Security Accreditation Scheme - Consolidated Security Requirements

Version 7.1

22 September 2021

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

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
1.1 Overview 3
1.2 Using this document 3
1.3 Intended audience 3
1.4 Related documents 3
1.5 Definitions 4
1.6 Abbreviations 6
1.7 References 7
1.8 Conventions 7
2 Security Requirements 8
2.1 Introduction 8
2.2 Application of requirements 8
2.3 Requirements 9
1 Policy, Strategy and Documentation 9
2 Organisation and Responsibility 10
3 Information 12
4 Personnel Security 12
5 Physical Security 13
6 Certificate and Key Management 15
7 Sensitive Process Data Management 17
8 SM-DP, SM-SR, SM-DP+ and SM-DS Service Management 19
9 Logistics and Production Management 20
10 Computer and Network Management 23
11 Two-Step Personalisation Process 29
Annex A Document Management 32
A.1 Document History 32
A.2 Other Information 32

1 Introduction

1.1 Overview

The GSMA operates Security Accreditation Schemes (SAS) for a number of sensitive processes (SPs). To fulfil the requirements of the relevant Security Accreditation Schemes, Auditees are required to follow the corresponding Standard, including achieving compliance with the relevant security requirements.

To ensure common standards across the schemes the GSMA publishes this Consolidated Security Requirements (CSR) document. The document sets out statements of requirement that are relevant to SAS Auditees.

These requirements are, in turn, supported by the Consolidated Security Guidelines (CSG) document [5] which provides practical guidance to SAS Auditees to help them design, implement and operate security controls that meet the CSR.

1.2 Using this document

This document is intended to provide requirements for all SPs within the scope of the different SAS schemes. Many of the requirements are common across all schemes, however some requirements are specific to individual SPs. The SPs for which each requirement applies are indicated in this document as described in 2.2.

The SAS Standard document relevant to each Auditee’s activities and certification will clearly define which of the SPs are, or may, be applicable.

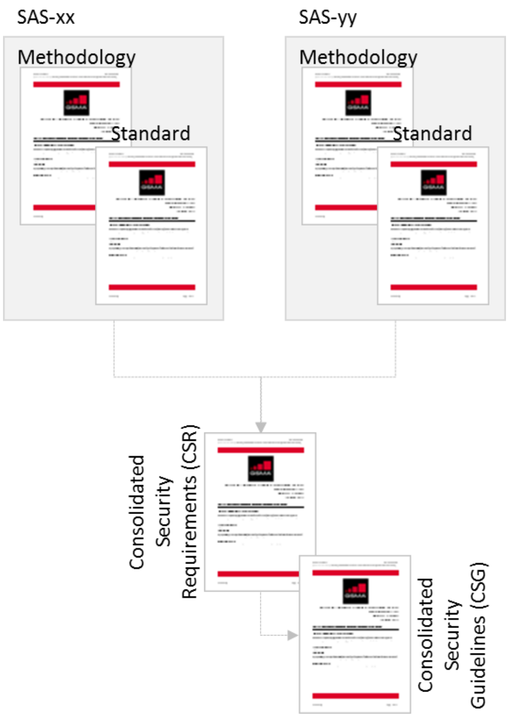
SAS Auditees are responsible for ensuring that they have determined which of the SPs and requirements are relevant to them. In the event of any query, Auditees should contact sas@gsma.com.

1.3 Intended audience

- Security professionals and others within organisations seeking to obtain or maintain accreditation under the GSM Association Security Accreditation Scheme
- Security professionals and others within organisations seeking to procure products or services within the scope of the GSM Association Security Accreditation Scheme
- SAS Subgroup members
- Auditors

1.4 Related documents

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


SAS-xx
Methodology
Standard
SAS-yy
Methodology
Standard
Consolidated Security Requirements (CSR)
Consolidated Security Guidelines (CSG)

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 (CSR)** describe all of the security requirements that may apply to SPs in the different SAS schemes.

The **Consolidated Security Guidelines (CSG)** provide 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 will utilise the same Consolidated Requirements and Guidelines.

References to the Standard and Methodology documents for each SAS scheme using the Consolidated Requirements and Guidelines can be found in section 1.7.

1.5 Definitions

Term	Description
Actor	Person who is involved in, or can affect, the Sensitive Process
Audit	The SAS audit carried out by the Audit Team at the Auditee’s Site
Audit Team	Two Auditors, one each from different GSMA-selected auditing companies, jointly carrying out the Audit on behalf of the GSMA.
Auditee	The supplier that is seeking SAS certification of its Site(s).
Auditor	A person qualified to perform SAS Audits
Business Continuity	Capability of the operator of a SP to continue to operate the SP at predefined levels (as determined by customer requirements) following a failure incident.
Certificate Authority	Responsible to issue Public Key Certificates. Could be the GSMA CI [12] or an independent eSIM CA [13] issuing certificates for EUM and SM-XX, or the EUM issuing certificates for eUICC
eUICC Management	A set of functions related to the registration of an eUICC to a SM-SR and the change of SM-SR for an eUICC.
Generation of Data for	Generation of Data for Personalisation, or Data Generation, refers to the generation of any data that is to be encoded into a device intended to act as a

Term	Description
Personalisation	UICC/eUICC to make it uniquely identifiable. This data may be: • Unique security keys that control future access to the device; • An eUICC Controlling Authority Security Domain (ECASD) and Issuer Security Domain - Root (ISD-R), and/or • MNO profile data.
GSMA CI	A Certificate Authority accredited by the GSMA to enable global interoperability within the GSMA eSIM ecosystem in accordance with the GSMA eUICC PKI Certificate Policy SGP.14 [12].
High Security Area	An area accessible only to authorised personnel in which sensitive assets are stored or processed. Appropriate physical protection and access controls will normally be deployed to protect the HSA.
Integrated eUICC	An eUICC conforming to the GSMA SGP.01/02/21/22 eSIM specifications 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
Key	Any logical key (e.g. cryptographic key or certificate)
Personalisation	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.
Personalisation Data	Data generated during the Generation of Data for Personalisation process.
Physical key	Any key and/or combination used for opening a physical lock (e.g. a door, vault, safe or secure cabinet)
PKI Certificate Management	PKI Certificate Management 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 definition refers only to the management of the key pair and certificate; the process of generating individual eUICC device certificates is included within the definition of "Generation of Data for Personalisation” for eUICCs.
Platform Management	A set of functions related to the transport, enabling, disabling and deletion of a Profile on an eUICC.
Profile	Combination of a file structure, data and applications to be provisioned onto, or present on, an eUICC and which allows, when enabled, the access to a specific mobile network infrastructure.
Profile Management	A set of functions related to the downloading, installation and content update of a Profile in a dedicated eUICC.
Reject	Finished or partially finished product containing sensitive information which has been ejected from the process.
Restricted area	An area, which may or not be a sub-area of an HSA, in which physical access is limited and enforced by access control devices where sensitive systems or components of the SP are installed.
SAS Subgroup	A group of GSMA members and staff that, together with the SAS Auditors, is responsible for maintenance and development of the SAS Standards,

Term	Description
	Methodologies, Consolidated Security Requirements and Consolidated Security Guidelines,
Sensitive Process	The security evaluation field, covering the processes and the assets within those processes. For the purposes of SAS, SPs can include activities related to UICC production, subscription management and certificate management.
Site	Auditee’s physical facility and its relevant controls that are subject to the Audit.
Universal Integrated Circuit Card	A smart card that conform to the specification written and maintained by the ETSI Smart Card Platform.

1.6 Abbreviations

Term	Description
CA	Certificate Authority
CSR	Consolidated Security Requirements
CSG	Consolidated Security Guidelines
eUICC	Embedded UICC (as defined above)
EUM	eUICC Manufacturer
FIPS	Federal Information Processing Standard
FS.nn	Prefix identifier for official documents belonging to GSMA Fraud and Security Group
GSMA	GSM Association
HSM	Hardware Security Module
IT	Information Technology
MNO	Mobile Network Operator
PKI	Public Key Infrastructure
SAS	Security Accreditation Scheme
SAS-SM	Security Accreditation Scheme for Subscription Management Roles
SAS-UP	Security Accreditation Scheme for UICC Production
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 [7])
SM-DS	Subscription Manager – Discovery Service
SM-SR	Subscription Manager – Secure Routing
SM-XX	SM-DP, SM-SR, SM-DP+, or SM-DS
SP	Sensitive Process
UICC	Universal Integrated Circuit Card (e.g. a SIM card)

1.7 References

Ref	Doc Number	Title
[1]	PRD FS.04	GSMA SAS Standard for UICC Production, latest version available at www.gsma.com/sas
[2]	PRD FS.05	GSMA SAS Methodology for UICC Production, latest version available at www.gsma.com/sas
[3]	PRD FS.08	GSMA SAS Standard for Subscription Manager Roles, latest version available at www.gsma.com/sas
[4]	PRD FS.09	GSMA SAS Methodology for Subscription Manager Roles, latest version available at www.gsma.com/sas
[5]	PRD FS.18	GSMA SAS Consolidated Security Guidelines, available to participating sites from sas@gsma.com
[6]	PRD SGP.01	Embedded SIM Remote Provisioning Architecture
[7]	PRD SGP.02	Remote Provisioning Architecture for Embedded UICC Technical Specification
[8]	PRD SGP.21	Remote SIM Provisioning (RSP) Architecture
[9]	PRD SGP.22	Remote SIM Provisioning (RSP) Technical Specification
[10]	RFC 2119	“Key words for use in RFCs to Indicate Requirement Levels”, S. Bradner, March 1997. Available at http://www.ietf.org/rfc/rfc2119.txt
[11]	BSI-CC-PP-0084-2014	Security IC Platform Protection Profile with Augmentation Packages. Version 1.0 (13.01.2014).
[12]	PRD SGP.14	GSMA eUICC PKI Certificate Policy
[13]	PRD SGP.28	eSIM CI Registration Criteria

1.8 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 [10].”

2 Security Requirements

2.1 Introduction

In order to consider activities secure, certain requirements must be met. These requirements are considered as minimum-security requirements for the environment in which the SP is used.

These requirements are, in general, non-prescriptive. Participants are permitted to meet requirements by deployment of appropriate controls rather than by using specific tools or solutions, provided that the same security objective is met to an acceptable level. An approach to meeting the security requirements is defined in the SAS Consolidated Security Guidelines (CSG) [5].

NOTE: Numbering of the sections and requirements below restarts at (1) and applies independently of other sections in this document. The requirements should be referenced by the numbering system herein which will be applied consistently across the SAS documentation.

2.2 Application of requirements

The applicability of requirements to different activities is indicated through the following scope symbols:

All	Applies to all participants, regardless of activity
UP	Applies to participants conducting UICC production
SM	Applies to participants conducting Subscription Management activities
CM	Applies to participants conducting Certificate Management activities
I	Applies to participants having Integrated eUICC form-factor
DC	Applies to participants conducting Data Centre Operations and Management activities, including those providing Cloud Services that host services subject to SAS certification.

In all cases the scope symbols apply:

- to the statement against which they are marked
- to all subsequent statements of the same numbering depth where no different scope has been indicated

All statements of lower depth in the numbering scheme inherit the scope from the parent, unless an alternative scope is indicated.

2.3 Requirements

1 Policy, Strategy and Documentation				
All	The security policy and strategy provides the business and its employees with a direction and framework to support and guide security decisions within the company and at the location where the SP takes place.			
	1.1	Policy		
		1.1.1	A clear direction shall be set and supported by a documented security policy which defines the security objectives and the rules and procedures relating to the security of the SP, sensitive information and asset management.	
		1.1.2	Employees shall understand and have access to the policy and its application should be checked periodically.	
	1.2	Strategy		
		1.2.1	A coherent security strategy must be defined based on a clear understanding of the risks. The strategy shall use periodic risk assessment as the basis for defining, implementing and updating the site security system. The strategy shall be reviewed regularly to ensure that it reflects the changing security environment through ongoing re-assessment of risks.	
	1.3	Business Continuity Planning		
		1.3.1	Business continuity measures must be in place:	
			(i)	to ensure an appropriate level of availability
			(ii)	to enable response and recovery in the event of a disaster.
	1.4	Internal audit and control		
		1.4.1	The overall security management system shall be subject to a rigorous programme of internal monitoring, audit and maintenance to ensure its continued correct operation.	

2	**Organisation and Responsibility**			
All	A defined organisation shall be responsible for ownership and operation of the security management system.			
	2.1	Organisation		
		2.1.1	To successfully manage security, a defined organisation structure shall be established with appropriate allocation of security responsibilities.	
		2.1.2	The management structure shall maintain and control security through a cross-functional team that co-ordinates identification, collation, and resolution, of security issues, independent of the business structure.	
	2.2	Responsibility		
		2.2.1	A security manager shall be appointed with overall responsibility for the issues relating to security in the SP.	
		2.2.2	Clear responsibility for all aspects of security, whether operational, supervisory or strategic, must be defined within the business as part of the overall security organization.	
		2.2.3	Asset protection procedures and responsibilities shall be documented throughout the SP.	
		2.2.4	Clear security rules shall govern the manner in which Employees engaged in such activities shall operate within the SP. Relevant guidelines should be in place and communicated to all relevant staff.	
	2.3	Incident response and reporting		
		2.3.1	An incident response mechanism shall be maintained that includes a process for the investigation and mitigation of:	
			(i)	accidental or deliberate breach of internal regulations and procedures
			(ii)	suspected or detected compromise of systems, or receipt of notification of system vulnerabilities
			(iii)	physical or logical penetration of the site

			(iv)	denial of service attacks on components (where applicable)
	2.4	Contracts and liabilities		
		2.4.1	In terms of contractual liability, responsibility for loss shall be documented. Appropriate controls and insurance shall be in place.	
		2.4.2	Where activities within scope of SAS certification are outsourced or sub-contracted, partners providing or operating these services shall be contractually responsible to ensure an appropriate level of compliance with the SAS requirements.	
			(i)	Responsibilities that fall within the scope of the auditee's SAS certification shall be clearly documented and agreed.
			(ii)	Contracts shall include a "right-to-audit" clause (or equivalent mechanism) to: • Enable auditees to confirm that contractual responsibilities and obligations are maintained at the required level by the outsourcing partner / sub-contractor. • Include the right of the auditee to require the outsourcing partner / sub-contractor to participate in the SAS audit process, where applicable.
UP CM		2.4.3	For eUICC production, transfer of class 1 assets between sites must enforce integrity of SAS-UP certification throughout the production chain.	
			(i)	eUICC production data must only be supplied to SAS-UP sites for further processing or production.
			(ii)	Physical eUICC devices must only be transferred to SAS-UP certified production sites until/unless: • They are personalised eUICCs already capable of accepting an operator profile in accordance with the GSMA specifications SGP.01 [6], SGP.02 [7], SGP.21 [8] and/or SGP.22 [9] as applicable.
			(iii)	Specified class 1 information assets must never be transferred unless specifically disclosed and agreed as part of the SAS-UP certification: • PKI certificate key pairs must only be used at designated sites, as described in 6.6.2.

3 Information

All	The management of sensitive information, including its storage, archiving, destruction and transmission, can vary depending on the classification of the asset involved.		
	3.1	Classification	
		3.1.1	A clear structure for classification of information and other assets shall be in place with accompanying guidelines to ensure that assets are appropriately classified and treated throughout their lifecycle.
	3.2	Data and media handling	
		3.2.1	Access to sensitive information and assets must always be governed by an overall ‘need to know’ principle.
		3.2.2	Guidelines shall be in place governing the handling of data and other media, including a clear desk policy. Guidelines should describe the end-to-end ‘lifecycle management’ for sensitive assets, considering creation, classification, processing, storage, transmission and disposal.

4 Personnel Security

All	A number of security requirements shall pertain to all personnel working within the SP and those with trusted positions.		
	4.1	Security in job description	
		4.1.1	Security responsibilities shall be clearly defined in job descriptions.
	4.2	Recruitment screening	
		4.2.1	An applicant, and employee, screening policy shall be in place where local laws allow
	4.3	Acceptance of security rules	
		4.3.1	All recruits shall sign a confidentiality agreement.
		4.3.2	Employees shall read the security policy and record their understanding of the contents and the conditions they impose.

		4.3.3	Adequate training in relevant aspects of the security management system shall be provided on an ongoing basis.
	4.4	Incident response and reporting	
		4.4.1	Reporting procedures shall be in place where a breach of the security policy has been revealed.
		4.4.2	A clear disciplinary procedure shall be in place in the event that a staff member breaches the security policy.
	4.5	Contract termination	
		4.5.1	Clear exit procedures shall be in place and observed with the departure of each Employee.

5	**Physical Security**			
All	Physical security controls are required at all sites where SPs are carried out, to consider the location and protection of the sensitive assets (both physical and information) wherever they are stored or processed. Buildings in which sensitive assets are processed or stored shall be of appropriate construction; robust and resistant to outside attack. Sensitive assets must be controlled within high security and restricted areas by using recognised security control devices, staff access procedures and audit control logs.			
	5.1	Security plan		
		Layers of physical security control shall be used to protect the SP according to a clearly defined and understood strategy. The strategy shall apply controls relevant to the assets and risks identified through risk assessment.		
		5.1.1	The strategy shall be encapsulated in a security plan that:	
			(i)	defines a clear site perimeter / boundary
			(ii)	defines one or more levels of secure area within the boundary of the site perimeter
			(iii)	maps the creation, storage and processing of sensitive assets to the secure areas
			(iv)	defines physical security protection standards for each level of secure area

	5.2	Physical protection		
		5.2.1	The protection standards defined in the security plan shall be appropriately deployed throughout the site, to include:	
			(i)	physical protection of the building and secure areas capable of resisting attack for an appropriate period
			(ii)	deterrent to attack or unauthorized entry
			(iii)	mechanisms for early detection of attempted attack against, or unauthorized entry into, the secure areas at vulnerable points
			(iv)	control of access through normal entry / exit points into the building and SP to prevent unauthorized access
			(v)	effective controls to manage security during times of emergency egress from the secure area and building
			(vi)	mechanisms for identifying attempted, or successful, unauthorized access to, or within the site
			(vii)	mechanisms for monitoring and providing auditability of, authorised and unauthorised activities within the SP
		5.2.2	Controls deployed shall be clearly documented and up-to-date.	
	5.3	Access control		
		5.3.1	Clear entry procedures and policies shall exist which cater for the rights of Employees, visitors and deliveries to enter the SP. These considerations shall include the use of identity cards, procedures governing the movement of visitors within the SP, delivery/dispatch checking procedures and record maintenance.	
		5.3.2	Access to each secure area shall be controlled on a ‘need to be there’ basis. Appropriate procedures shall be in place to control, authorise, and monitor access to each secure area and within secure areas.	
	5.4	Security staff		
		5.4.1	Security staff are commonly employed by suppliers. Where this is the case the duties shall be clearly documented and the necessary tools and training shall be supplied.	

	5.5	Internal audit and control	
		5.5.1	Physical security controls shall be subject to a rigorous programme of internal monitoring, audit and maintenance to ensure their continued correct operation.

6	**Certificate and Key Management**		
UP SM CM I	Technical and procedural controls shall be applied to cryptographic keys and certificates related to the SP at the site. Applicable requirements will vary according to the level of SP. Specific requirements applying to Root Certificate Authorities (CAs) are highlighted where applicable.		
	6.1	Classification	
		6.1.1	Keys and certificates shall be classified as sensitive information. Logical, physical, personnel and procedural controls shall be applied to ensure that appropriate levels of confidentiality, integrity and availability are applied.
	6.2	Roles and responsibilities	
		6.2.1	Responsibilities and procedures for the management of certificates and cryptographic keys shall be clearly defined.
		6.2.2	Auditable dual-control shall be applied to sensitive steps of key management.
	6.3	Cryptographic key specification	
		6.3.1	Technical specifications for cryptographic keys and certificates shall be selected that are: • compliant with relevant or applicable standards or • of an appropriate level to the asset(s) protected, based on risk and lifespan.
	6.4	Cryptographic key management	

		6.4.1	Cryptographic keys, certificates and activation data shall be generated, exchanged, stored, backed-up and destroyed securely.	
		6.4.2	The cryptographic key management process shall be documented and cover the full lifecycle of keys & certificates.	
	CM SM	6.4.3	The storage and cryptographic computation for keys and certificate generation (derivations, random generations) involved in the protection of the sensitive data (i.e. Class 1 data) shall rely on hardware security modules (HSM) that are FIPS 140-2 level 3 certified.	
	6.5	Audit and accountability		
		6.5.1	Key management activities shall be controlled by an audit trail that provides a complete record of, and individual accountability for, all actions.	
CM SM	6.6	GSMA Public Key Infrastructure (PKI) Certificates		
		6.6.1	Supplier certificates used as part of any GSMA PKI shall be signed by a CA authorized by and acting on behalf of the GSMA	
		6.6.2	PKI certificate private keys shall only ever be installed and used at sites:	
			(i)	That are agreed with the GSMA.
			(ii)	That are SAS certified with the appropriate scope.
			(iii)	In accordance with the certificate policy.
		6.6.3	PKI certificate key pairs shall only ever be transferred and installed to a different operational site:	
			(i)	With the prior agreement of the GSMA.
			(ii)	Where the new operational site is SAS certified with the appropriate scope.
			(iii)	In accordance with the certificate policy.
			(iv)	By a mechanism that ensures an appropriate level of security for the transfer of the sensitive assets.

		6.6.4	Where auditees make use of the same PKI certificate private key at multiple sites, in addition to the requirements of 6.6.2 and 6.6.3:	
			(i)	A single, nominated, site within the auditee organization shall be responsible for control and issue of the certificate key pair.
			(ii)	All transfer of certificate private keys shall originate from the nominated site.
			(iii)	Controls shall be in place to prevent certificate private keys being transferred except under the control of the nominated site.
			(iv)	All transfer of certificate private keys shall be recorded and auditable.
UP		6.6.5	Where auditees make use of the same EUM PKI certificate private key at multiple sites, in addition to the requirements of 6.6.4:	
			(i)	Auditees shall ensure that all generation and signing of eUICC device certificates shall be traceable to the site where data generation was carried out, based on EID.
			(ii)	Controls shall be in place to ensure the confidentiality, integrity and availability of the traceability data.

7 Sensitive Process Data Management

UP SM	The site shall be responsible for lifecycle management of Class 1 data used within the SP. Information and IT security controls must be appropriately applied to all aspects of lifecycle management to ensure that data is adequately protected. The overall principle shall be that all data is appropriately protected from the point of receipt through storage, internal transfer, processing and through to secure deletion of the data.		
	7.1	Data transfer	
		7.1.1	Sites shall take responsibility to ensure that electronic data transfer between themselves and other third parties is appropriately secured.
	7.2	Sensitive data access, storage and retention.	
		7.2.1	Sites shall prevent direct access to sensitive process data where it is stored and processed.

			(i)	User access to sensitive data shall be possible only where absolutely necessary. All access must be auditable to identify the date, time, activity and person responsible.
			(ii)	System and database administrators may have privileged access to sensitive data. Administrator access to data must be strictly controlled and managed. Administrative access to data shall only take place where explicitly authorized and shall always be irreversibly logged.
		7.2.2	Data shall be stored protected appropriate to its classification.	
		7.2.3	Data retention policies shall be defined, monitored and enforced.	
UP	7.3	Data generation		
		7.3.1	As part of the Personalisation process secret data may be generated and personalized into the UICC. Where such generation takes place:	
			(i)	The quality of the number generator in use shall be subject to appropriate testing on a periodic basis. Evidence of testing, and successful results, shall be available.
			(ii)	Clear, auditable, controls shall be in place surrounding the use of the number generator to ensure that data is taken from the appropriate source.
UP SM	7.4	Auditability and accountability		
		7.4.1	The sensitive process shall be controlled by an audit trail that provides a complete record of, and individual accountability for the lifecycle of information assets to ensure that:	
			(i)	all assets created, processed and deleted are completely accounted for
			(ii)	access to sensitive data is auditable
			(iii)	responsible individuals are traceable and can be held accountable
		7.4.2	The audit trail shall be protected in terms of integrity and the retention period must be defined. The audit trail shall not contain sensitive data.	

		7.4.3	Auditable dual-control and 4-eyes principle shall be applied to sensitive steps of data processing.	
	UP	7.4.4	For UICC production the audit trail shall include:	
			(i)	Generation of Data for Personalisation and processing of that data
			(ii)	Personalisation
			(iii)	re-Personalisation
			(iv)	access to sensitive data
			(v)	Production of customer output files
	7.5	Duplicate production		
		7.5.1	Controls shall be in place to prevent duplicate production.	
UP SM	7.6	Data integrity		
		7.6.1	Controls shall be in place to ensure that the same, authorized, data from the correct source is used for the sensitive process and supplied to the customer.	
	7.7	Internal audit and control		
		7.7.1	Sensitive data controls shall be subject to a rigorous programme of internal monitoring, audit and maintenance to ensure their continued correct operation.	

8 SM-DP, SM-SR, SM-DP+ and SM-DS Service Management

SM	8.1	SM-DP, SM-SR, SM-DP+ and SM-DS Service	
		8.1.1	Systems used for the remote provisioning, management of eUICCs and management of Profiles shall support the secure interfaces as defined in SGP.01 [6], SGP.02 [7], SGP.21 [8] and/or SGP.22 [9] as applicable.
		8.1.2	Exchange of data within the SM-DP, SM-SR, SM-DP+ or the SM-DS

			IT system shall be secured to the level required by its asset classification.	
		8.1.3	The SM-DP, SM-SR, SM-DP+ and SM-DS must prevent cross-contamination of assets between different customers.	
		8.1.4	Multi-tenant SM-DP, SM-SR, SM-DP+ and SM-DS solutions on the same physical hardware shall ensure customer data is logically segregated between different customers.	
	8.2	Remote Entity Authentication		
		8.2.1	All authorized entities in the SM-DP, SM-SR, SM-DP+ and SM-DS processes shall be authenticated by appropriate authentication protocols for example, SM-SR, SM-DP, SM-DP+, SM-DS, MNO.	
	8.3	Audit trails		
		8.3.1	The SP shall be logged in an audit trail that provides a complete record of, and individual accountability for:	
			(i)	Profile Management, Platform Management, IT system and eUICC Management procedures, events management, and communication with other entities through the secure interfaces.
			(ii)	Access to sensitive data
		8.3.2	The audit trail shall be managed in accordance with the requirements of 7.4.	

9	**Logistics and Production Management**		
UP	UICC production processes shall be subject to appropriate controls that ensure integrity of, and accountability for, all sensitive assets and prevent duplicate production.		
	9.1	Order management	
		9.1.1	The ordering format shall be agreed between operator and supplier and rules to preserve the integrity of the ordering process shall be in place.
	9.2	Raw materials	

		9.2.1	Raw materials classified as lower than class 2 (plastic sheets, GSM generic components, blank mailers, etc.) are not considered to be security sensitive. However, appropriate controls shall be established for stock movements. The availability of these assets must be ensured.	
		9.2.2	Raw materials classified as class 2 (e.g. non-personalised devices) are considered to be security sensitive. Controls shall be established that:	
			(i)	account for stock movement
			(ii)	prevent unauthorized access
			(iii)	preserve the integrity of batches
			(iv)	prevent availability of class 2 assets within the production environment undermining the quantity control and reconciliation mechanism for class 1 assets.
	9.3	Control, audit and monitoring		
		9.3.1	The production process shall be controlled by an audit trail that:	
			(i)	ensures that the quantities of class 1 assets created, processed, rejected and destroyed are completely accounted for
			(ii)	ensures that the responsible individuals are traceable and can be held accountable
			(iii)	demands escalation where discrepancies or other security incidents are identified.
		9.3.2	The stock of all Class 1 assets must be subject to end-to-end reconciliation in order that every element can be accounted for.	
		9.3.3	Auditable dual-control and 4-eyes principle shall be applied to sensitive steps of the production process, including:	
			(i)	control of the quantity of assets entering the Personalisation process
			(ii)	authorization of re-Personalisation for rejected UICCs
			(iii)	control of the quantity of assets packaged for dispatch to customers
			(iv)	destruction of rejected assets

		9.3.4	Application of 4-eyes principle shall be auditable through production records and CCTV.	
		9.3.5	Regular audits shall be undertaken to ensure the integrity of production controls and the audit trail.	
		9.3.6	Suppliers must demonstrate an ability to prevent unauthorised duplication within the production process during Personalisation and re-Personalisation.	
		9.3.7	Suppliers must demonstrate an ability to preserve the integrity of batches within the production environment to prevent:	
			(i)	cross-contamination of assets between batches
			(ii)	uncontrolled assets in the production environment undermining the integrity of the asset control mechanism.
	9.4	Destruction		
		9.4.1	Rejected sensitive assets must always be destroyed according to a secure procedure and logs retained.	
	9.5	Storage		
		9.5.1	Personalised product shall be stored securely prior to dispatch to preserve the integrity of the batches. Where personalised product is stored for extended periods additional controls shall be in place.	
	9.6	Packaging and delivery		
		9.6.1	Packaging of goods shall be fit for the intended purpose and strong enough to protect them during shipment. Appropriate measures shall be in place to ascertain whether or not goods have been tampered with.	
		9.6.2	Secure delivery procedures shall be agreed between the customer and the supplier which shall include agreed delivery addresses and the method of delivery.	
		9.6.3	Collection and delivery notes must be positively identified. Goods shall only be handed over following the production of the appropriate authority documents. A receipt should be obtained.	

	9.7	Internal audit and control	
		9.7.1	Production security controls shall be subject to a rigorous programme of internal monitoring, audit and maintenance to ensure their continued correct operation.

10 Computer and Network Management			
All	The secure operation of computer and network facilities is paramount to the security of data. In particular, the processing, storage and transfer of Class 1 information, which if compromised, could have serious consequences, must be considered. Operation of computer systems and networks must ensure that comprehensive mechanisms are in place to preserve the confidentiality, integrity and availability of data.		
	10.1	Policy	
		10.1.1	A documented IT security policy shall exist which shall be well understood by employees.
	10.2	Segregation of roles and responsibilities	
		10.2.1	Roles and responsibilities for administration of computer systems should be clearly defined. Administration of systems storing or processing sensitive data shall not normally be carried out by users with regular operational responsibilities in these areas. Roles for review of audit logs for sensitive systems should be separated from privileged users (e.g. administrators).
	10.3	Access control	
		10.3.1	Physical access to sensitive computer facilities shall be controlled.
		10.3.2	An access control policy shall be in place and procedures shall govern the granting of access rights with a limit placed on the use of special privilege users. Logical access to IT services shall be via a secure logon procedure.
		10.3.3	Passwords shall be used and managed effectively.
	10.4	Remote Access	

		Remote access for a user to connect to a network, system or service from a location other than as part of the certified secure area(s) at the site shall only be permitted in accordance with the requirements of 10.4. Remote access requirements shall be applied to any environment containing assets (networks, systems or information) within the scope of SAS certification. The remote access requirements describe connection from a remote **endpoint** via a secure **channel** to the **target** environment.	
		10.4.1	Where remote access is implemented it shall: • Enforce appropriate protection of sensitive systems, networks and information. • Be implemented based on strict principles of minimum access. • Be fully auditable. • Be subject to a clear, documented risk assessment. • Be governed by a defined remote access policy and procedure.
		10.4.2	Remote access controls secure the connection from the remote user to the target environment. All operations carried out across the remote access connection shall enforce an equivalent security level to corresponding activities conducted locally on-site.
		10.4.3	Where remote access for operational **read-only** monitoring of systems is granted, such connections shall take place with/via systems on a DMZ rather than directly into a high security network. Access to view sensitive data shall not be possible.
		10.4.4	Where remote access for connection to **pre-defined services** is granted, such connections shall take place with/via systems on a DMZ rather than directly into a high security network. Access to view sensitive data shall not be possible.
		10.4.5	Where remote **interactive** access to sensitive systems and networks within SAS certified sites is granted for administration or operational reasons, such access shall take place from clearly designated, physically controlled environments. The originating system shall have at least the same level of physical and logical security controls as the target systems, up to the level required for SAS compliance.

		10.4.6	Remote access carried out other than according to 10.4.3, 10.4.4 and 10.4.5 shall not normally be accepted at SAS certified sites. Where auditees wish to utilise other solutions as exceptions to those normally accepted they shall provide evidence that either: • The remote access does not allow access to networks, systems or information within the scope of SAS certification. Or, for SAS-SM only: • A full and appropriate risk assessment, accepted by the audit team prior to implementation, has been conducted that considers both the access to systems and the visibility of sensitive information. And • The site containing the endpoint systems is owned by the auditee or its contracted supplier(s). And • The remote access is temporary, monitored and controlled in real-time from a SAS-SM certified environment, with no ability to export data. In all cases, controls described in 10.4.7 shall apply.	
		10.4.7	Connectivity between the originating endpoint and the targeted system(s) must be appropriately secured, as follows:	
			(i)	Endpoint security The security of the endpoint from which remote access originates shall enforce appropriate logical and physical security controls to ensure a level of protection equivalent to those applied to direct access to the target system. Specifically, endpoints shall be: • Positively identified, with access strictly limited to pre-authorised devices that are: o Owned and controlled by the auditee organisation. o Subject to appropriate hardening controls. o Configured according to a defined security policy o Up-to-date with the latest security patches at the time of the connection.

				• Only located in clearly designated physically secure environments to which access is controlled on strict-need-to-be-there principles. • Connected to a local network dedicated to the purpose of remote access to sensitive network systems that can only be accessed from within the designated physically secure environments.
			(ii)	Security of the channel The channel used to connect from the endpoint network to the target network environment shall be secured: • End-to-end between devices that are configured and managed under physical and logical security controls within the scope of the SAS certification process. • Using appropriate technologies to ensure the required level of security. o Keys and credentials used for authentication and encryption of the channel should be generated, stored and exchanged according to secure processes.
			(iii)	Security of the target network The remote access channel used for user access shall terminate in a dedicated remote access network containing one or more jump hosts configured to control and monitor access for authorized endpoints and end users to connect to pre-determined target systems. The remote access network shall be configured to permit access: • Inbound only via the secure channel. • Outbound: o Via one or more firewalls. o Only to those target systems to which remote access is specifically required. o Only using pre-determined methods of connection (e.g. RDP, SSH) for each system. Jump hosts shall be used within the frontend/DMZ zone to connect to devices or servers in that zone. Additional jump hosts shall be used within the backend

				zone to connect to devices or servers in that zone. A jump host shall be used within the relevant network security zone in which the targeted servers are logically and physically located.
			(iv)	Authentication Remote user access mechanisms must employ enhanced authentication mechanisms (e.g. multi-factor authentication), whenever remote access is granted: • across networks of lower security level than that being connected to • from off-site locations
			(v)	Audit trails and logs Monitoring and full logging shall be in place to ensure full traceability of all access sessions. Integrity of these logs and logging mechanisms shall be protected to prevent modification, deletion or disabling.
	10.5	Network security		
		10.5.1	Systems and data networks used for the processing and storage of sensitive data shall be housed in an appropriate environment and logically or physically separated from insecure networks.	
		10.5.2	Data transfer between secure and insecure networks must be strictly controlled according to a documented policy defined on a principle of minimum access.	
		10.5.3	The system shall be implemented using appropriately configured and managed firewalls incorporating appropriate intrusion detection systems.	
		10.5.4	Controls shall be in place to proactively identify security weaknesses and vulnerabilities and ensure that these are addressed in appropriate timescales	
		10.5.5	Systems providing on-line, real-time services shall be protected by mechanisms that ensure appropriate levels of availability (e.g. by protecting against denial-of-service attacks).	
	10.6	Systems security		

		10.6.1	Systems configuration and maintenance	
			(i)	Security requirements of systems shall be identified at the outset of their procurement and these factors shall be taken into account when sourcing them.
			(ii)	System components and software shall be protected from known vulnerabilities by having the latest vendor-supplied security patches installed.
			(iii)	System components configuration shall be hardened in accordance with industry best practice
			(iv)	Change control processes and procedures for all changes to system components shall be in place.
			(v)	Processes shall be in place to identify security vulnerabilities and ensure the associated risks are mitigated.
			(vi)	Comprehensive measures for prevention and detection of malware and viruses shall be deployed across all vulnerable systems.
			(vii)	Unattended terminals shall timeout to prevent unauthorised use and appropriate time limits shall be in place.
			(viii)	Decertification/decommissioning of assets (such as IT Systems) used as part of the SP shall be documented and performed in a secure manner.
		10.6.2	System back-up	
			(i)	Back-up copies of critical business data shall be taken regularly. Back-ups shall be stored appropriately to ensure confidentiality and availability.
	10.7	Audit and monitoring		
		10.7.1	Audit trails of security events shall be maintained and procedures established for monitoring use.	
	10.8	External facilities management		
		10.8.1	If any sub-contracted external facilities or management services are used, appropriate security controls shall be in place. Such facilities and services shall be subject to the requirements stated in this	

			document.
	10.9	Internal audit and control	
		10.9.1	IT security controls shall be subject to a rigorous programme of internal monitoring, audit and maintenance to ensure their continued correct operation.
SM	10.10	Software Development	
		10.10.1	The software development processes for the SM-DP, SM-SR, or SM-DP+ or SM-DS shall follow industry best practices for development of secure systems.
DC		10.10.2	The software development processes for applications and bespoke software deployed within the SM environment shall follow industry best practices for development of secure systems.
DC	10.11	Multi-Tenancy Environments	
		10.11.1	Multi-tenant solutions must prevent cross-contamination of assets between different customers.
		10.11.2	Multi-tenant solutions on the same physical hardware shall ensure customer data is logically segregated between different customers.
		10.11.3	Each customer running their own applications must use a unique ID for that customer for the running of these application processes
		10.11.4	Restrictions shall be put in place for all customers on shared infrastructure by restricting use of shared system resources.
DC SM		10.11.5	The auditee shall ensure that customer data is only stored within SAS certified physical locations, including any Sites where data may be replicated to as part of business continuity plans, meeting all requirements detailed in section 5 of this document.

11 Two-Step Personalisation Process

I	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		
	11.1	Control of duplicate production	
		11.1.1	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
	11.2	Generation of hardware security credentials	
		11.2.1	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.
	11.3	Personalisation of security credentials (Perso_SC)	
		11.3.1	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.
		11.3.2	Perso_SC can occur only once within the device lifecycle.
	11.4	Generation of UICC OS credentials	
		11.4.1	The generation of UICC OS credentials shall be considered a sensitive process and be evaluated according to the requirements om section 7 of this document.
	11.5	Personalisation of UICC OS credentials (Perso_UICC)	
		11.5.1	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.
		11.5.2	Personalisation of UICC OS credentials to a device shall be carried

			out by establishing a secure channel that:	
			(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.
		11.5.3	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.

Annex A Document Management

A.1 Document History

Version	Date	Brief Description of Change	Editor / Company
1.0	26 Jul 2016	Created based on SAS-UP Standard document v6. 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
3.0	26 Jun 2019	Added two-step personalisation process (Integrated eUICC) requirements	Or Elnekaveh, Qualcomm & James Messham, FML.
4.0	25 Jul 2019	Added requirements for transfer of sensitive assets between sites.	SAS subgroup
5.0	18 Jun 2020	Development of remote user access requirements	SAS subgroup
6.0	20 Nov 2020	Add specific requirements for auditing of cloud service providers.	SAS subgroup
7.0	2 Jul 2021	Add new requirement 2.4.2 - clarify subcontractor responsibilities	James Messham, FML & Neil Shepherd, SRC
7.1	22 Sep 2021	Clarifications to HSM requirements. Addition of SAS-UP definitions.	Saïd Gharout, Kigen

A.2 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.

Your comments or suggestions & questions are always welcome.