-UP	4.	Data generation	Receipt and processing of input data; production data generation and preparation; output data generation; preparation and transfer.
Scope of SAS-UP	5.	Personalisation	Receipt and management of physical assets for personalisation; electronic and graphical personalisation of assets using production data; packaging and delivery. Re-work of defective or reject personalised assets. Secure destruction of defective or rejected assets.
	6.	User	Commences when the network operator takes responsibility for the personalised device. Includes the operator's storage, distribution and activation of the device and subsequent use by the customer.
	7.	End-of-life	When the card reaches a stage where it can no longer perform the functions for which it was produced

Table 1 - UICC Product lifecycle

2.1.2 eUICC

	#	Title	Description
	1.	Software development	Basic software and operating system development; application software development, integration and validation
	2.	IC design	IC development; hardware development, initialisation and test program development, integration and validation, initialisation of identification information and delivery keys
	3.	Production	Manufacture, assembly and testing of the device to be personalised.
Scope of SAS-UP	4.	Certificate generation	Generation of key pair; generation of certificate signing request (CSR) and submission to certificate issuer (CI). Secure distribution of certificate private key to production environment. (For example: generation of the EUM PKI key pairs, signing by a GSMA CI and distribution of the private key for generation of eUICC device certificates as part of data generation).
Scope of SAS-UP	5.	Data generation	Receipt and processing of profile input data; production data generation; device certificate key pair generation and signing; production data preparation; output data generation, preparation and transfer.
Scope of SAS-UP	6.	Personalisation	Receipt and management of physical assets for personalisation; electronic and graphical personalisation of assets using production data; packaging and delivery. Re-work of defective or reject personalised assets. Secure destruction of defective or rejected assets.
	7.	Integration	Integration of the eUICC into the host device in a removable or permanently-installed form-factor.
	8.	User	Commences when the network operator takes responsibility for the personalised device through activation of a profile.
	9.	End-of-life	When the eUICC or host device reaches a stage where it can no longer perform the functions for which it was produced

Table 2 - eUICC Product Lifecycle

2.2 Scope of Certification

For each of the scope elements identified in 2.1, the scope of certification for the site has a number of options as described below.

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

2.2.1 Generation of Data for Personalisation

Scope	Generation of data for personalisation
Definition	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 my be used to personalise UICCs at the certified site, or at another site.
Scope options	
UICC	Generates data for conventional UICCs only. Will typically process customer-generated input files to produce personalisation data and customer response data.
eUICC	Generates data for eUICCs, including the generation of individual eUICC certificates and data files for subscription management.
2-step personalisation:	
For 2-step personalisation, the 2 steps may be carried out at different times, in different environments, under the control of different entities and are certified separately.	
Perso_SC	Generates unique hardware security credentials for the target device for use in the first step of a 2-step personalisation process.
Perso_UICC	Generates UICC OS credentials for use in the second step of a 2-step personalisation process,
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.	

2.2.2 Personalisation

Scope	Personalisation
Definition	Personalisation is the process of encoding each device intended to act as a UICC/eUICC with the information (personalisation data) generated during the data 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.
Scope options	
Card	Personalises card form-factor UICCs/eUICCs. Typically includes standard 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.
Embedded	Personalises embedded form factor UICCs/eUICCs. Typically includes 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.
Wafer	Personalises UICCs/eUICCs in parallel at wafer level, normally as part of wafer

	testing. Dies from personalised wafers will typically be used to produce WLCSP packages that can be directly mounted onto circuit boards.
2-step personalisation:	
For 2-step personalisation, the 2 personalisation steps may be carried out at different times, potentially in different environments under the control of different entities.	
Perso_SC	Personalises a target device with unique hardware security credentials as the first step of a 2-step personalisation process.
Perso_UICC	Personalises an authenticated hardware device as a UICC using UICC OS credentials. The authenticated hardware instance must have previously been personalised with security credentials in a Perso_SC process that has been SAS-UP certified.
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.	

2.2.3 Management of PKI Certificates

Scope	Management of PKI certificates
Definition	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 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".
Scope options	
GSMA PKI Ready	Has appropriate controls in place for issue of certificate(s) as part of the GSMA PKI from one of the Association's certificate issuers. 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.
GSMA PKI Live	As for GSMA PKI Ready, except that site has demonstrated compliant controls with GSMA PKI certificate(s) in use.

2.2.4 Post-Personalisation Packaging

Scope	Post-personalisation packagaing
Definition	Post-personalisation packaging is the process of performing some value-added operation on personalised UICC/eUICC.
Scope options[1]	
Card	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.
Wafer	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.

3 The Process Models

The life cycle is used to depict the security target implementation. The representation of the steps within the process is based on product and data flows. All possible combinations are not described and chronological order is not necessarily represented.

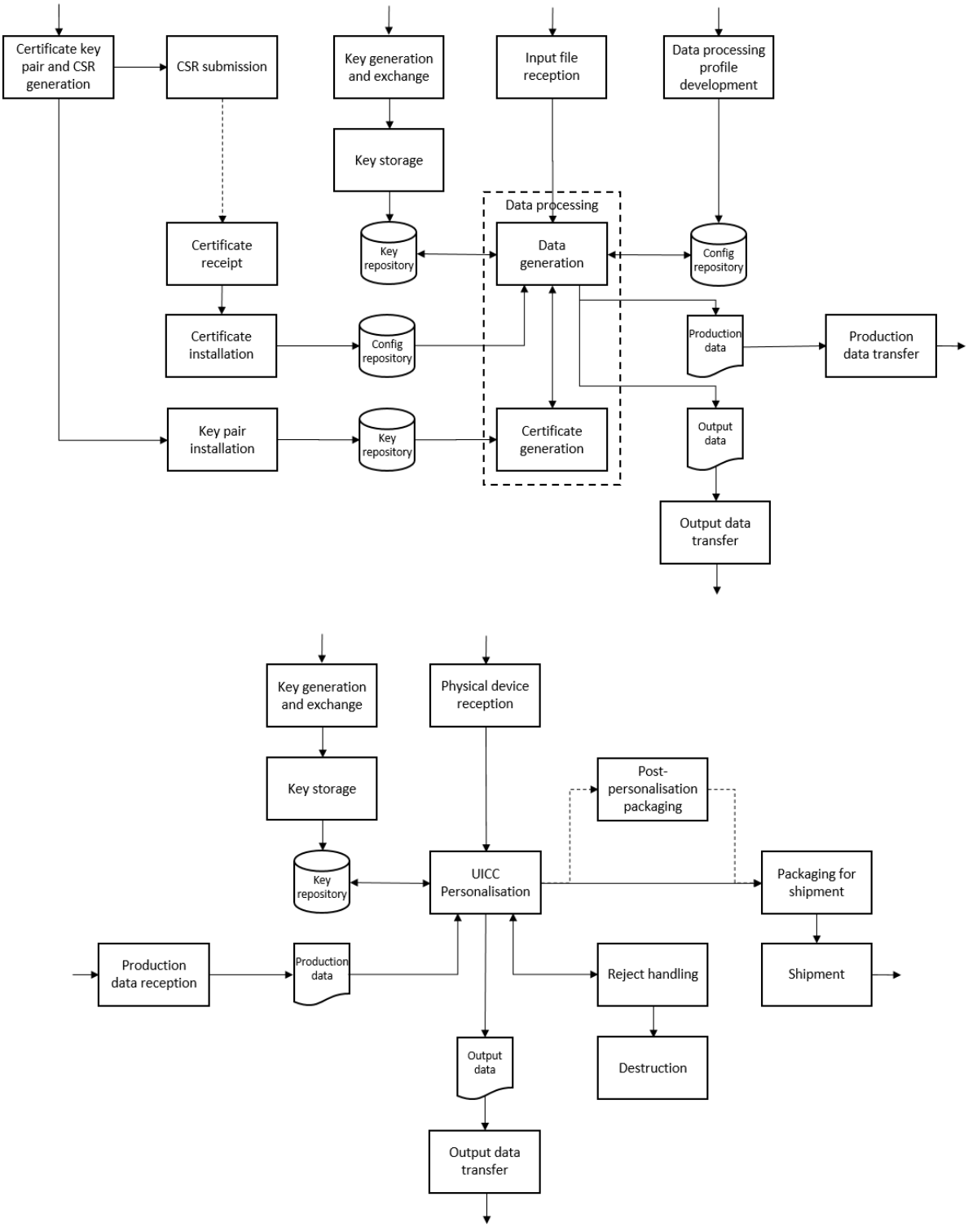


Figure 2 - UICC/eUICC Production Process Model

3.1 The Actors

There are four classes of actor:

1. Internal Authorised – [**INT_AUTH**] - Employees authorised to access the SP and supporting environment
2. Internal Unauthorised – [**INT_UNAU**] - Employees not authorised to access the SP, but who can access the supporting environment
3. External Authorised – [**EXT_AUTH**] - Third party with authority to access the SP and supporting environment
4. External Unauthorised – [**EXT_UNAU**] - Third party not authorised to access the SP or supporting environment.

4 The Assets

4.1 Introduction

Within the processes described above, assets are highly regarded and their security must be protected. Most assets are located in the personalisation process. However, customer specific requirements may make certain devices more sensitive if the production cycle involves additional steps prior to the personalisation process.

This document is limited to the production of UICCs for a single issuer. Other products are not part of the subject matter. The assets are laid on in tabular form below.

Incoming sensitive components (ISC)
Incoming files (ISC_INF)
Algorithms (ISC_ALG)
Information and Keys (MNO_INF, MNO_KEY, ASI_KEY)
IMSI (ISC_IMS)
Non-personalised eUICCs / devices (ISC_DEV)
Partly finished products (PFP)
UICCs /devices not completely personalised (PFP_UICC)
Finished products(FIN)
Personalised UICCs / devices (FIN_UICC)
Outgoing files (FIN_OUF)
Sensitive information (SEN)
Customer Information (SEN_CUI)
Management Data (SEN_MAD)
Profile Metadata (SEN_EIS, SEN_IIS)

Personalisation Rejects (PRJ)
UICCs/Devices (PRJ_UICC)

Table 3: Assets

4.2 Assets Classification

The assets that require protection are in various forms within the personalisation processes. The protection required can be complex, unless classes are arranged logically. A classification table is contained in Annex A.

4.3 Asset Characteristics

Files and data are transmitted, stored and used in many media and transport forms.

Finished products and partly finished products may be used as examples that only follow the same security rules as the corresponding assets when they contain customer data.

4.4 Incoming Sensitive Components (ISC)

Incoming sensitive components such as algorithms, products, files and keys are supplied to the manufacturing sites and can be sent between production sites.

Incoming sensitive components include:

- Incoming files containing classified information which must be protected in terms of integrity, confidentiality, and availability commensurate with the highest class of information contained in the file [**ISC _INF**]
- Information and Keys [**MNO_INF, MNO_KEY**] whose confidentiality, integrity and availability must be protected
- Algorithms [**ISC_ALG**] which must be protected in terms of availability, confidentiality, and integrity.
- UICCs **[ISC_DEV]** for personalisation

4.5 Partly Finished Products (PFP)

Partly finished products come from ISC transformations or ISC usage inside the same production site.

Partly finished products include:

- UICCs not completely personalised [PFP_UICC]

These assets must be protected in terms of availability and integrity. Traceability must also be ensured.

4.6 Finished Products (FIN)

Finished products are made up of:

- UICCs or other devices successfully personalised [**FIN_UICC**]
- Outgoing files [**FIN_OUF**]

- [**A_OUT_FIL1**] must be protected in availability, integrity and confidentiality as they contain sensitive information e.g. Ki
- [**A_OUT_FIL2**] must be protected in availability and integrity. They do not contain sensitive information e.g. PIN and PUK
- [**A_OUT_FIL3**] only need to have the integrity preserved as they do not contain sensitive information e.g. MSISDN
- **[A_OUT_FIL4**] must be protected in confidentiality, integrity and availability preserved in the context of [4] and [5] for remote provisioning for M2M devices or [6] and [7] for remote provisioning for consumer devices, e.g. eUICC information or OTA Keysets.

In all cases, if the files contain different classes of data the higher class shall prevail.

4.7 Personalisation Rejects (PRJ)

Personalisation rejects are:

- UICCs [**PRJ_UICC**], confidentiality must be protected

The integrity and traceability of these assets must be assured until they are destroyed.

4.8 Sensitive information (SEN)

Sensitive information is:

- Customer information [**SEN_CUI**]**,** information from the personalisation site that is created or can be obtained inside or by a third party attack. Customer information can be recorded in the following devices:
  - Security elements **[DE_SEC]** such as mother UICCs, batch UICCs, security modules etc.
  - Random number generators **[DE_RNG]**
  - Transmission and ciphering systems **[DE_TRA]**
  - Testing systems **[DE_TST]**
  - Production file systems **[DE_PRD]**
- Management Data [**SEN_MAD**], information on the management of batches and UICCs. This can consist of:
  - **[SEN_PRD]** production data which, if it contains classified information, must be protected in terms of integrity, confidentiality, and availability.
  - **[SEN_MAT**] traceability information which should allow the supplier identify the person, or group of persons, who worked on a batch
  - **[SEN_MAU**] audit information which should be available in relation to the recorded production history of a UICC/batch of UICCs for up to 12 months, subject to local laws.
- eUICC information [**SEN_EIS**], information received and exchanged with MNO and SM-SR in the context of [4] and [5] for remote provisioning of M2M devices, or received and exchanged with MNO in the context of [6] and [7] for remote provisioning of consumer devices.

- Integrated eUICC information **[SEN_IIS]**, information received and exchanged between Integrated eUICC OS instance running on Integrated eUICC hardware and Integrated eUICC OS maker.

The integrity of sensitive information must be assured and the confidentiality protected. Sensitive information includes all files, particularly working, temporary or safeguarded files that contain the information outlined above.

4.9 Cryptographic Keys (KEY)

- Secret [ASI_KEY] whose confidentiality, integrity and availability must be protected.
- Private keys [KEY_PRI] whose authenticity, confidentiality, integrity and availability must be protected.
- Public keys [KEY_PUB] whose authenticity, integrity and availability must be protected.

5 The Threats

5.1 Introduction

The threat analysis has been completed to identify the main threats to the UICC supplier. The list is not intended to be exhaustive.

The main threats to data are loss of availability, confidentiality and integrity.

The threats are listed in sections 5.2 and 5.3 independently of the process step concerned. In 5.4 each threat is associated to a step in the production process.

In the threat description, data means all type of data assets described in section 4.

5.2 Direct Threats Description

Threats	Actors	Assets	Description
T_DOUB_TEC		PFP_UICC, FIN_UICC, SEN_MAD	Physical duplicate or mismatch creation resulting from a technical mistake/bug
T_DOUB_REW	INT_AUTH INT_UNAU EXT_AUTH	PFP_UICC, FIN_UICC, SEN_MAD, PRJ_UICC,	Physical duplicate creation resulting from non destroyed material after a rework (error or malevolence)
T_DOUB_REU	INT_AUTH INT_UNAU	PFP_UICC, FIN_UICC, SEN_MAD, PRJ_UICC	Physical duplicate creation resulting from reused sensitive information (error or malevolence)
T_LOSS	INT_AUTH INT_UNAU EXT_AUTH EXT_UNAU	ALL SENSITIVE ASSETS	Loss or theft of classified assets (1, 2)
T_CONT	INT_AUTH INT_UNAU EXT_AUTH	FIN_UICC, PFP_UICC, PRJ_UICC, ISC_DEV	Accidental or deliberate cross-contamination of assets in the production environment

Threats	Actors	Assets	Description
	EXT_UNAU		
T_DISC	INT_AUTH INT_UNAU EXT_AUTH EXT_UNAU	ALL ASSETS CONTAINING CLASSIFIED INFORMATION	Disclosure of classified information
T_MODIF	INT_AUTH INT_UNAU EXT_AUTH	ALL ASSETS CONTAINING CLASSIFIED INFORMATION	Unauthorised modification of classified information causing loss of integrity through error or malevolence

Table 4 - Direct Threats Description

Additional threats can result from combinations of those threats listed above.

5.3 Indirect Threats Description

Threats	Actors	Assets	Description
T_SEF	ANY	ANY	Accidental or deliberate security failure.

Table 5 - Indirect Threats Description

5.4 Application of Threats in the Process

	T_DOUB_TEC	T_DOUB_REW	T_DOUB_REU	T_LOSS	T_CONT	T_DISC	T_MODIF	T_SEF
Customer Order Reception			✓	✓		✓	✓	✓
Incoming files reception	✓		✓	✓		✓	✓	✓
Production data generation and preparation	✓	✓	✓	✓		✓	✓	✓
Internal and external transfer of production data	✓	✓	✓	✓		✓	✓	✓
Output data generation and preparation	✓	✓	✓	✓		✓	✓	✓
Outgoing files delivery	✓			✓		✓	✓	✓
Incoming materials receipt, storage and issue				✓	✓	✓	✓	✓
Pre personalisation	✓			✓	✓	✓	✓	✓
Materials transfer to personalisation				✓	✓	✓	✓	✓
UICC/device personalisation	✓	✓	✓	✓	✓	✓	✓	✓
UICC / device packaging	✓			✓	✓	✓	✓	✓
Supplies delivery (finished products)	✓			✓	✓	✓	✓	✓
Transport between sites				✓		✓	✓	✓

Table 6 - Application of Threats in the Process

6 Security Objectives

6.1 Introduction

The supplier is responsible to ensure that assets are protected from the security risks to which they are exposed, as defined by the security objectives. It is this protection that provides assurance to the MNOs. The security objectives relate to both the sensitive process and its environment. All the objectives must be addressed but higher levels of assurance are needed depending on the asset classification.

6.2 Security Objectives for the Sensitive Process

#	Objective	Threat	Description
1	The SP must control the production process	T_DOUB_TEC T_DOUB_REW T_DOUB_REU T_LOSS T_MODIF T_CONT	To prevent clone, mismatch, anomalies
2	The SP must control, manage and protect data against loss of integrity and confidentiality	T_DOUB_REU T_LOSS T_DISC T_MODIF	To prevent: • any disclosure of assets • any non-conforming finished product due to loss of integrity
3	The SP must guarantee a secure product flow	T_DOUB_REU T_LOSS T_DISC T_SEF T_CONT	To prevent theft, loss, misappropriation of assets
4	The SP must manage the elements that are specified as auditable	T_MODIF	To look for possible or real security violation
5	The SP must be designed in such a way that independence of different customer files (asset) is always achieved	T_DISC	To prevent one customer's data being disclosed to another customer

Table 7 - Security Objectives for the Sensitive Process

6.3 Security Objectives for the Environment

#	Objective	Threat	Description
1	The SP environment must manage the elements that are specifically auditable	T_SEF	To look for possible or real security violation
2	The SP environment must guarantee a secure product flow	T_SEF	To prevent theft, loss or misappropriation of assets

Table 8 - Security Objectives for the Environment

7 Security Requirements

In order to consider the personalisation processes secure, certain requirements must be met. These requirements are specified in the SAS Consolidated Security Requirements and Guidelines (CSRG) document [2] as relevant to UICC production, specifically addressing the requirements for:

- Policy, strategy and documentation (including business continuity planning)
- Organisation and responsibility
- Information
- Personnel security
- Physical security
- Certificate and key management
- Production data management
- Logistics and production management
- Computer and network management
- Two-Step Personalisation Process

These requirements are considered as minimum-security requirements for the environment in which the SP is used.

The requirements of the SAS-UP Standard should be met by established processes / controls for which evidence of correct operation exists.

Annex A Assets

	Code	Asset	Class
Products	FIN_UICC	Finished UICCs	1
	PFP_UICC	UICC / device not completely personalised	1
	PRJ_UICC	Personalised rejected UICC	1
Information	ISC_ALG	Incoming algorithms	1
	SEN_CUI	Customer information	2
	MNO_KEY	MNO Cryptographic keys (e.g. Ki, OP, OPC, OTA keys... ISD and SSD keys)	1
	KEY	Clear cryptographic keys/key components protecting class 1 assets for confidentiality and integrity. An asset protected by these cryptographic keys is considered a class 2 asset.	1
	ASI_KEY	A cryptographic key that is used with a secret-key (symmetric) cryptographic algorithm that is uniquely associated with one or more entities and is not made public.	1
	KEY_PRI	The private component of the asymmetric key pair	1
	KEY_PUB	The public component of the asymmetric key pair	2
	MNO_INF	Information in the context of [4] and [5] for remote provisioning for M2M devices (e.g. POL 1 for profile), and [6] and [7] for remote provisioning for consumer devices.	1
Products	ISC_DEV	Incoming devices before entering personalisation process	2
Information	SEN_MAD	Management data. Information on the management of batches and UICCs. This may contain: • Production data, which may contain classified information • Traceability information, which should allow the supplier to identify the person(s) who, worked on a batch • Audit information related to the recorded production history of a UICC or batch of UICCs. If a file managed Class 1 information, these information have to be Class 1 protected and the file Class 2 protected	2
	SEN_EIS	eUICC information in the context of [4] and [5] for remote provisioning for M2M devices or [6] and [7] for remote provisioning for consumer devices. If a file manages Class 1 information, the information has to be Class 1 protected and the file has to be Class 2 protected	2
	SEN_IIS	Integrated eUICC information in the context of to Integrated eUICC production process.	2

	Code	Asset	Class
		If a file manages Class 1 information, the information has to be Class 1 protected and the file has to be Class 2 protected	
	ISC_INF	Incoming files. If the file contains class 1 information, it needs to be protected as a class 1	2
	FIN_OUF	Outgoing files. If the file contains class 1 information (E.g. Ki, EIS), this information has to be Class 1 protected.	2
	ISC_KEY_PIN	UICC PIN	2
	ISC_KEY_PUK	Unblocking PIN	2
	ISC_IMS	International Mobile Subscriber Information	2

Annex B Document Management

B.1 Document History

Version	Date	Brief Description of Change	Editor / Company
3.1.0	24 Jul 2003	Stable version in use.	James Moran, GSMA
3.2.2	16 Nov 2006	Significant clarifications added to security requirements to aid interpretation by auditees. New coversheet.	James Messham, FML
3.2.4	11 Sep 2008	New logo. Minor updates. Appendix B removed	James Messham, FML
3.3	16 Oct 2012	Applied updated GSMA document template and version numbering.	David Maxwell, GSMA
4.0	5 Mar 2013	Remove embedding process from scope of SAS and update assets, threats and security requirements as appropriate	James Messham, FML
4.1	10 Apr 2013	Replaced term “smart card” with “UICC” to clarify that non-card form factor (e.g. M2M) products are included in SAS scope.	David Maxwell, GSMA
4.2	7 Aug 2013	Correction of minor error: removed duplicated column in Table 7 - Application of Threads in the Process	David Maxwell, GSMA
4.3	30 Oct 2013	Removed design media from scope	James Messham, FML
5.0	23 Apr 2014	Integrate the SM-SR & SM-DP ecosystem. Removed personalisation of PIN mailers from SAS scope. General editorial update, including re-numbering of requirements.	SAS subgroup
6.0	14 Mar 2016	Update certificate handling requirements and separation of remote access requirement	SAS subgroup
7.0	27 Jul 2016	Replace requirements with reference to new Consolidated Security Requirements (CSR) PRD.	SAS subgroup
8.0	31 Mar 2017	Updates to reflect addition of remote SIM provisioning for consumer devices (ref. SGP.21/SGP.22) within SAS scope	RSPSAS subgroup
9.0	26 Jun 2019	Addition of Integrated eUICC production process Update/addition of UICC/eUICC lifecycle and process models	Or Elnekaveh, Qualcomm James Messham, FML
9.1	1 Apr 2022	Removed references to FS.17, allowing withdrawal of that PRD (content merged into FS.18)	David Maxwell, GSMA
9.2	12 Apr 2023	Updated GSMA logo.	David Maxwell, GSMA
9.3	19 Jul 2024	CR1006 – Merge SAS-UP scope definitions into this document	Saïd Gharout, Kigen

B.2 Other Information

Type	Description
Document Owner	SAS 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

Your comments or suggestions & questions are always welcome.