Security Accreditation Scheme - Consolidated Security Requirements and Guidelines

Version 11.1

18 September 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

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 and Guidelines (CSRG) document. This document sets out:

- Statements of requirement that are relevant to SAS Auditees
- Guidelines associated with the requirements that provide practical guidance to SAS Auditees to help them design, implement and operate security controls that meet the requirements.

The guidelines in this document are intended to help Auditees understand how to interpret and apply the GSMA SAS standard operationally. The guidelines should be read and used in conjunction with the statements of requirement and relevant scheme Standard and Methodology and are not intended to replace or supersede these statements of requirement or documents.

1.2 Audits

The SAS Audit itself will remain the basis on which compliance with the SAS Standard is assessed. Certification by the GSMA will be based on the Audit Team's assessment and recommendation.

The Audit Team will consider the quality and effectiveness of the implemented solutions and security management system to ensure that:

- They are integrated into the normal operations of the business
- They make appropriate consideration of security risks at the Site
- They are sustainable
- Evidence exists of their ongoing successful application
- They comply with the basic principles of the Standard
- The quality of the solution is consistent with that judged acceptable at other, similar, Sites.

Where the Audit Team is not satisfied that sufficient evidence exists that the solutions in place satisfy the above criteria, certification may not be recommended, even where solutions are based on the guidelines in this document.

It is difficult for the Audit Team to assess processes or controls that are newly introduced due to the lack of evidence. When scheduling certification Audits, Sites are strongly recommended to ensure that evidence exists of 4-6 weeks of continuous operation of the controls to be audited. Where changes are minor, the Audit may consider evidence of previous versions of the process or control in addition to that in place at the time of the audit. In some cases, shorter periods of evidence may be acceptable.

Alternative solutions to those provided in the guidelines in this document may also be acceptable to the Audit Team if they do satisfy the above criteria.

1.3 Using this document

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

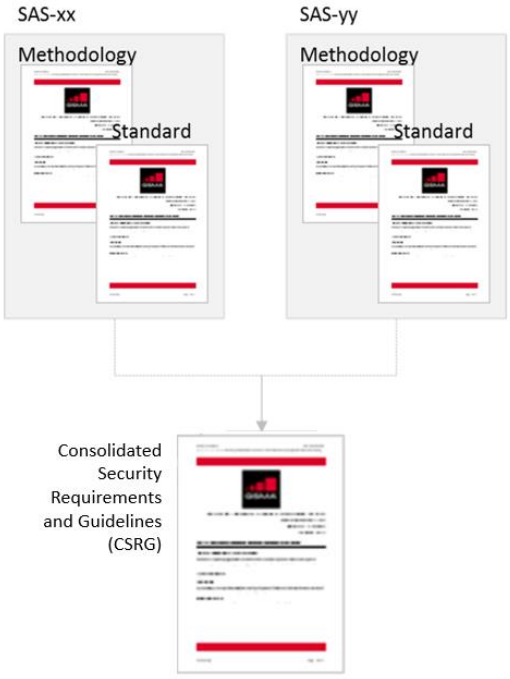
SAS Auditees are responsible for ensuring that they have determined which of the SPs and requirements are relevant to them. In the event of any query, Auditees should contact sas@gsma.com.

1.4 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 Group members
- SAS Auditors.

1.5 Related documents

This document is part of the Security Accreditation Scheme documentation published by the GSM Association. 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)** describes 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 through the accompanying *guidelines*.

Figure 1 - SAS Documentation Structure

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

References to the Standard and Methodology documents for each SAS scheme can be found in section 1.9.

1.6 Document Updates and Applicability

This permanent reference document is classified by GSMA as an Industry Specification (as defined in GSMA AA.35 – Procedures for Industry Specifications [13]) and is maintained by the GSMA in accordance with the provisions set out in AA.35. In addition to the provisions of AA.35, the following conventions are followed, and the following examples are provided in relation to updates of this document.

1.6.1 Substantive Changes to Requirements

From 1 April 2022, substantive changes to the requirements in this document may normally be made no more frequently than once every six months, with major releases (indicated by an increment in the first digit of the document version number) permitted on 1 April and 1 October only. Substantive changes to the requirements are changes that would materially affect how an Auditee would implement controls to comply with the requirements.

Examples of the contents of substantive changes to requirements are:

- “Shall” to “should” or “should” to “shall”
- The addition, deletion, or revision of requirements, regardless of the number of changes
- The addition or modification of mandatory compliance with referenced standards.

Following publication of a major release of this document, a 6-month phased introduction period from the date of issue of the major update is allowed before Auditees are required to demonstrate compliance with the new release. Accordingly, Audit assessments during the phased introduction period are only made against the requirements as specified in the previous version of this document. Audits carried out after the end of the phased introduction period will apply the normal assessment criteria against the latest version of this document.

1.6.2 Non-Substantive Changes

Examples of non-substantive changes are:

- Changes to requirements in this document that are not considered as substantive changes. For example:
  - Editorial changes
  - Error corrections and clarifications of requirements previously unclear
  - Changes to informative requirements text that is unlikely to significantly impact Auditees

  or

- Any changes to the guidelines in this document.

Non-substantive changes (indicated by an increment in the second digit of the document version number) may occur at any time subject to the normal GSMA document approval process. The latest version of the document becomes immediately applicable from its publication date.

1.7 Definitions

Term	Description
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).
Auditee's Corporate Network	A private IT network managed by the Auditee that is outside the scope of the SAS Audit.
Auditor	A person qualified to perform SAS Audits.
Bastion Host	See Jump Host
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	An entity responsible to issue Public Key Certificates. In the specific context of SAS, could be: • A GSMA CI [11] or an independent eSIM CA [12] issuing certificates for EUM and SM-XX or • The EUM issuing certificates for eUICC. See also "GSMA CI".

Term	Description
Class 1	Class 1 information, data or asset are protected in terms of integrity, authenticity, confidentiality and availability (e.g. private Keys).
Class 2	Class 2 information, data or assets are protected in terms of integrity, authenticity and availability (e.g. public Keys).
Discrete eUICC	An eUICC implemented on discrete standalone hardware, including its own dedicated volatile and non-volatile memory. A Discrete eUICC can be removable or non-removable.
Duplicate	Two or more assets of the same nature showing a set of information that should be individual according to the correct process
eIM Configuration Operation	As defined in SGP.32 [15][9].
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.
eSIM IoT remote Manager	The eSIM IoT Remote Manager is responsible for remote Profile State Management Operations (PSMO) on a single IoT Device or a fleet of IoT Devices. If supported by the eIM, the eIM can also be used to perform eIM Configuration Operations (eCO) on the eUICC when it is associated with the eUICC. See SGP.32 [15] for all the operations an eIM can perform.
eUICC	A removable or non-removable UICC which enables the remote and/or local management of Profiles in a secure way. NOTE: The term originates from "embedded UICC".
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 Personalisation	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 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 [11].
HSM	A physical computing device that provides tamper-evident and intrusion-resistant safeguarding and management of digital Keys and other secrets, as well as crypto-processing. FIPS 140-2 specifies requirements for HSMs. In the context of this document an HSM is defined by its FIPS 140-2 boundary.
HSM Partition	HSM Partition: An HSM Partition is an isolated environment in an HSM providing safeguarding and management of digital Keys and other secrets, as well as crypto-processing. An HSM Partition has its own data, access control, security policies and administration, isolated and independent from other partitions. The isolation might be logical or both logical and physical.

Term	Description
HSM Profile	A HSM account and its associated privileges and/or role. HSM accounts are commonly configured as administrator, Key administrator, Key custodian and application account.
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.
IoT Device	As defined in SGP.32 [15].
IoT Profile Assistant	As defined in SGP.32 [15].
Key	Any logical key (e.g. cryptographic key or certificate).
Key Ceremony	A formal session during which cryptographic Keys or certificates are generated by, and/or imported to, an HSM or Key management system. The ceremony is carried under the control of members of a Key management team according to defined procedures that are specifically designed to preserve confidentiality and integrity.
Multi-tenant	A software architecture in which multiple independent instances of one or multiple applications operate in a shared environment. The instances (tenants) are logically isolated, but physically integrated.
Personalisation	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	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.
Primary Site	See “Site”.
Profile	A combination of data and applications to be provisioned on an eUICC for the purpose of providing services. Profiles may be provisioned under the control of the EUM as part of the initial Personalisation process, or may be provisioned during the eUICC lifecycle through Platform Management.
Profile Management	A set of functions related to the downloading, installation and content update of a Profile in a dedicated eUICC.

Term	Description
Profile State Management Operation	As defined in SGP.32 [15].
Reject	Finished or partially finished product containing sensitive information which has been ejected from the process.
Re-personalisation	The process of re-using Personalisation Data to perform Personalisation of a device to replace one that has already been Personalised successfully, but subsequently rejected during the production 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 Group	A group of GSMA members and staff (including the Audit Management) that, together with the SAS Auditors, is responsible for maintenance and development of the SAS Standards, Methodologies, Consolidated Security Requirements and Guidelines,
Secondary Site	See “Site”.
Sensitive Data	Any information that could result in significant harm to the Auditee or its customer(s) through unauthorised or unintended disclosure or manipulation. Harm may be caused directly (e.g. disclosure of commercial or customer information) or indirectly (e.g. disclosure of information about security controls that could increase the risk of other security compromise). Examples of Sensitive Data would include: •Information classified as Class 1 under the SAS requirements (including Keys used to protect other Class 1 information). •Information classified in the upper levels of a typical information classification system (e.g. confidential / strictly confidential). •Status or configuration information that controls how Sensitive Data, systems or processes operate or are protected (e.g. transaction status information) •Detailed configuration information that describes physical and logical Environments that could be of use to an attacker (e.g. firewall rules, CCTV or intruder alarm configuration).
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.
Sensitive Process Data	Class 1 Sensitive Data relating specifically to the delivery of the SM or UP service
Site	Auditee’s physical facility and its relevant controls that are subject to the Audit. May be a: Primary Site — The main Audit site for which the SAS certificate will be issued. Supporting Site — Any independent locations that are subject to separate certification Audits. Audit findings will be documented separately in another SAS Audit report. Dependence of

Term	Description
	the Primary Site on the Supporting Site(s) will be noted as part of the certification of the Primary Site. Secondary Site: Any location directly supporting the activities of a Primary Site and included as part of the same Audit process and Audit report. Secondary Sites will not be issued with SAS certificates, but will be noted as part of the certification of the Primary Site.
Supporting Site	See “Site”.
Tenant	A single entity using one or multiple applications. Referred to as “single tenant” when operating in a dedicated logical and physical environment.
UICC	The platform, specified by ETSI, which can be used to run multiple security applications. These applications include the SIM for 2G networks, USIM for 3G, 4G and 5G networks, CSIM for CDMA, and ISIM (not to be confused with integrated SIM) for IP multimedia services. UICC is neither an abbreviation nor an acronym.

1.8 Abbreviations

Term	Description
BCP	Business Continuity Plan
CA	Certificate Authority
CM	Certificate Management
CSP	Cloud Service Provider
CSRG	Consolidated Security Requirements and Guidelines
eCO	eIM Configuration Operation
eIM	eSIM IoT remote Manager
eUICC	Embedded UICC (as defined above)
EUM	Embedded UICC Manufacturer
FIPS	Federal Information Processing Standard
FS.nn	Prefix identifier for official documents belonging to GSMA Fraud and Security Group
GSMA	GSM Association
HSA	High Security Area
HSM	Hardware Security Module
IPA	IoT Profile Assistant
IT	Information Technology
LMK	Local Master Key
LPA	Local Profile Assistant
MNO	Mobile Network Operator
PKI	Public Key Infrastructure
PRD	Permanent Reference Document
PSMO	Profile State Management Operation

Term	Description
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
SLA	Service Level Agreement
SM	Subscription Management
SM-DP	Subscription Manager – Data Preparation
SM-DP+	Subscription Manager – Data Preparation +
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

1.9 References

Ref	Doc Number	Title
[1]	PRD FS.04	GSMA SAS Standard for UICC Production
[2]	PRD FS.05	GSMA SAS Methodology for UICC Production
[3]	PRD FS.08	GSMA SAS Standard for Subscription Manager Roles
[4]	PRD FS.09	GSMA SAS Methodology for Subscription Manager Roles
[5]	PRD SGP.01	Embedded SIM Remote Provisioning Architecture
[6]	PRD SGP.02	Remote Provisioning Architecture for Embedded UICC Technical Specification
[7]	PRD SGP.21	Remote SIM Provisioning Architecture
[8]	PRD SGP.22	Remote SIM Provisioning Technical Specification
[9]	RFC 2119	“Key words for use in RFCs to Indicate Requirement Levels”, S. Bradner, March 1997.
[10]	BSI-CC-PP-0084-2014	Security IC Platform Protection Profile with Augmentation Packages. Version 1.0 (13.01.2014).
[11]	PRD SGP.14	GSMA eUICC PKI Certificate Policy
[12]	PRD SGP.28	eSIM CI Registration Criteria
[13]	PRD AA.35	Procedures for Industry Specifications
[14]	PRD SGP.31	eSIM IoT Architecture and Requirements
[15]	PRD SGP.32	eSIM IoT Technical Specification

1.10 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 [9].

2 Security Requirements and Guidelines

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 guidelines.

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/guidelines

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
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 Requirement Statements and Guidelines

Requirement Statements			Guidelines	
1 Policy, Strategy and Documentation				
All	The security policy and strategy provide 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.		A documented security policy should exist, either as a stand-alone document, or as part of a security manual. The policy should be a statement of overall security principles and management intent. The security policy document should be endorsed by senior management at the Site. The policy should be supported by appropriate documentation – either as individual policies, or as part of an overall security manual.
	1.1.2	Employees shall understand and have access to the policy and its application should be checked periodically.		Objectives and rules should be available to Employees. A mechanism should exist for ensuring that important changes to security rules and documents can be communicated effectively to all affected Employees.
	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		There should be evidence of a coherent security strategy based on a clear understanding of the risks, based on risk assessment, and design of the security management system to address them appropriately. There should be evidence of regular formal security risk assessments taking place. Results of risk assessment should be used to drive revisions to the security strategy and security management system. The risk assessment methodology should demonstrate clear structures for:

Requirement Statements			Guidelines	
		changing security environment through ongoing re-assessment of risks.		•Risk identification; •Assessment/evaluation of the identified risks. The SAS Standards set out one sample framework for risk identification. Many formal methodologies exist for risk assessment, although most will involve evaluation of likelihood and impact (possibly in conjunction with other factors) on defined scales. Such scales should be clearly defined to ensure that they are applied in a consistent and repeatable way, e.g. by quantitative definition. Whilst the same risk assessment methodology can often be applied to different types of risk it is normally beneficial for a security risk assessment to be undertaken separately from other risk assessments (e.g. Business Continuity) to ensure correct focus on the relevant assets and threats.
	1.3	Business Continuity Planning		
	1.3.1	Business Continuity measures must be in place:		The Business Continuity plan (BCP) should be developed as a working business document (rather than one developed specifically for SAS compliance). The BCP should reflect the availability requirements of the SP and any specific customer service level agreements (SLAs) in place. SAS compliance will require specific issues to be addressed, including: •Definition of incidents that critically affect the SP based on a Business Continuity risk assessment and impact analysis; •Processes for management of scenarios that affect the SP; •Mechanisms and processes in place to ensure continuity of operations; •Management of customer contact and customer data; •Maintenance of the integrity of the security system and production processes. All personnel with BCP responsibilities should receive formal training.

Requirement Statements			Guidelines	
				The BCP should be subject to periodic testing (e.g. once per year). Scenario-based testing will normally be appropriate for most periodic tests. For the purpose of SAS, a scenario-based test would typically comprise a simulation of a BCP incident: •A sample scenario is defined that could or would lead to a Business Continuity incident. •Key personnel are presented with the scenario. •The BCP team execute the BCP as a simulated desktop-based exercise. Each member of the team role-plays their individual actions and interactions. •Interfaces to external stakeholders (customers, suppliers, corporate teams) may be tested from time to time as appropriate but will normally be simulated. •At the end of each test a review will allow improvements to the plan and to team training to be identified. Scenarios should be selected that exercise all elements of the BCP for response and recovery. Scenarios should be varied for each test to ensure appropriate coverage of all elements of the BCP.
	(i)	to ensure an appropriate level of availability		Availability requirements will vary dependant on the SP, its implementation and the relationship with other entities (e.g. customers). Auditees will always be required to make clear the level of availability that is required for the relevant SPs and the relationships with other entities (e.g. by contract).
				Where high availability is required then appropriate controls should be in place, to consider where applicable: •Continuous, uninterrupted access to electric power; •Control of temperature and relative humidity within a defined operating range; •Live switchover to an alternative / backup site where necessary.

Requirement Statements			Guidelines	
			CM	Facilities should be sufficient to: •Lock out input, finish any pending actions, and record the state of the equipment automatically before a shutdown; •Provide sufficient continued operation for repositories (containing Certificate Authority (CA) Certificates and Certificate revocation status) in the absence of commercial power, to maintain the required level of availability.
			UP	There is no specific requirement within SAS-UP for a backup site, however Sites with no backup agreement should ensure that this is contractually acceptable to customers.
	(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.		A programme of internal checks and audits should be defined that demonstrates appropriate consideration of: •The frequency of checks required for each area addressed by the internal audit mechanism; •The structure of the audits themselves, including clear guidance on what should be checked and how. The recording / documentation and follow-up process for audits undertaken. The Auditors will expect to see evidence that processes and systems are working correctly, and that internal checks have been carried out according to the schedule. There should be appropriate coverage of all aspects of the system; the audit programme should be defined around the need to provide appropriate coverage, rather than the availability of audit resource. The programme should normally consider controls at a number of different levels:

Requirement Statements			Guidelines	
				• Operational controls and checks should be conducted regularly as part of the normal function of each area, or as an integrated part of business processes. Such checks may be conducted by operational or supervisory personnel within the area, or as an independent control by an auditor or audit group from another business area. • Independent checks should be conducted periodically to validate the effectiveness of the operational controls. Checks should be conducted by an auditor or audit group independent of operational or supervisory personnel from the area concerned. ○ Records of operational controls should be checked to ensure their completeness. ○ Independent validations of their effectiveness should also be carried out. • Reviews of the whole audit system should be conducted periodically to ensure the completeness and appropriateness of its coverage. • Additional levels may be required in some areas, dependent on the scale of the operation. • Care should be taken to ensure that a rigid or prescriptive audit system does not prevent identification of new or emerging issues. Auditors should have received appropriate training in the structure and content of internal audits.

Requirement Statements			Guidelines	
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.		The security organisation should be clearly defined and documented as part of the security management system.
	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.		A cross-functional forum for discussion, escalation and resolution of security issues and solutions should exist and meet regularly (at least once per quarter). The forum should include senior management representatives. Evidence should exist of forum meetings taking place.
	2.2	Responsibility		
	2.2.1	A security manager shall be appointed with overall responsibility for the issues relating to security in the SP.		Security responsibilities of the security manager should be clearly defined. Although it may not always be appropriate to have a dedicated / full-time security manager role, Auditees should be able to demonstrate that sufficient time is available for security management activities.
	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.		Responsibilities should be clearly documented and well understood within the business. Where security management roles are defined separately (e.g. physical and IT security), suppliers should be able to demonstrate an overall co-ordinated / integrated approach to security management with responsibilities clearly defined.
	2.2.3	Asset protection procedures and responsibilities shall be documented throughout the SP.		Employees should be made responsible and accountable for sensitive assets (both physical and information) within their care throughout the Sensitive Process.

Requirement Statements			Guidelines	
				Responsibility should be clearly defined, even where assets are in intermediate / temporary storage between Sensitive Process stages, such that a clear 'owner' can always be identified. Control of access to assets should reflect the assigned responsibility (such as Key management, customer interface, IT administration). Procedures for documenting handover of assets should be clearly defined. Asset protection mechanisms applicable at each processing stage should be documented as part of the production process and supporting documentation. Protection mechanisms should be clearly understood by the Employees affected.
	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:	All	An escalation process / mechanism should be in place where security breaches are identified. When any security breach is identified, an incident management process should be activated including impact analysis, setup of remediation plan and notification to any external third parties possibly impacted. All such security breaches should be tracked and reported.
			CM	The incident response mechanism should require the Public Key Infrastructure (PKI) Policy Authority to be promptly notified of any incidents that may have affected the integrity and trust of the PKI.

Requirement Statements				Guidelines	
	(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.			Contracts with customers and suppliers should clearly define responsibility and liability for loss. Where contracts with customers are not standardised (i.e., different contracts may be agreed with different customers) mechanisms should exist to ensure that all contracts are in line with an overall framework for liability and loss. Evidence should exist that the supplier is able to cover its liabilities for loss of physical assets or data, and for consequential loss where defined within contracts. Normally it will be expected that insurance will be in place to cover such losses.
	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.			Outsourcing agreements may relate to: •Personnel (that are not Employees of the Auditee) conducting activities at the Primary certified location; •Separate physical locations (Secondary or Supporting Sites) where substantive elements of the activities within scope of SAS certification are carried out.

Requirement Statements				Guidelines	
					The concepts of Primary, Secondary and Supporting Sites within SAS certification are defined within the respective sections of the SAS-UP (FS.05) and SAS-SM (FS.09) Methodologies. The overall objectives are always to ensure that an equivalent level of control is applied to activities that are outsourced, compared to those carried directly by an Auditee, and that the Auditee has assurance of this.
	(i)	Responsibilities that fall within the scope of the Auditee's SAS certification shall be clearly documented and agreed.			Contracts or associated documents (e.g. service level agreements) should clearly define the role and responsibilities of outsourcing partners that provide services to the Auditee that fall within the scope of the SAS Audit. These documents will often form part of the standard business level agreement, rather than being something created specifically for the purpose of SAS certification. Where the sub-contractor is specifically required to operate or maintain security controls there should be clear references to the internal or external standards that must be maintained. •For outsourced personnel operating at the primary certified Site, this may simply be a requirement for them to work in-line with the Site's own local security policies. •For physically separate Sites, these standards may be the Auditee's own internal/corporate standards, specific requirements defined as part of the contract, or may be references to external standards (such as the SAS requirements).
	(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			New contracts should always have a right-to-audit clause included to enable the Auditee's internal audit team to validate the responsibilities of the outsourcing partner or sub-contractor. Where existing contracts do not contain a right-to-audit clause, Auditees should work with the external providers to ensure that operational agreements are in place to facilitate reasonable audit requests, with mechanisms to escalate where co-operation is withheld without good reason. Where applicable, contracts should clearly define the responsibility to maintain compliance with the relevant SAS requirements and to participate in the SAS Audit process. This applies regardless of whether the external provider is an

Requirement Statements				Guidelines	
		to participate in the SAS Audit process, where applicable.			outsourcing provider working on-site, an independent participant in the scheme, or a Secondary or Supporting Site to the Auditee's own certification. Auditees should be aware that refusal by an outsourcing partner or sub-contractor to co-operate or participate in an SAS Audit process may critically impact the Auditee's own ability to achieve certification.
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.			The strict obligation to hold SAS-UP certification for eUICC production activities applies to destination sites performing any of: •"EUM PKI Certificate Management" (where GSMA PKI certificates are in use); •"Generation of Data for Personalisation"; •"Personalisation". Destination sites performing "Post-personalisation packaging" of eUICCs only are not required to be SAS-UP certified under this requirement. Where SAS-UP certified Sites are transferring Class 1 assets related to eUICC production, contracts with each receiving site should mandate that the site holds SAS-UP certification for the activities within scope of SAS-UP that are performed.
	(i)	eUICC production data must only be supplied to SAS-UP Sites that have the appropriate scope of certification 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 [5] and SGP.02 [6], SGP.21 [7] and SGP.22 [8], or SGP.31 [14] and SGP.32 [15] 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.			

Requirement Statements			Guidelines	
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.		An information and asset classification structure should be documented that is consistent with, or exceeds, those set out within the relevant SAS standard. The classification structure should not exist in isolation. Evidence should exist that the classification structure: •Links to a set of asset protection requirements / standards; •Maps onto business processes to identify where sensitive assets are handled, and the asset protection standards are applied; •Specifies the treatment during the entire lifecycle (that is, creation, processing, storage, transmission and disposal). The Auditors will expect to see evidence of the classification structure being applied throughout the operation during the Audit.
	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.		Individual physical and logical access rights should be formally documented. The ‘need to know’ principle should be used to ensure that an individual is granted no more than sufficient access to perform his or her job.
	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.		A clear desk policy should be defined that considers both electronic and physical information assets. Guidelines should be in place to assist Employees in understanding the asset classification scheme and defining the treatment of assets throughout their lifecycle.

Requirement Statements			Guidelines	
				Specific controls should be in place for the secure handling of all media at end-of-life. Procedures should be in place for: •The disposal of sensitive information to prevent its unauthorised use, access, or disclosure; •The treatment of Sensitive Data in electronic form stored on old or faulty equipment.

Requirement Statements			Guidelines	
4 Personnel Security				
All	A number of security requirements shall pertain to all personnel working within the SP and those with trusted positions.			General requirements should be applied to all personnel working inside the Site where SPs are conducted. Trusted positions include all Employees (both permanent and temporary), contractors, and consultants that have access to or control:
			All	•Sensitive information or assets.
			CM	•Those authentication or cryptographic operations relevant to the SP at the Site that may materially affect the following functions (typically applicable only to CAs): ○ The acceptance, rejection, or other processing of Certificate Applications, revocation requests, or renewal requests, or enrolment information; ○ The issuance, or revocation of Certificates, including (in the case of Processing Centres) personnel having access to restricted portions of its repository; ○ The handling of Subscriber information or requests.
	4.1	Security in job description		
	4.1.1	Security responsibilities shall be clearly defined in job descriptions.		All individuals having: •Access to sensitive assets; •A specific security role or security responsibilities should have a job description in which security tasks are clearly defined. For all other individuals a general security declaration should be defined.
	4.2	Recruitment screening		
	4.2.1	An applicant, and Employee, screening policy shall be in place where local laws allow		All Employees should be subject to a screening process that should include: •Formal interview;

Requirement Statements			Guidelines	
				•Validation of education and employment history. Clear policies should be defined for the periods of employment history that should be validated. Where local laws allow, screening should also include: •Criminal background checks; •Credit checks. Where permitted, re-checking of criminal background and credit checks should be carried out on a regular basis (e.g. every 1 or 2 years). All checks should be documented to ensure that there is an auditable record of what checks were carried out, when and by whom.
	4.3	Acceptance of security rules		
	4.3.1	All recruits shall sign a confidentiality agreement.		All Employees should sign a confidentiality agreement as part of, or in parallel with, their contract of employment. Agreements should define clear obligations to maintain confidentiality beyond the end of the period of employment. Obligations should persist until such time as information is no longer confidential (e.g. due to the company de-classifying or publishing the information). Temporary Employees, contractors and visitors should sign confidentiality agreements.
	4.3.2	Employees shall read the security policy and record their understanding of the contents and the conditions they impose.		All Employees should sign to indicate their understanding and accepting of the security policy as part of, or in parallel with, their contract of employment. Employees should be reminded of their acceptance of the security policy on a regular basis. Employees may be requested to re-confirm their acceptance of the policy on a regular basis; this may be done as part of the refresher training programme (see 4.3.3).
	4.3.3	Adequate training in relevant aspects of the security management system shall be provided on an ongoing basis.		The scope and frequency of the security training awareness programme should be clearly defined, along with responsibility for its deployment and monitoring. All new Employees should be provided with training covering basic security principles applicable throughout the Site (e.g. general rules surrounding physical

Requirement Statements			Guidelines	
				and logical security, information security, security organisation and responsibilities, incident reporting): •As part of the induction process; •As part of a programme of regular refresher training (e.g. annually). Specific, focused, security training should be conducted for Employees: •With specific security responsibilities; •With access to high security areas; •Participating in Sensitive Processes. Employees may be asked to re-confirm their understanding and acceptance of security policy as part of refresher training. Mechanisms should be in place to ensure that all Employees receive the appropriate security training; auditable records should exist of training taking place, and those Employees trained. Access (both physical and logical) should be contingent on maintaining the appropriate level of security training.
	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.		Mechanisms should be in place for Employees to make confidential reports of security incidents or suspicions. Follow-up and escalation mechanisms should exist for incidents reported.
	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.		Exit checklists should be in place to ensure that company property has been retrieved and all privileges (e.g. physical and logical access) have been revoked. Procedures should exist to escort Employees from the premises where appropriate.

Requirement Statements		

Guidelines	
	Employees should be reminded of their obligations under the confidentiality agreement prior to leaving the company.

Requirement Statements			Guidelines	
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.		Security risk assessments should be conducted / updated on a regular basis (e.g. annually). Risk assessment findings should be used to drive continuous improvement and modification of controls.
	5.1.1	The strategy shall be encapsulated in a security plan that:		
	(i)	defines a clear Site perimeter / boundary		The Site boundary / perimeter is considered to be the point at which physical security controls - considering physical protection and access control - begin. Sites will vary in their definition of the boundary / perimeter. The boundary / perimeter from a physical security perspective will not always be the same as the boundary of the Site itself (for example, where there is no boundary fence). In all cases Sites will be expected to have considered, and defined, the Site boundary and its role within the overall protection strategy for the Site.
	(ii)	defines one or more levels of secure area within the boundary of the Site perimeter		It is expected that all sensitive assets will be wholly contained within one or more high security areas (HSA) throughout their lifecycle.

Requirement Statements			Guidelines	
				HSAs should be clearly defined and documented to include: •The perimeter of the HSA; •The protection measures used to secure the HSA. Suppliers may choose to define several levels of HSA, to reflect the sensitivity of assets contained.
	(iii)	maps the creation, storage and processing of sensitive assets to the secure areas		The lifecycle of sensitive assets should be mapped against the HSAs defined.
	(iv)	defines physical security protection standards for each level of secure area		The expected, or required, physical protection standard for each level of HSA should be defined, to consider those elements defined in 5.2.1. Where multiple levels of HSA are defined, protection standards should be defined for each.
	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		Sites should make use of visible security mechanisms to act as a deterrent, which may include: •Fences at the Site boundary; •Perimeter lighting; •CCTV; •Access control; •Guard presence / Site monitoring.
	(ii)	deterrent to attack or unauthorized entry		Response and escalation times for secure areas should be defined. Requirements for attack times for secure areas should be set accordingly. Physical protection of secure areas should achieve, or exceed, stated attack times by ensuring that: •Walls are of strong construction;

Requirement Statements			Guidelines	
				•Points of access (windows and doors) to HSAs are minimised; •Doors and windows giving direct access into secure areas from outside (e.g. emergency exit doors) are physically hardened to increase attack time. Suppliers should pay particular attention to the design of hinges and locking mechanisms used on access points to secure areas from outside: •Multi-point locking mechanisms (including emergency doors) should be used. •Removal or cutting of hinges should not allow doors to be opened.
	(iii)	mechanisms for early detection of attempted attack against, or unauthorized entry into, the secure areas at vulnerable points		When considering attack and response times, a response will be triggered only when an attack is identified. Sites should identify vulnerable points for access to secure areas (doors and windows; walls of weak construction; roof accesses). Detection mechanisms should be in place to identify attacks against these areas when they are taking place, rather than when they are successful. Mechanisms may include: •Movement detection sensors (microwave or infra-red); •Barrier systems (microwave or infra-red); •Seismic and vibration sensors; •CCTV movement detection (based on automated image analysis).
	(iv)	control of access through normal entry / exit points into the building and SP to prevent unauthorized access		Automated access control systems should be in use.
	(v)	effective controls to manage security during times of emergency egress from the secure area and building		It is accepted that the priority during emergency evacuation of buildings is to ensure the safety of people. However, emergency evacuations often introduce vulnerabilities in Site security, and may be exploited by attackers. Mechanisms should be in place to protect sensitive assets during such evacuations. Evacuation procedures should consider: •Responsibility for ensuring that high security areas are cleared of all personnel during evacuation. •Attempts to restrict unauthorised re-entry to buildings and high security areas, including:

Requirement Statements			Guidelines	
				• Monitoring of emergency exit doors by nominated personnel; • Use of self-closers on emergency exit doors. Procedures for addressing weaknesses in physical protection introduced as a result of emergency incidents (e.g. damaged security systems or physical controls). Mechanisms to ensure that all assets are accounted for prior to SPs re-commencing.
	(vi)	mechanisms for identifying attempted, or successful, unauthorized access to, or within the Site		Intrusion detection (alarm) systems should be in use. The alarm system should make appropriate use of detection technologies to protect the secure areas, configured as one or more detection zones within the alarm system. Mechanisms should be in place to ensure that alarm zones are armed in accordance with a defined policy. Consideration should be given to automatic arming of alarm zones covering sensitive areas (e.g. data processing rooms, production server rooms, areas used to store or process Class 1 assets) when they are not occupied. Alarms should be recorded to a system-generated log. Controls should be in place to enforce the integrity of the log. Actions taken in response to each alarm should be recorded as part of the response process. Independent checks should be carried out to validate that reasons are recorded for all alarms.
	(vii)	mechanisms for monitoring and providing auditability of authorised and unauthorised activities within the SP		CCTV systems should be in use. CCTV images should be recorded and retained for a minimum of: •90 days where this is legally permissible; •The maximum period legally permitted where this is less than 90 days. • Sites may be asked to provide evidence of legal restrictions. It is acceptable for image capture and recording to be event-driven. Images should be recorded with sufficient frequency to provide good auditability of activities. As a guide:

Requirement Statements			Guidelines	
				•Cameras providing general coverage of movement of larger assets (e.g. packaged, sealed boxes), or of personnel movement, should typically exceed 3fps; •Cameras providing detailed coverage of Sensitive Processes involving handling of individual UICCs should typically exceed 6fps; •Some applications may demand higher frame rates, particularly where cameras are an integral part of the control systems used for counting product. Appropriate illumination should be provided for external CCTV cameras. Stored / archived CCTV images should be retrievable for specified dates / times / locations. Physical and logical controls should be in place to preserve the integrity of the CCTV recordings arising from: •Unauthorised manipulation of / interference with the recorder hardware; •Unauthorised access to suppress, delete or overwrite video files. Where digital CCTV systems are in use, mechanisms should be in place to ensure sufficient storage space is available. Compression settings for images should be chosen carefully to ensure that image quality is not adversely affected. Positions of fixed cameras should be clearly defined. Reference images should be available for security / control room personnel to enable positions and live images to be validated. CCTV systems should be checked regularly to identify problems with cameras, images or system equipment, including: •Quality of live images, considering clarity, focus, exposure / light balance; •Quality of recorded images, considering clarity, compression, actual frame rate, continuity and retention period; •Correct framing of images (using reference pictures). Procedures for maintenance (including regular cleaning of camera housings) should be in place.

Requirement Statements			Guidelines	
	5.2.2	Controls deployed shall be clearly documented and up-to-date.		Physical security controls should be clearly documented and available to relevant Site personnel. All changes to physical security controls should be documented.
	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.		An access control policy should be in place, enforced by an access control system. The policy should define authorities for access to secure areas by Employees, visitors, contractors and security personnel. All Employees should be issued with ID cards. Configuration of access rights should be under strict control. All changes to access rights should be auditable and accountable to the operator making the change and awarded on a strict need to access basis. Specific controls should be in place to prevent Employees from accessing secure areas in excess of their own privileges resulting from: •Ability to change or re-assign access rights in the access control system; •Access to highly privileged access rights or cards intended for Employees, visitors or emergency access. Where highly-privileged access cards are handled by, or accessible to, Employees additional controls should be in place to prevent unauthorised use. Visitors to secure areas should be authorised by an appropriate authority according to a defined procedure. All visitors requiring access to secure areas should be registered in the access control system. Movement of materials to/from the HSA(s) should be controlled. Transfer of materials should be controlled using an intermediate / buffer zone or materials trap, e.g. within the delivery bay area. In production Environments, vehicle movements should be logged and drivers positively identified before being admitted to delivery bays. Separation should be enforced between personnel inside secure areas and delivery drivers / vehicles. All Physical Keys managed as part of the Site's security management system should be catalogued. Issue of keys to Employees should be tracked according to

Requirement Statements			Guidelines	
				an auditable system. Keys to secure areas should be under strict control and subject to regular audit.
	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.		All access to secure areas should be strictly controlled and auditable using the access control system. One-by-one mechanisms should be in use to strictly control access to HSAs. Anti-passback controls should be in place for access to, and within the HSA. All Employees, visitors and contractors to the secure areas should be uniquely identifiable to the access control system. Access to sensitive locations within the high security areas should make use of two-factor authentication (e.g. ID card + PIN), or dual control (e.g. 2 people must be present within the area). Sensitive locations may include: •Secure storage (vault areas); •Data processing rooms; •Key Ceremony rooms; •Server rooms. Movements into, and out of, the secure areas, and between defined zones within the secure areas should be tracked by the access control system. Attempts to enter access control zones should be logged by the access control system and reviewed; repeated attempts to exceed access privileges should be followed-up with Employees. Access to secure production areas where Class 1 and Class 2 assets are created, stored and processed should be enforced on a one-by-one basis. Access to secure areas where Class 1 and Class 2 assets are created, stored and processed should be on a strict ‘need to be there’ basis, covering Employees, contractors and visitors to the Site. To enforce a ‘need to be there’ principle, consideration should be given to separation of secure areas where Class 1 and Class 2 assets are processed.
	5.4	Security staff		

Requirement Statements			Guidelines	
	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.		Security staff should have received specific training in their roles and responsibilities and operational procedures. Security staff should have an understanding of the operations of the Site and the sensitive assets handled. Operational security procedures should be clearly documented, and available to security staff within the control room. Security staff should be familiar with the security systems provided (access control, alarm system, CCTV system). The Auditors expect that security staff will demonstrate a basic competence in their operation during the Audit.
	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.		A programme of internal audits/controls should be defined that demonstrates appropriate consideration of: •The frequency of checks required for each area addressed by the internal audit/control mechanism; •The structure of the audits/controls themselves, including clear guidance on what should be checked and how; •The recording / documentation and follow-up process for audits/controls undertaken. The Auditors will expect to see evidence that processes and systems are working correctly, and that internal audits/controls have been carried out according to the schedule. There should be appropriate coverage of all aspects of the system; the audit/control programme should be defined around the need to provide appropriate coverage, rather than the availability of resource. In particular, there should be evidence that the internal audit system has been designed to validate all of the physical security controls in place, including regular testing of systems. Auditors should have received appropriate training in the structure and content of internal audits/controls.

Statements from CSR				Guidelines	
6 Certificate and Key Management					
All	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 CA(s) 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.			Systems used for processing and storage of Keys and certificates should be configured, managed and operated in-line with the relevant requirements for infrastructure security from the CSR and CSG. Specifically, systems should be: •Managed consistent with the requirements in section 10; •Operated in an Environment consistent with the requirements of section 5; •Operated by personnel subject to the controls described in section 4.
				DC	The same requirements apply to an Auditee offering hardware security modules (HSM) managed as a service (see section 6.7).
	6.2	Roles and responsibilities			
	6.2.1	Management of keys shall always take place under the direct control of the Auditee. Responsibilities and procedures for the management of certificates and cryptographic Keys shall be clearly defined. Except for activities permitted under 6.7.2, Key management activities shall only be undertaken by authorised personnel		UP SM CM	Key management activities should not be outsourced, but always be carried out by a team of individuals that are part of, appointed by, accountable to, and have an employment contract with the Auditee (i.e., Auditee Employees). A Key manager should be assigned to manage the overall responsibility of the cryptographic systems and Key management. A back-up Key manager should also be appointed. Key management activities should be conducted using fully authorized and trained personnel.

Statements from CSR				Guidelines	
		that are directly accountable to, and have an employment contract with, the Auditee.			All personnel should: • Be formally appointed following completion of appropriate enhanced vetting controls to confirm their suitability. • Have formally accepted their duties and their responsibility. Be subject to periodic re-vetting to reconfirm their suitability.
				DC	In the case of an HSM managed as a service (see section 6.7), HSM infrastructure management activities should be conducted using fully authorised and trained CSP personnel.
UP SM CM	6.2.2	Auditable dual control shall be applied to sensitive steps of Key management.			All Key management activities that take place at the Site and are relevant to the SP, except component loading/extraction, should be conducted under dual control. These activities may include some or all of:
				UP SM CM	•The administration of Key management systems and mechanisms: ○ Set up; ○ Configuration; ○ Maintenance; ○ Management of user profiles; ○ Operations on cryptograms; ○ Key files back-up and restore.
				CM	•And the following activities typically applicable only to the CA itself: ○ Validation of information in Certificate Applications; ○ Acceptance, rejection, or other processing of Certificate Applications, revocation requests, Key recovery requests or renewal requests, or enrolment information; ○ Issuance, or revocation of Certificates, including personnel having access to restricted portions of the repository; ○ Handling of subscriber information or requests; ○ Generation, issuing or destruction of a CA Certificate;

Statements from CSR				Guidelines	
					•And the following activities typically applicable only to a sub-CA: ○ Loading or removal of a CA to/from a production Environment.
UP SM CM	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.			The CSRG does not describe technical specifications for cryptographic Keys and certificates. Requirements will vary dependant on the value of the assets to be protected, the Environment(s) in which they are used and the expected lifespan. Advances in computing power and developments in cryptanalysis techniques will drive changes/obsolescence of acceptable algorithms and Key lengths over time. Where technical standards or requirements are laid down for Keys/certificates (e.g. as part of contractual agreements for participation within an ecosystem) then Auditees will be expected to demonstrate that implementations are compliant with the relevant specifications, including: •Section 2.3.3 of SGP.02 [6], which specifies the secure channel Key length and algorithm used on the ES5 interface (SM-SR - eUICC); •Section 2.5 of SGP.02 [6], which specifies the secure channel configuration, Key length and algorithm to be used on the ES8 interface (SM-DP - eUICC); •Section 2.6.5 of SGP.22 [8], which specifies the Key length and algorithm to be used for remote secure communication involving an SM-DP+. •Section 2.6.4 of SGP.32 [15], which specifies the Keys, Certificates, and algorithms to be used for remote secure communication involving an eIM. Where no specific technical standards are laid down, then Auditees will be expected to demonstrate application of appropriate best-practice in selecting cryptographic algorithms and Key lengths.

Statements from CSR				Guidelines	
	6.4	Cryptographic Key management			
	6.4.1	Cryptographic Keys, certificates and activation data shall be generated, exchanged, stored, backed-up and destroyed securely.			Keys should be only used for the purpose intended. Key management should be governed by the following two major principles: •Knowledge is always split (not accessible by one person alone); •Process activities are conducted under dual control. A Key should only be in clear-text form when residing within the HSM. Outside of the HSM, Keys may only exist in the form of a cryptogram or be split into a minimum of 2 components. Where Keys are split into components, the individual components should be under the sole control of the relevant and designated custodian only. Principles should apply during the whole life cycle. Test Keys and Live Keys should never be found on the same operational system. Prototypes are understood to be “test” Keys, though “pilot” Keys are deemed “live” Keys associated to production. Key management activities should be operated in a separate area within the HSA where access to the area is logged via the Access Control system and equipped with intrusion detection and CCTV. Key lifecycle Generation •Entities responsible for the generation of Key pairs should ensure that Key pairs are generated: ○ By an appropriate mechanism (e.g. during a formal Key Ceremony); ○ In an Environment with appropriate protection. Exchange and storage •Key component and related Sensitive Data should be stored securely under the control of the respective owning custodian. •During Key transport, the Key received from a 3rd party should be conveyed either as a cryptogram or in minimum 2 components exchanged between authorized custodians and exchanged using tamper evident serialised envelope.

Statements from CSR				Guidelines	
					○ Key components should not be opened or accessed outside of the secure Environment where the Key Ceremony takes place. •Keys should be loaded under appropriate control (e.g. during a formal Key Ceremony). •After successful loading of a Key, the Key components should be destroyed. •Controls should be in place for the exchange of public Keys to ensure trust by the recipient. ○ Specific formal methods for exchange and validation should be used for public Keys submitted for signing to a Certificate Authority. Backup •Where Key backups are manually generated, these should be performed under dual control. •Where Key backups are automatically generated, restore should be performed under dual control. •The security level of the backup should equal at a minimum that of the Key being backed up. •CA private signature Keys should not be archived or escrowed. Destruction •Appropriate mechanisms should be used for the destruction of Keys and Key components to prevent their theft, disclosure or unauthorized use. Where relevant to the SP, activation data used to unlock private Keys should: •Have an appropriate level of strength for the Keys or data to be protected; •Be appropriately protected throughout its lifecycle to prevent loss, theft, modification, disclosure or unauthorized use; •Be updated as appropriate. Auditees should be capable of demonstrating a Key Ceremony (for example during a dummy/simulated ceremony) which shows that: •Defined processes are followed correctly;

Statements from CSR				Guidelines	
					•Dual control and required restraints during the ceremony are applied appropriately and are effective; •At no time Keys or components are disclosed or visible to any unauthorised person; •Audit log reports are correctly established and maintained.
	6.4.2	The cryptographic Key management process shall be documented and cover the full lifecycle of Keys & certificates.			This documentation should specify the actors (Key custodians), the involved Keys, the entire lifecycle management (generation, distribution, loading, storage, usage, backup/recovery, destruction, audit trail) and incident management (compromise).
CM SM DC	6.4.3	The storage and cryptographic computation for Keys and certificate generation (derivations, random generations) involved in the protection of the Sensitive Process Data (i.e., Class 1 data) shall rely on hardware security modules (HSM) that are either: (i) FIPS 140-2 level 3 certified and in live use by 21 September 2026. or (ii) FIPS140-3 level 3 certified. or (iii) Common Criteria EAL4+/AVA_VAN.5 certified		CM SM	This requirement is mandatory for: • Private Keys used in session Key derivation and signing for Profile Binding (e.g. SM-DP and SM-DP+); • EUM private Keys used to sign eUICC certificates. It is not mandatory for the private Keys used in TLS/DTLS session between server (e.g. SM-DP+ or SM-DS, eIM) and local profile assistant (LPA) / IoT Profile Assistant (IPA), or mutual authentication between server (e.g. SM-DP+ or SM-DS) and eUICC as per the protocols defined in SGP.22 [8], or the eIM private Keys used to sign eUICC Packages. Cryptographic Keys related to IT protocols between servers (e.g. between SM-DP and SM-SR) are out of the scope of SAS-SM. The service provider should provide a copy of the FIPS or Common Criteria certification proving the identification of the hardware board and associated firmware of the cryptographic device used. Equipment should be subject to a documented commissioning and/or decommissioning process. Customization of cryptographic devices is acceptable as long as native functions (Key generation, Key diversification, random number generator, algorithmic computation) are not altered. HSMs used for CM (e.g. EUM) or SM (e.g. SM-DP+) functions should be dedicated to those sole purposes.

Statements from CSR				Guidelines	
					Sites may use a single HSM for EUM and SM functions, provided that: •SM and EUM Environments are logically separated, as described in 10.5.1. •The shared HSM is configured to provide only the required HSM services to the SM and EUM Environments, and to prevent any direct connection between the two Environments. •The HSM is logically partitioned, with SM and EUM activities utilising different HSM Partitions, each exposed only to the relevant logical Environment. •Each HSM Partition is configured with its own Master Key, generated and managed according to secure processes under the control of the relevant team. •The HSM is subject to the full scope of the logical, physical, Key management and data processing elements of all SAS Audits carried out on-site at both a platform and partition level. •The Auditee accepts that the use of a shared physical HSM for SM and EUM activities will be noted in the Site's certificate and be visible to MNOs and other end-users. •The HSM is not used for any other purpose where: ○ Lower security levels than those required by SAS-UP/SAS-SM are applied; ○ The management of the HSM is carried out by personnel other than those included in the SAS Audit processes; ○ Connections are made to the HSM from outside of the logical or physical Environments within the scope of the SAS Audit processes. Any activity on the HSMs should be logged. The integrity of audit trail logs should be ensured.

Statements from CSR				Guidelines	
				DC	For HSM managed as a service (see section 6.7), the Auditee should provide a copy of the FIPS or Common Criteria certification proving the identification of the hardware board of the cryptographic device used. Equipment should be subject to a documented commissioning, decommissioning, allocation and/or de-allocation process.
	6.5	Auditability 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.			All Key management processes should be documented in an audit trail that: •Gives evidence as to all operations, Key usage, equipment and roles involved in the process; •Is clearly documented (who, when, what, why) for the full life cycle of Keys and systems deployed. All activities related to Keys/Key management should be logged. Integrity of the audit trails should be ensured and protected against manipulation.
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 authorised by and acting on behalf of the GSMA			The Auditee should verify that the CA is authorised and acting on behalf of the GSMA and that certificate issuance is done in accordance with the official GSMA procedure. Only duly authorized staff of the supplier can request services from the CA.
	6.6.2	PKI certificate private Keys shall only ever be installed and used at sites:			The GSMA eUICC certificate policy is published as SGP.14 [11]. Auditees can obtain the certificate policy and details of the scope of SAS certification for each certified Site from the GSMA website.
	(i)	That are agreed with the GSMA.			
	(ii)	That are SAS certified with the appropriate scope.			
	(iii)	In accordance with the certificate policy.			

Statements from CSR				Guidelines	
	6.6.3	PKI certificate Key pairs shall only ever be transferred and installed to a different operational site:			The GSMA seeks to maintain oversight of where PKI certificates (EUM, SM-DP, SM-SR, SM-DP+ and SM-DS) are in use through a registration process, managed under the control of the RSP/eSIM Compliance team. All requests and notifications should be communicated via: rspcompliance@gsma.com The availability of PKI certificate private Keys at each site is within the scope of the SAS certification and may be subject to validation during the Audit process. Evidence of failure to comply with the requirements for notification may be grounds for an NC assessment. Transfer of certificates and Key components should be controlled according to their sensitivity. PKI Certificate private Keys are highly sensitive assets and should always be treated accordingly. Auditees will be expected to demonstrate clear compliance with the requirements of 6.6.3 where transfer of Key components occurs.
	(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:			Transfer of private Keys should only take place under strict control, with all transfers originating from the nominated site with overall responsibility for control of the Key pair. Specifically, Auditees should consider how they can demonstrate that: •Private Keys are always be protected during the transfer process using a wrapping Key that is generated, exchanged and controlled using hardware, systems and processes equivalent to the private Key itself. •Private Keys are never available in unwrapped / plaintext form during the import, export or transfer process. •Controls in place to ensure that: ○ The wrapped Key can only be imported only to nominated Key management systems at the destination site; ○ The wrapped Key cannot be re-keyed to change the wrapping Key used; ○ Once imported into the Key management system, the private Key cannot be re-exported under the control of the destination site.
	(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.			

Statements from CSR				Guidelines	
					Technical controls to enforce these principles should always be considered as the preferred approach. Procedural controls involving multi-party control may be an acceptable alternative where technical implementation is not feasible or effective. However, involvement of multiple parties should always be enforced, logged and auditable. In the event that private Keys are found to have been transferred between sites without sufficient security they may be considered to be compromised, necessitating revocation and replacement of the certificate.
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:			Although it is permitted for Auditees to install EUM private Keys at multiple sites, each Auditee remains responsible for demonstrating that it maintains complete traceability of all EIDs to the originating site: •Where sites apply a strict policy of assigning individual EUM private Keys for exclusive use of a single site then it is generally acceptable that the certificate provides the necessary level of traceability. Auditees should be able to demonstrate that: ○ Internal records are maintained of the period of use for each EUM PKI certificate at each site. ○ Appropriate controls are in place to preserve the integrity and availability of these records for the period of validity of the PKI certificate. •For any EUM private Key that is used across multiple sites, Auditees should be able to demonstrate that: ○ A mechanism is in place that records the originating site for each EID. ○ Appropriate controls are in place to preserve the integrity and availability of the mechanism and the associated records for at least the period of validity of the PKI certificate. ○ The mechanism is configured, operated and maintained: ▪ Consistent with the relevant sections of the SAS Consolidated Security Requirements. ▪ At a site that is subject to SAS-UP Audit.
	(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.			

Statements from CSR				Guidelines	
					In most cases, Auditees are encouraged to consider the real business need for simultaneous use of EUM private Keys at multiple sites. Maintenance of unique certificates for each site is generally considered to be the preferred solution. SGP.22 v3.0 permits entities holding an appropriate EUM CA certificate to issue their own EUM SubCA certificates, e.g. for different products. Internal issue of individual EUM SubCA certificates for different sites is generally considered a preferable solution to sharing of the same EUM CA certificate across multiple sites.
SM DC	6.7	HSM as a managed service			An HSM as a managed service may be managed and hosted in a SAS certified Support Site, including a Site managed by a subcontractor to the Auditee. The subcontractor may be a cloud service provider (CSP) or other entity. Certificate management activities under the scope of SAS-SM are allowed.
	6.7.1	The Auditee shall only use a HSM that is managed by an SAS certified data centre or cloud region. In addition to the requirements of 2.4.2, the specific responsibilities assignment shall be documented and agreed between the Auditee and the subcontractor managing the HSM.			See 6.7.2 for responsibility assignment guidelines.
	6.7.2	Design, implementation and controls shall ensure that cryptographic Keys and certificates are only accessible to the SM service provider.			The responsibility assignment matrix and its implementation should demonstrate that only the approved key management personnel of the SM service provider can access cryptographic Keys and certificates. In particular, it is expected that the role of the subcontractor managing the HSM is limited to the physical installation, management of a physical HSM dedicated to the SM service provider, the management of IT infrastructure and decommissioning whereas the SM service provider approved personnel are responsible for operations related to providing HSM functional modules, HSM profiles, Local Master Key (LMK) and Key ceremony. Below is an example of expected responsibilities and assignments when the HSM managed service is offered by a CSP:

Statements from CSR			Guidelines				
				Operation	**CSP**	**SM service provider**	**Comment**
				Physical installation and management	X		
				Firmware		X	The SM service provider is responsible for the loaded firmware and, ensuring it is a genuine HSM vendor firmware, it has not been tampered with and it complies with the service provider's security and control policies.
				HSM Profile		X	HSM Profiles are under the sole control of the SM service provider: Key administrator(s), Key custodians and applications account.
				LMK		X	Local Master Key provisioning and management is under the sole control of the SM service provider.
				Key Ceremony		X	
				Managing IT Infrastructure	X		
				Upgrade Management		X	
				Decommissioning	X	X	The SM service provider "zeroes" the HSM upon releasing it to the CSP. In order to handle abnormal conditions that could prevent the SM service provider from zeroing the HSM, the CSP zeroes the HSM prior to

Statements from CSR				Guidelines	
					integrating it back into its pool of HSMs and has a process to securely destroy the HSM at the end of its service life even if the HSM is not functional anymore. In case where a HSM managed as a service stores the SM service provider cryptographic Keys and certificates outside the HSM, they should be wrapped with a storage Key under the sole control of the SM service provider and secured within the managed HSM.
	6.7.3	Remote Key management activities shall be possible only upon demonstrating a trusted path.			Remote Key management is the process of performing Key management activities from a location different from the HSM location. In all cases, the Auditee will be required to demonstrate a trusted path that provides an appropriate level of security, even if direct physical access to the managed HSM by the SM service provider is not possible (as is often the case with CSP services and hosting).
	(i)	Remote Key management activities shall be performed from a certified Environment in accordance with the requirements of section 6.4.1 and 10.4.			
	(ii)	Remote Key management activities shall be performed through a point-to-point secure channel from the SM service provider's Key management system to the HSM. The channel shall provide confidentiality, integrity, authenticity, replay protection and forward secrecy.			The secure channel should connect the SM service provider's Key management system directly to the target HSM system. It should be based on a well-established and proven cryptographic system.
	(iii)	The SM service provider shall have controls in place restricting management remote access to trusted sources and authorised personnel only.			A remotely managed HSM typically exposes a management interface on the network; see 6.2.2 for applicable dual-control requirements and 6.4.1 and 10.4 for applicable requirements.

Statements from CSR				Guidelines	
	6.7.4	An HSM supporting partitions must have all its partitions allocated to a single SM service provider.			

Requirement Statements			Guidelines	
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.		A document should identify the relevant data transfer and its associated protection. Appropriate electronic data transfer mechanisms should be agreed with customers including encryption of Sensitive Process Data. Suppliers should demonstrate that they have worked to ensure data transfer mechanisms are appropriate to the sensitivity of the data concerned. Where customers demand insecure data transfer mechanisms, suppliers should formally notify (in writing) the customer of the unsuitability of the data transfer mechanism.
			SM	Encryption of Sensitive Process Data should be compliant with SGP.02 [6], SGP.22 [8], or SGP.32 [15] when applicable or agreed with external third parties when not applicable.
	7.2	Sensitive Process Data access, storage and retention		
	7.2.1	Sites shall prevent direct access to Sensitive Process Data where it is stored and processed.		

Requirement Statements			Guidelines	
	(i)	User access to Sensitive Process Data shall be possible only where absolutely necessary. All access must be auditable to identify the date, time, activity and person responsible.		Sensitive Process Data should normally be encrypted at all stages of storage, processing and transmission, except where decrypted data is specifically required to complete the processing stage (e.g. Personalisation). Appropriate data encryption technologies should be used to protect Sensitive Process Data. Keys should be managed securely. Please refer to the "General Consideration on Algorithm and Key Length" section in SGP.02 [6] to protect sensitive production data. Sensitive Process Data should be deleted after use. Decrypted data should always be deleted using a secure wipe mechanism. Suppliers should be aware of the potential vulnerabilities arising from temporary files and memory paging when evaluating the risks around Sensitive Process Data processing. Appropriate controls should be in place to minimise such risks. Data generation and processing mechanisms that require manual intervention / processing of un-encrypted data files should be avoided wherever possible. Automated systems that encrypt data on-the-fly during processing are always preferred. Where manual access to Sensitive Process Data is possible or required it must always be auditable. Control of the audit trail must be independent of personnel with access to data.
	(ii)	System and database administrators may have privileged access to Sensitive Process 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:		Guidelines in section 7.3 apply to those Sites requiring Generation of Data for UICC Personalisation to be within the scope of the SAS-UP certificate. "Local Site" refers to the Site participating in the SAS-UP scheme and being audited by the SAS-UP Auditors.
	(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.		Random numbers generated as part of data processing for GSM production should be produced by a source whose quality has been: •Certified to a recognised international standard. Evidence of certification should be available during the Audit.

Requirement Statements			Guidelines	
				Or •Subjected to a series of recognised tests of randomness with results that indicate that an acceptable level of randomness has been achieved. Evidence of the testing process and evaluation of results should be available during the Audit. Mechanisms should be in place to ensure that randomness is maintained (periodic re-testing, or re-seeding of PRNG may be appropriate). Evidence should always be available at the Local Site, even where the random source is part of a 'black box' Personalisation solution (i.e., there is no detailed understanding of its inner workings by local personnel).
	(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.		An auditable mechanism should be in place to ensure that the correct random source is used for generation of data. Appropriate mechanisms may include independent, auditable validation at time of development of data generation applications or configuration profiles. Where applications or configurations are developed by an off-site team the Local Site should still take responsibility to ensure that: •Validation has been carried out Validation may be carried out: ○ on-site by the local team as part of the process to receive the new application/configuration and install it into the production Environment or ○ off-site as part of the development process, provided that the evidence of independent, auditable validation is available to the Local Site for review as part of the process to receive the new application/configuration and install it into the production Environment •Evidence exists of the validation being carried out. Where data generation applications or configuration profiles are used, integrity controls should be considered to ensure that: •The correct application / profile is used for data generation / processing •The application / profile cannot be changed from that approved / validated.

Requirement Statements			Guidelines	
				Controls may include: ○ Restricted logical access to locations that applications / profiles are stored ○ Encryption / encoding of applications or profiles to limit the ability of operational personnel to modify the applications / profiles ○ Checksum / hashing mechanisms that seek to validate integrity at run-time.
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:		A complete, automated audit trail should be in place for all data processing and manipulation activities. The audit trail should record: •The identity of the user carrying out the action / processing stage •The date and time of the action •The nature of the action •The success / failure of the action (including attempts to exceed privileges). Where data processing activities are normally handled by a set of dedicated applications, parallel audit trails should exist for any attempted / successful manipulation of data outside of these applications (e.g. using operating system or generic database tools) The integrity of the audit trail should be preserved. The audit trail should be subject to regular review to identify irregular or unauthorised activity. Role separation should ensure that the audit trail cannot be modified / deleted by members of the data processing team. Based on the asset lists, a log should exist for the entire lifecycle of the asset. A log should exist for the entire user access lifecycle.
	(i)	all assets created, processed and deleted are completely accounted for		
	(ii)	access to Sensitive Process Data is auditable		
	(iii)	responsible individuals are traceable and can be held accountable		

Requirement Statements			Guidelines	
	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 Process Data.		Audit trails should not be modified via technical or procedural processes. Retention period guidelines shall be defined. The retention period is expected to be in accordance with the customer SLA (maximum or minimum).
	7.4.3	Auditable dual-control and 4-eyes principle shall be applied to sensitive steps of data processing.		Sensitive Process Data processing steps will include any action that introduces a risk of unauthorised or Duplicate production, and may include: •Manual generation or manipulation of production data •Changes to the status of production data (e.g. resetting UICCs already produced).
UP	7.4.4	For UICC production the audit trail shall include:		Management of the UICC audit trails should be consistent with the controls in sections 7.4.1-3.
	(i)	Generation of Data for Personalisation and processing of that data		
	(ii)	Personalisation		
	(iii)	Re-personalisation		
	(iv)	access to Sensitive Process Data		
	(v)	Production of customer output files		
	7.5	Duplicate production		
	7.5.1	Controls shall be in place to prevent Duplicate production.		Prevention of Duplicate production is a fundamental principle of SAS. Systems for data processing and production must be designed to prevent opportunities for Duplicate production from occurring except where: •These have been explicitly requested and authorised by the customer MNO •The creation of the Duplicate does not violate the relevant technical standards or undermine the integrity of the ecosystem.

Requirement Statements			Guidelines	
				Where production systems are reliant on file-based mechanisms, multiple levels of control should be in place to restrict access to data files. Experience shows that single levels of control (e.g. third-party software limiting access to operating-system tools) are vulnerable; weaknesses can often be introduced. Where production systems are reliant on centralised or database-driven mechanisms, access to manipulate the database / system status should be strictly controlled and fully auditable. Where mechanisms exist for exchange of data between different production Sites additional controls should be in place to ensure that Duplicate production across Sites is prevented.
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.		Control of authentication should be done between actors as per the functional specifications (for example, the certificate chain in the reference document SGP.02 [6]) when applicable. When not applicable, there should be a specific authentication mechanism with the third party (for example, specific communication link or specific data transfer process) equivalent to the above document.
	7.7	Internal audit and control		
	7.7.1	Sensitive Process Data controls shall be subject to a rigorous programme of internal monitoring, audit and maintenance to ensure their continued correct operation.		A programme of internal audits/controls should be defined that demonstrates appropriate consideration of: •The frequency of checks required for each area addressed by the internal audit/control mechanism •The structure of the audits/controls themselves, including clear guidance on what should be checked and how •The recording / documentation and follow-up process for audits/controls undertaken.

Requirement Statements		

Guidelines	
	The Auditors will expect to see evidence that processes and systems are working correctly, and that internal audits/controls have been carried out according to the schedule. There should be appropriate coverage of all aspects of the system; the audit/control programme should be defined around the need to provide appropriate coverage, rather than the availability of audit resource. Auditors should have received appropriate training in the structure and content of internal audits/controls.

Requirement Statements				Guidelines
8 SM-DP, SM-SR, SM-DP+, SM-DS and eIM Service Management				
SM	8.1	SM-DP, SM-SR, SM-DP+,SM-DS, and eIM 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 [5] /SGP.02 [6], SGP.21 [7] /SGP.22 [8] , and/or SGP.31 [14] /SGP.32 [15] as applicable.		The objective is not to demonstrate that the system is compliant with the functional specifications but to show the existence of the different secure interfaces The Auditee will be expected to follow Annex D of the FS.09 Methodology document and ensure that the solution can be fully demonstrated for each of the following: •SM-SR and SM-DP ○ Unpersonalised Profile creation ○ Profile ordering and personalisation ○ Processing of eUICC registration ○ Download of a Profile with personalised data ○ Installation of a Profile ○ Enabling of a Profile ○ Disabling of a Profile ○ Deletion of a Profile •SM-DP+ ○ Unpersonalised Profile creation ○ Profile ordering and personalisation ○ Download of a Profile with personalised data ○ Installation of a Profile ○ Enabling of a Profile ○ Disabling of a Profile ○ Deletion of a Profile

				○ SM-DS ○ Certificate enrolment and verification ○ Event registration and retrieval. •eIM ○ Enabling of a Profile ○ Disabling of a Profile ○ Deletion of a Profile ○ Download of a Profile in case of Indirect Profile Download [15] (optional) ○ Add a new eIM to the eUICC (optional) ○ Update an Associated eIM (optional) ○ Delete an Associated eIM from the eUICC (optional) ○ Event retrieval from SM-DS (optional). In order to support the demonstration, audit trails should be available. These should include but are not limited to application log files and firewall log files.
	8.1.2	Exchange of data within the SM-DP, SM-SR, SM-DP+, SM-DS, or the eIM IT systems shall be secured to the level required by its asset classification.		Refer to SGP.02 [6], SGP.22 [8] , or SGP.32 [15] to identify Sensitive Process Data exchanges.
	8.1.3	The SM-DP, SM-SR, SM-DP+, SM-DS, and eIM must prevent cross-contamination of assets between different customers.		Prevention should be ensured by use of Key segregation (SM-SR, SM-DP, SM-DP+), access rights allocation (SM-DS).
	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.		Logically segregated means the same hardware, the same instance but different access rights.
	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.		Control of authentication should be done between actors as per the functional specifications (for example, the certificate chain in the reference document SGP.02 [6], SGP.22 [8], or SGP.32 [15]) when applicable. When not applicable, there must be an equivalent specific authentication mechanism with the third party (for example, specific communication link or specific data transfer process)
	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.		The minimum information related to the application (Profile Management, Platform Management, and eUICC Management) which should be logged are: •Initiator of the request (if applicable), •ID of the request (if applicable), •Type of the request (if applicable), •Timestamp of the request (if applicable), •Timestamp for the completion (if applicable), •Profile identifier (if applicable), •eUICC ID (if applicable), •MNO_ID (if applicable), •SM-SR ID (if applicable), •SM-DP ID (if applicable), •SM-DP+ ID (if applicable), •eIM ID (if applicable). The minimum information related to the IT system which should be logged are: •Users' logins (successful/unsuccessful) •Resource access •Activity description.

	(ii)	Access to Sensitive Process Data		The minimum information related to the access to Sensitive Process Data which should be logged are: •Users' logins (successful/unsuccessful) •Reason for accessing Sensitive Process Data •List of Sensitive Process Data accessed •Timestamp of the log in and log out
	8.3.2	The audit trail shall be managed in accordance with the requirements of 7.4.		

Requirement Statements			Guidelines	
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.		Low sensitivity assets for GSM production should be subject to basic stock controls and reconciliation. Complete accountability for individual assets is not expected.
	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:		Asset control mechanisms should be applied to Class 2 assets. Where Class 2 assets are stored and/or processed in separate Environments to Class 1 assets (with physical separation and independent access control – e.g. separate workshops) different control mechanisms may be applied. Where assets of different classes are processed in unified physical Environments appropriate controls should be applied to ensure that the expected level of control for the highest level of assets is maintained and that the risks of uncontrolled assets and cross-contamination are managed appropriately.

				Auditees are encouraged to seek specific guidance on the acceptability of controls for unified Environments in advance of their first Audit via the GSMA and/or Audit Team.
	(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		The audit trail should record quantities of Class 1 and Class 2 assets by type (e.g. card bodies, modules) and status (e.g. good, surplus, rejected) at each processing stage. It is accepted that the quantity of modules is difficult to control. Suppliers should, however, track quantities of modules used / remaining for each module reel. It is acceptable to use the manufacturer's reported quantity of 'good' modules on each reel as a starting point for the module tracking process. Modules that cannot be used, or are wasted, in setting up equipment should be classed and treated as Rejects and recorded in the audit trail. Card bodies can be controlled effectively. Quantities of card bodies entering embedding should be subject to 100% control. Quantities of card bodies throughout processing of Class 1 and Class 2 assets should be subject to 100% control.
	(ii)	ensures that the responsible individuals are traceable and can be held accountable		Accountability for Class 1 and Class 2 assets should always be in place. Responsibility for assets should be documented within the audit trail.

				Assets should be subject to a formal, auditable, handover where responsibility changes. Quantities of assets should be subject to 100% control as part of the handover process.
	(iii)	demands escalation where discrepancies or other security incidents are identified.		An escalation process / mechanism should be in place where discrepancies are identified. It is expected that all such discrepancies are tracked and reported. Where discrepancies cannot be resolved, a risk assessment should be carried out and appropriate action taken. A register of unresolved incidents/discrepancies should be maintained.
	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.		The audit trail described in section 9.3.1 should be independently reviewed at the end of production to carry out a reconciliation of all assets. Interim reconciliations within the production process are strongly recommended to aid identification and resolution or discrepancies. Any discrepancies should be documented and escalated. Where Class 1 assets are temporarily held within production areas between production stages, they should be appropriately stored to preserve their integrity. Locked cages, trolleys, or storage cupboards are sufficient, provided that Physical Keys are controlled. Responsibility and accountability for assets should be identified. Appropriate re-counting of assets should take place prior to sensitive production stages (e.g. Personalisation). Asset control mechanisms should ensure that all elements of each asset are accounted for. Where assets incorporate removable or re-pluggable elements (e.g. plug-ins) these should be verified as part of the asset at each stage. Missing elements should be identified and treated as incidents.
	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		Quantities of assets entering Personalisation should be counted under dual control (either two separate 100% counts by two different individuals, or a single count under 4-eyes principle).
	(ii)	authorization of Re-personalisation for rejected UICCs		Authorisation of Re-personalisation should take place under auditable 4-eyes principle. Prior to Re-personalisation, Rejects should be electrically disabled

				and physically marked to indicate their rejected status. Disablement should take place under 4-eyes principle.
	(iii)	control of the quantity of assets packaged for dispatch to customers		During production assets should be controlled 100% on a one-by-one basis. At the point of initial packaging, control will normally change from one-by-one to box-by-box control. At the point of packaging: Assets should be subject to a final count / control. For cards, the count may be undertaken using a card counter. For cards packaged with card carriers, or other fulfilment mechanisms, the count may be undertaken by machine counter, weight check or another counting device. Auditees will be expected to show that the counting mechanism used is accurate. The counted assets should be packed and sealed using a tamper-evident seal immediately following the final count / control. The final count / control should be under clear CCTV coverage Assets must be under clear, continuous CCTV coverage from the point of counting to the point the box being sealed. Appropriate CCTV coverage is best achieved using an overhead camera covering the counting / packing workstation. Where possible, Auditees should increase the integrity of the control process by implementing automated audit trails of the assets counted. Counting and sealing of boxes under 4-eyes principle is also accepted. Good CCTV coverage is still required to provide auditability of the application of 4-eyes principle. Where fulfilment results in the UICC being wholly contained within other packaging (e.g. an envelope or box), mechanisms should be in place to validate that each package contains a UICC prior to the final count / control taking place.
	(iv)	destruction of rejected assets		Destruction of rejected assets should take place under 4-eyes principle.
	9.3.4	Application of 4-eyes principle shall be auditable through production records and CCTV.		Time and date of each control, and identities of Employees responsible, should be documented within the audit trail. Recording of time and date will enable CCTV records to be identified and checked.

	9.3.5	Regular audits shall be undertaken to ensure the integrity of production controls and the audit trail.		Audit trails within production must be subject to regular internal control to ensure that processes are being followed. Discrepancies should be investigated and appropriate follow-up actions taken.
	9.3.6	Suppliers must demonstrate an ability to prevent unauthorised duplication within the production process during Personalisation and Re-personalisation.		Appropriate controls must be in place around the availability of Personalisation Data, as described in section 7.2. Availability of embedded card bodies should be under appropriate control at point of issue. Reconciliation of production should ensure that all assets are accounted for. Authorisation of Re-personalisation should require rejected UICCs to be disabled under 4-eyes principle (as described in section 9.3.3) prior to Re-personalisation taking place.
	9.3.7	Suppliers must demonstrate an ability to preserve the integrity of batches within the production Environment to prevent:		Within the production Environment it is normal for different batches to be processed at the same time. This may include batches in 'live' production and batches being held between processing stages. The 'production Environment' to which these controls apply will always include the physical Environment in which Personalisation takes place. Other activities included within the same physical Environment should be subject to appropriate controls to prevent the asset control and reconciliation mechanism being undermined by uncontrolled assets and/or cross contamination of products and/or batches. These activities may include Personalisation of other products (e.g. payment cards) or less Sensitive Processes (e.g. card body manufacturing, embedding). Activities taking place in other physical Environments (e.g. physically separate workshops under separate access control with different operational personnel) could be carried out with different asset controls appropriate to their sensitivity.
	(i)	cross-contamination of assets between batches		Auditees should demonstrate that appropriate controls are in place to prevent accidental or deliberate cross-contamination of assets from different batches. Typically controls would include use of one or more of the following: •Locked trolleys or cabinets for temporary storage of materials in process or between processing stages •Sealing of individual boxes of assets.

				Such controls help to restrict unauthorised access and preserve the integrity of counts and may also provide evidence of any unauthorised access / tampering.
	(ii)	uncontrolled assets in the production Environment undermining the integrity of the asset control mechanism.		Asset control mechanisms often rely on counting systems / technologies that do not individually identify each asset. For example, card counters typically count a quantity of cards by identifying the edge of each card in a stack. Any uncontrolled assets within the production Environment could, intentionally or accidentally, undermine the integrity of counts and controls if they are mixed with assets in the production process. To help manage this risk all assets entering the production Environment should be controlled. Quantities should be checked before new assets are transferred into the production Environment.
	9.4	Destruction		
	9.4.1	Rejected sensitive assets must always be destroyed according to a secure procedure and logs retained.		Destruction should take place regularly to avoid large stocks of rejected assets being accumulated (e.g. daily or weekly), and to simplify reconciliation. Destruction of Class 1 and Class 2 assets should take place locally, on-site under most circumstances. Rejected card / module assets should always be destroyed on-site. Assets for destruction should be reconciled against records of assets rejected immediately prior to destruction taking place. Reconciliation should take place under 4-eyes principle (4EP). Reconciliation may be based on: •Counting of individual assets immediately prior to destruction •Packs of assets counted at the point of rejection under 4EP and sealed using a tamper evident mechanism. The integrity of the tamper evident seal must be checked immediately prior to destruction, and the number and identity of sealed packs verified. The destruction process for Class 1 and Class 2 assets should always be controlled under 4EP. Control may be achieved by: Either: •Both parties responsible for destruction witnessing all of the assets entering the body of the destruction device to a point from which they cannot normally be retrieved intact

				Or: •Both parties witnessing the entry of all of the assets into a feeder for the destruction device, access to which is completely and solely under the control of the two parties taking responsibility for the destruction. The feeder may be locked and sealed and left unsupervised during the destruction process provided that: ○ The feeder can only be re-opened by the two designated parties. ○ The feeder can only be re-opened in the presence of both designated parties simultaneously. ○ A means is in place for the two designated parties to confirm that the locking mechanism has not been opened •Locking of the feeder may be achieved by restricting access to the device itself, or to a self-contained area where the feeder device is located. In either case: •The complete destruction process should be auditable using the CCTV system. There should be complete continuity of coverage between reconciliation and destruction; this is best achieved by performing reconciliation within the destruction area. •Processes should be in place to ensure that all materials entering the shredding/destruction process have been destroyed. Destruction equipment should be inspected under 4EP at the end of each destruction to ensure that all materials have been destroyed. For 4EP to be effective, the two Employees performing reconciliation and destruction should be from separate business areas. Wherever possible, the combination of Employees carrying out destruction should be varied. The date, start time, end time and identities of the 2 Employees carrying out reconciliation and destruction should always be recorded against an inventory of those items destroyed. Output from the shredding / destruction process should ensure that the active area of the device is reduced to half its original size in at least one dimension. For 2FF and 3FF plug-ins this is typically 3-4mm. For 4FF micro-SIMs this is

				typically 2-3mm. Measurements for embedded devices will be significantly smaller and require specialist destruction equipment. Output from the shredding / destruction process should be periodically checked to ensure that the mechanism in use is effective.
	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.		Following final control and sealing of finished boxes, goods should be packaged ready for despatch. It is sufficient for packaged goods to be held in secure production or despatch areas prior to despatch, provided that they are: •Visible on CCTV •Dispatched within 48hrs. If goods are to be dispatched more than 48hrs after packaging, they should be stored in a physically separate area under separate access control. CCTV coverage should be provided.
	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.		Appropriate packaging should provide protection against damage or unauthorised tampering. All transfers of finished or part-finished product, including intra- and inter- site transfers, should be included.
	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 shall be positively identified. Goods shall only be handed over following the production of the appropriate authority documents. A receipt shall 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.		A programme of internal audits/controls should be defined that demonstrates appropriate consideration of: •The frequency of checks required for each area addressed by the internal audit/control mechanism •The structure of the audits/controls themselves, including clear guidance on what should be checked and how •The recording / documentation and follow-up process for audits/controls undertaken. The Auditors will expect to see evidence that processes and systems are working correctly, and that internal audits/controls have been carried out according to the schedule. There should be appropriate coverage of all aspects of the system; the audit/control programme should be defined around the need to provide appropriate coverage, rather than the availability of resource. In particular, there should be evidence that the internal audit/control system has been designed to validate correct operation of the security controls in each part of the production process. Appropriate coverage should be provided of different shifts, products and fulfilment activities. Auditors should have received appropriate training in the structure and content of internal audits/controls.

Requirement Statements			Guidelines	
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.			Requirements should be applied to all networks that support functions relevant to the scope of certification. IP networks and their associated systems used for physical security (e.g. CCTV, access control, alarm systems) should be treated as IT networks and be subject to appropriate IT security controls.
	10.1	Policy		
	10.1.1	A documented IT security policy shall exist which shall be well understood by Employees.		An IT security policy should be defined and available to all Employees as part of the Site security documentation.
	10.2	Segregation of roles and responsibilities		
	10.2.1	Roles and responsibilities for administration of computer systems shall 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).		Roles and responsibilities for administration of computer systems should be clearly defined. Users whose function it is to handle and process production data should not have the capability to administer the production systems. Where exceptions are necessary to the segregation of security-related and operational duties, additional controls should be in place.

Requirement Statements			Guidelines	
	10.3	Access control		
	10.3.1	Physical access to sensitive computer facilities shall be controlled.		Servers and sensitive computer facilities (e.g. data processing) should be located in Restricted Areas within one or more HSAs. Access to such rooms should be restricted on a need-to-be-there basis. Access should be auditable. Sensitive computer facilities should be protected by the Site alarm system when not in use.
	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.		A process should be in place for requests for access to computer systems. The process should be auditable and include an authorisation mechanism. The process should cover creation, modification and deletion of access rights. The authorisation process should apply to all access, including the creation of administrator and 'machine' accounts. Access should not be provided without the appropriate authorisation process having been completed. Details of authorised users and user accounts should be maintained in a consolidated list, independent of the systems themselves, as a reference. Processes should be in place to reconcile the reference list against the systems periodically.
	10.3.3	Passwords shall be used and managed effectively.		A clear password policy should be defined and enforced for all users of all systems and applications. The password policy should normally include: •Length •Complexity •Regular change •Control of re-use of earlier passwords. Where systems are not capable of enforcing the policy, additional procedural controls should be used to ensure the policy is applied. Where split passwords are used to attempt to enforce dual control:

Requirement Statements			Guidelines	
				•The scope of the dual control should be clearly defined to determine whether this is only applicable to the logon itself, or for the entire session resulting from the logon. •Additional mechanisms should be in place to make sure that dual control is effective, including: ○ Application of password policy over each component of the password ○ Independent audit of account activity to ensure that logon has taken place under dual control; for example, by use of CCTV to confirm that logons (and, where appropriate, the resulting sessions) recorded in the system audit trail were carried out with the correct individuals present.
	10.4	Remote Access Remote access for a user to connect to a network, system or service within a HSA from another 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 the Auditee's **corporate network**, using a secure **channel** to the **target** Environment.		Remote access requirements described in 10.4 are not intended to address system-to-system connections involving networks, systems or services at different certified Sites. Such connections will be assessed against the requirements of section 10.5. Remote access to target networks where Sensitive Data is transmitted, stored or processed can introduce significant risks. Any remote access must be carefully considered to ensure that these risks are avoided altogether or managed appropriately. The requirements and guidelines in section 10.4 are intended to provide Auditees with a model of how such access should be implemented to comply with the requirements of SAS for: •Appropriate security of the endpoint from which remote access originates •Security of the channel from the endpoint, via the Auditee's corporate network, to the target Environment •Security of the termination of the channel to a Jump Host in order to connect to assets within the target Environment. These requirements are not intended to consider the secure exchange of data, as is required for both SAS-UP and SAS-SM Environments: •For SAS-SM and SAS-UP, customer access to data transfer platforms (e.g. secure file transfer servers) on dedicated networks (e.g. customer data

Requirement Statements			Guidelines	
				transfer DMZ) is typically required solely for the exchange of input, response (including Profile) and production data. •Such access normally involves remote interaction with an exposed service that offers limited capability. Controls within the secure network Environment should assure the integrity, authenticity and confidentiality of the data transferred.
	10.4.1	Where remote access is implemented, it shall: • Be governed by a defined remote access policy and procedure. • 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. • Ensure that risks to sensitive information and systems are no greater than where the activities are conducted locally on-site from within the certified secure area(s).		Remote access may be permissible under highly controlled circumstances where the risk of such access has been fully evaluated. The risk methodology must take into account the classification of the data on the systems being remotely accessed and whether the remote access is: •Read-only, providing access only to view information about the status of systems at the certified Site with no access to modify information, configuration or system operation, or to view Sensitive Data •Connecting to a pre-defined service, designed to allow remote triggering of an activity or function with little or no ability to affect the operation of that activity •Full/limited interactive or administrative access, enabling the user to modify system configuration or operation, access or manipulate data being stored or processed, or affect the processing of data in a way equivalent to a user on-site using a command line or graphical environment. Access and controls should be implemented in accordance with 10.4.3-10.4.6. Evaluation of the risk assessment by the Audit Team will consider: • The information and assets identified by the Auditee's risk assessment. • The level(s) of access being provided to those assets. • How access to the assets is controlled and restricted to designated personnel and originating endpoints. The technical controls implemented to ensure the security of the endpoint, channel (via the Auditee's Corporate Network) and target system(s).

Requirement Statements			Guidelines	
				Where third party-remote access is required for support and involves remote access to Environments containing networks, systems or data within the scope of SAS certification it is expected that this would be declared prior to the Audit. The remote access mechanism will typically combine a secure channel (via the Auditee's corporate network) with appropriate user authentication and logging, Once the channel is established, the remote user will connect to systems at the target Site via Jump Host(s) to perform operational activities (as described in 10.4.6(vii). These activities should always enforce an appropriate level of security that ensures the risks to sensitive information and systems are at a level equivalent to, or lower than, the same activities carried out on-site. Where an equivalent security level cannot be assured through the remote channel then activities should not be carried out remotely.

Requirement Statements				Guidelines
	(i)	The requirements for remote access shall be applied based on the following summary		

Applicable controls	Type of remote access to target system / Environment: Read-only (10.4.2)	Pre-defined services (10.4.3)	Limited interactive (10.4.4)	Full interactive (10.4.5)
Physical control of endpoint location				
HSA in a certified Site	✓	✓	✓	✓
Pre-defined location (e.g. Auditee office (certified Site but outside HSA, or at uncertified site), uncertified subcontractor site, home office), or appropriately secure hotel room.	✓	✓	✓	✘
External, uncontrolled location (e.g. off-site roaming user)	✘	✘	✘	✘
Logical Security Controls				
Remote Access Policy	See 10.4.6 (i)			
Location(s)	See 10.4.6 (ii)			
User(s)	See 10.4.6 (iii)			
Endpoint Security	See 10.4.6 (iv)			
Authentication	See 10.4.6 (v)			
Security of Channel	See 10.4.6 (vi)			
Security of the target network	See 10.4.6 (vii)			
Audit trails and logs	See 10.4.6 (vii)			

Requirement Statements			Guidelines	
	10.4.2	Where remote access for operational **read-only** monitoring of systems is granted: • Access to view Sensitive Data and Class 1 assets shall not be possible. • Connections shall always be made in accordance with the requirements set out in 10.4.6.		Examples of such remote operational access include: •Monitoring - access to network or system performance, status or event data published by a system. •Log reviews. Examples of Sensitive Data include: •Class 1 data related to the SAS-certified activities •Information about system or security configuration that could be of use to a potential attacker e.g. firewall rules. Class 2 information and assets may be visible under read-only access, although Auditees will be required to demonstrate that this visibility does not place any Sensitive Data at risk, particularly where this read-only access takes place from outside of a secure area at a certified Site. Read-only access (inherently) should not permit any deletion or modification of any information or assets. Where it is necessary or possible for modification or deletion to be carried out, remote access will be considered as a higher level of access (e.g. 10.4.4 or 10.4.5). Technical controls in place at the primary certified Site to restrict the level of access for remote users should be demonstrated at the Audit. The Auditors will expect to see evidence that these controls are implemented at and managed from a certified Site..
	10.4.3	Where remote access for connection to **pre-defined services** is granted: • Access to view Sensitive Data or perform Key management shall not be possible. • Connections shall always be made in accordance with the requirements set out in 10.4.6.		Examples of such remote operational access include: •Pre-defined service access – Initiating a service or process either: • With some limited variability or user input but where the scope of activity is limited and clearly controlled e.g., a file transfer mechanism • As a fixed process with no variability e.g., triggering of a data processing operation. In all cases, the access should only permit access to execute the pre-defined actions. Access that permits a flexible interaction with systems, information or assets, remote access will be considered as a higher level of access (e.g. 10.4.4 or 10.4.5).

Requirement Statements			Guidelines	
				Access to view Sensitive Data (e.g., key material, Class 1 assets) or access to configuration data (access control, system configuration) should not be possible. Pre-defined services may be initiated from outside of a high-security area where a full risk assessment has been conducted but should never include: • Key management activities. • Any activity that provides visibility of Class 1 data. • Class 2 information and assets may be visible under read-only access, although Auditees will be required to demonstrate that this visibility does not place any Sensitive Data at risk, particularly where this access takes place from outside of a secure location. • Any activity that modifies or affects the security controls that protect sensitive information or the systems and networks on which such information is stored or processed, including those relating to logging of activities. Technical controls in place at the Site to restrict the level of access for remote users should be demonstrated at the Audit. The Auditors will expect to see evidence that these controls are implemented at, and managed from, a certified Site. Control of the pre-defined services exposed to remote users should be demonstrated at the Audit. The Auditors will expect to see evidence that services are designed, implemented and executed in a way that: • Limits the scope to clearly defined roles. • Restricts any visibility of sensitive information. Examples of sensitive information include: • Class 1 data related to the SAS-certified activities. • Information about system or security configuration that could be of use to a potential attacker e.g., firewall rules.

Requirement Statements			Guidelines	

	10.4.4	Where **limited interactive remote access** to systems and networks within SAS certified Sites is granted for administration or operational reasons:
		• Access to view Sensitive Data or perform key management shall not be possible.
		• Connections shall always be made in accordance with the requirements set out in 10.4.6.
		• Access may be permitted to take place remotely from specified locations outside of the certified Site subject to specific criteria being satisfied and controls being appropriate.
		• Remote access shall only be permitted where:
		  • The type of system and reason for access are both specifically permitted within FS.18.
		and
		  • Auditees are able to demonstrate that access to these systems does not introduce a risk of disclosure or manipulation of sensitive information.
		In all other cases, 10.4.5 shall apply.
				To facilitate operations within SAS Environments, a limited level of interactive access is permitted to perform some specific administrative and operational activities on some specified systems, provided that:
				• This is always done in accordance with SAS requirements.
				• No sensitive information or assets are at risk of possible disclosure as a result of the remote access (e.g. by being visible or accessible at the location where the remote access originates).
				• Auditees are able to demonstrate that the limited interactive access is restricted only to the specified systems and activities and that a remote user cannot gain access to other systems, functions or assets, or cause others to be granted access to other systems, functions or assets.
				Assets and activities permitted are defined in Annex A.

Requirement Statements			Guidelines	
	10.4.5	Where **full interactive remote** 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.		Examples of sensitive systems for SAS include: • Personalisation systems • Key management systems • Network firewalls or switches • Back-end data transfer servers • Data generation servers This type of access is more common within SAS-SM, and is the primary method of connecting to the target Environment from a secure room(s), which is included in the Site's certification. Full administrative and operational activities are undertaken. Examples of other remote interactive access include: • An interactive shell or desktop session on a workstation, server or network component such as a firewall. This level of access carries the highest level of risk. By default, certified Sites that permit this level of inbound access are expected to demonstrate that these activities are carried out from within an Environment where the logical and physical security controls and associated processes comply with the requirements of SAS. In most cases this will require the Site hosting the endpoint(s) to be subject to an SAS Audit from the relevant scheme (UP or SM) as part of the certification process. Where remote management is provided through an administration portal or tool that permits administrative actions but no direct access to the system; the portal or tool itself may also fall within the scope of the Audit (e.g., portal/tool audit logs, evidence of patch management, penetration testing against portal/tool). If a system is presented as off-line / air-gapped for the purpose of the SAS certified activities, then no level of remote access would be expected.
	10.4.6	The governance and controls for remote access must be clearly defined and connectivity between the originating		

Requirement Statements			Guidelines	
		endpoint and the targeted system(s) must be appropriately secured, as follows:		
	(i)	Remote Access Policy The company's remote access implementation and usage must be clearly defined in a remote access policy and supporting procedures. Relevant Employees and third parties shall have access to the documentation and acknowledge their understanding of its content.		A documented remote access policy should exist, either as a stand-alone document or as part of the overall information security policy/manual. The policy should be supported by appropriate procedures that define the accepted method(s) for remote access to the target network(s) and should incorporate the requirements of section 10.4. A mechanism should exist for ensuring that important changes to the policy and procedures can be communicated effectively to relevant individuals and they must confirm acknowledgement and understanding of what is required by them (e.g. by completion of a signed undertaking by each individual user). • Employees should always be required to complete the declaration process as part of the initial granting of remote access. Access should not be granted where the acknowledgement has not been completed. • Where existing Employees are required to provide an updated declaration, mechanisms should be in place for escalation (and, ultimately, revocation of access) if this is not done within reasonable timescales.
	(ii)	Location(s) The location(s), where remote access can be performed, must be: • Documented; • Subject to risk assessment; • Appropriately secure; and • Approved.		Where full interactive remote access is required (section 10.4.5), it is expected that the location will be a secure room with appropriate access control to only permit individuals on a "need to be there" basis (see 10.3.1). The room is expected to have appropriate physical security controls in place (see section 5). Where read-only access (section 10.4.2), pre-defined service access (section 10.4.3) or limited interactive remote access is required (section 10.4.4), Auditees are expected to maintain a register of approved locations, including specific rooms to be used where feasible. These locations:

Requirement Statements			Guidelines	

				• Should be subject to risk assessments to ensure that no increased risk exists such as the endpoint screen being viewable by unauthorised personnel from within or outside of the location).
				• Should be pre-approved:
				  • On an individual basis for locations in regular use (e.g. Auditee or sub-contractor offices, Employee home offices).
				  • On the basis of documented principles for other locations that can be appropriately secured, but where individual pre-approval is not possible (e.g. hotel rooms).
				  • Specific hotel rooms are not expected to be documented, risk-assessed or approved individually, but this should be done generally by the Auditee as a location type. Authorised users performing remote access from hotel rooms should ensure that the specific room is appropriately secure, in accordance with guidelines or policies defined by the company.
				• Should not include public spaces such as cafes, hotel lobbies, or airports, or general office space (even at a certified Site) shared with other individuals that do not have to satisfy the user requirements in 10.4.6. (iii).
				• Should be the subject of documented policies or guidelines about controls that should be in place at the approved Environment before each remote access session is initiated, that may include ensuring that:
				  • No unauthorized personnel are present within the room.
				  • The door of the room is secured to prevent unauthorized personnel entering for the duration of the session.
				  • No screens displaying the remote session are visible to any other person.

Requirement Statements			Guidelines	
				In all cases the Employee performing the remote access should understand, accept and act upon their individual responsibility to ensure that requirements are met for each session. As described in 10.4.6(iii) this may include requiring the Employee to provide specific confirmation as part of the connection process. • The Audit Team will check compliance primarily through review of policies and guidelines and their enforcement, rather than technical controls.
	(iii)	User(s) Remote access must only be carried out by personnel that are: • Subject to HR controls as defined in section 4 of the requirements. ○ Sub-contractors are expected to comply with all applicable requirements (including section 4), as per section 2.4.2. • Specifically authorized to perform the remote access tasks • Have received relevant training • Are operating under a clear access agreement as part of which they accept their obligations to comply with defined policies.		Auditees should demonstrate that the requirements of section 4 are applied to all users that are authorised to use endpoint devices. Personnel should sign specific user access agreements that acknowledge and accept internal regulations relating to Employee responsibilities. Training and regulations should include specific reference to, and acknowledgement of, the need to ensure that no sensitive information is at risk from potential unauthorised disclosure or eavesdropping that may arise from: • Visibility of the endpoint screen (e.g. shoulder-surfing, photography or videoing of the endpoint screen, including visibility from CCTV installations). • Broadcast of any audio from the endpoint, or spoken or relayed by the user of the endpoint (e.g. telephone discussions about activities being carried out on the endpoint). • Information copied or transcribed from the endpoint electronically or on paper or other media (e.g. printed from the endpoint, written notes by the endpoint user). Consideration should be given to a requirement for Employees to positively confirm that remote access requirements for the physical location are met as part of each session (e.g. through an on-screen acknowledgement).
	(iv)	Endpoint security The security of the endpoint from which remote access originates shall enforce appropriate security controls to ensure a		The workstations utilised for remote access shall be pre-approved and subjected to a filtering mechanism (IP filtering, MAC address…) to limit potential connections.

Requirement Statements			Guidelines	
		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: Owned and controlled by the Auditee organisation or a sub-contractor. Subject to appropriate hardening controls, including restricting/disabling of ports Configured according to a defined security policy, including no local administrator rights granted and session locking Up to date with the latest security patches and anti virus/malware protection at the time of the connection. • Only located in clearly designated secure Environments to which access is controlled on strict-need-to-be-there principles.		The devices should be hardened, up to date with the latest security patches, and running appropriate and up-to-date anti-malware controls. The location where the remote end point workstation is hosted should be within an appropriate location, as specified in (ii).
	(v)	Authentication Remote user access mechanisms must employ multi-factor authentication or other enhanced authentication mechanisms whenever remote access is granted:		Multi-factor authentication mechanisms increase the resistance any system has to unauthorized access by requiring the end user to have knowledge of a password and a possess access to a token device or application that generates a secondary code to be authenticated prior to the user being granted system access.

Requirement Statements			Guidelines	
		•across networks of lower security level than that being connected to •from off-site locations		
	(vi)	Security of channel The channel used to connect from the endpoint device to the target network Environment shall be secured: • The endpoint must be connected to the Auditee's Corporate Network. • End-to-end between devices that are configured and managed under security controls within the scope of the SAS certification process. • Using appropriate technologies to ensure the required level of security. • Keys and credentials used for authentication and encryption of the channel should be generated, stored and exchanged according to secure processes.		Channels for remote access will often be established between different Sites across public, shared, or lower-security networks. Connections should always take place through secured / trusted networks. • For full interactive remote access to sensitive systems (as described in 10.4.5), this should always be through the Auditee's network by wired connection directly linked to the physical Environment from which access is permitted; • For other remote access, read-only (section 10.4.2) pre-defined (section 10.4.3) or limited interactive remote access (section 10.4.4), this should be through either: o wired connection to the Auditee's network; o a trusted and pre-approved wired/wireless connection (e.g. Auditee Site Wi-Fi, home office Wi-Fi, company issued mobile device (tethered or hotspot) using an approved VPN In both cases, the expectation is that the individual is connected to the Auditee's Corporate Network. • Unknown or public networks (either fixed or wireless) should never be used, even if the channel utilises a VPN across the network. From the Auditee's Corporate Network, channels should be established to the target network Environment using appropriate technologies to ensure mutual authentication and confidentiality (typically through encryption). Appropriately configured IPsec or SSL VPNs are generally considered acceptable solutions to provide manageable and controlled connection using pre-specified security mechanisms.

Requirement Statements			Guidelines	

	(vii)	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. All connections must terminate in the DMZ/frontend zone with no direct access remotely to the secure (backend) or high secure (HSM) zones.
		The remote access network shall be configured to permit access:
		• Inbound only via the secure channel.
		• Outbound:
		  • Via one or more firewalls.
		  • Only to those target systems to which remote access is specifically required.
		  • Only using pre-determined methods of connection (e.g., RDP, SSH) for each system.
		A Jump Host shall be used within the relevant network security zone in which the targeted servers are logically and physically located:
		  • The initial connection must only permit access to a Jump Host in the DMZ/frontend zone. This Jump Host shall be used to
				Jump Hosts provide a mechanism of authenticating a user connecting from a lower security zone to a higher security zone when this type of connectivity would normally be prohibited by network security policies.
				For limited interactive remote access, companies should consider implementing additional controls within the Auditee's Corporate Network, such as:
				• Live monitoring of the connection to the target network(s) by the security operations centre.
				• Ability to terminate the connection if suspicious activity is detected.

Requirement Statements			Guidelines	
		connect to devices or servers in that zone and/or to a Jump Host located in the secure (backend) zone. • The Jump Host located in the secure (backed) zone shall be used to connect to devices or servers in that zone. • Remote access to the high secure (HSM) zone is only permitted through full interactive remote access		
	(viii)	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.		Logs for all remote access should be generated and stored according to a defined and documented policy. Logs should typically include: • Establishment of the VPN(s). • Authentication of the remote user to the Auditee's Corporate Network • Authentication of the remote user to the relevant Jump Host. • Authentication of the remote user within the target Environment (for example, Active Directory/LDAP). • Access to network devices, systems and applications by the remote user. Logs may also include: • Full session recording.
	10.5	Network security		
	10.5.1	Systems and data networks used for the processing and storage of Sensitive Process Data and related Sensitive Data shall be housed in an appropriate Environment and logically or physically separated from insecure networks.		Network configuration should be clearly documented. Secure networks should be defined and separated according to function/use. •Auditees operating SM and EUM Environments at the same Site should implement these as logically separate networks

Requirement Statements			Guidelines	
				○ Connections for transfer of data between SM and EUM Environments should normally be treated as external connections to reinforce this separation. All processing of customer data should take place on secure networks. Secure networks should be dedicated networks that are physically or logically separated from insecure networks (which would typically include those used for general business administration purposes such as office networks, HR, accounting etc.). Where multiple networks are defined, the relative security levels of the networks should be documented as part of the network security strategy. Where secure networks are logically separated, the secure network should be protected using one or more firewalls.
	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.		There should be no direct connections made between the secure network and systems on uncontrolled, untrusted or third-party networks, even where these connections are made through the firewall(s). Systems used for data exchange between the secure network and uncontrolled, third-party, networks (e.g. customers), should be positioned on de-militarized zones (DMZs). Extension of secure networks across multiple sites may be compliant with the requirements of SAS where: •Each site is SAS certified •Inter-site connections are made using appropriately secured channels (e.g. VPN). Where secure networks are extended across multiple sites and these criteria are not met for one or more of the sites, the overall secure network is unlikely to meet SAS requirements. Controls should be in place to prevent creation of unauthorised connections to secure networks, including implementation of port-level security. Where virtual server Environments are in use physical server platforms should not be used to support virtual servers on networks of different security level.

Requirement Statements			Guidelines	
	10.5.3	The system shall be implemented using appropriately configured and managed firewalls incorporating appropriate intrusion detection systems.		The configuration of firewalls and change process must be documented with the validation of the request prior to the effective change and the control after the implementation. •Firewalls should be managed from the protected (i.e. secure) network •Firewalls should be configured to provide the minimum access required only, restricted by address and port. Connections across the firewall should be originated from the secure network •Services used for permitted connections should be selected to minimise the risks to the integrity of: ○ Sensitive Data ○ Secure clients ○ Secure networks. •A business-level firewall policy document should be defined, documenting access to be provided by the firewall and the business-level requirement for it. All changes to the policy should be subject to authorisation. Authorisation should be independent of the firewall and network administrators •Firewalls should be configured in accordance with the firewall policy and subject to periodic review •It should not be possible for unauthorised changes to be made to firewall configuration (even by authorised personnel). Appropriate preventative controls could include: ○ All changes to firewall configuration being possible only under dual control ○ Automated mechanisms being in place that provide real-time notification to independent personnel of any change to firewall configuration •Firewalls should be configured to log key events; logs should be reviewed regularly (e.g. weekly). It should be demonstrated that intrusion detection systems are implemented, and alerts are treated, including an escalation process.

Requirement Statements			Guidelines	
	10.5.4	Controls shall be in place to proactively identify security weaknesses and vulnerabilities and ensure that these are addressed in appropriate timescales		Programmes of penetration testing should be in place to proactively identify potential weaknesses and vulnerabilities. Penetration tests should consider: •All networks and systems within scope of SAS certification. •Networks and identified hosts that are intentionally exposed to networks and clients of lower security level (e.g. data transfer networks) validating that other networks and hosts are not exposed. Penetration tests should normally be conducted at least 1-2 times per year or when significant changes are made to network or security configuration (e.g. creation of new data transfer networks, migration of firewalls to new platforms).
	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.		An up-to-date inventory list of the IT systems should be available including their configurations.
	(ii)	System components and software shall be protected from known vulnerabilities by having the latest vendor-supplied security patches installed.		The entire IT system environment should be maintained with the latest vendor-supplied security patches as and when they become available. Whilst immediate application of patches may not always be possible, they should be applied within reasonable timescales. Out-of-support environments should not normally be in use. Migration strategies should be in place where environments are approaching end-of-life or end-of-support by the vendor.

Requirement Statements			Guidelines	
	(iii)	System components configuration shall be hardened in accordance with industry best practice		A hardening policy should be defined and applied to systems or components based on risk. •Security devices (e.g. firewalls) should always be hardened. •Sensitive systems (systems in networks where Sensitive Data is stored, processed or transmitted) should be hardened, particularly where commodity OSs are used (e.g. Windows, Linux). •Exposed systems (e.g. customer data transfer servers) should be considered as sensitive. Auditees should be able to demonstrate how the policy has been applied to systems or components. A range of recognised international standards, recommendations and guidance for OS and system hardening are available and should be considered by Sites, (e.g. those available from NIST, CIS, RSI, SANS). Vendor recommendations should also be considered.
	(iv)	Change control processes and procedures for all changes to system components shall be in place.		Any change to IT systems should be subject to a documented change management process with a formal validation process.
	(v)	Processes shall be in place to identify security vulnerabilities and ensure the associated risks are mitigated.		A programme of regular vulnerability scanning should be in place to consider: •All systems on the secure network(s); •All systems on networks used for customer data transfer. Scans should be completed: •After each major change; •Monthly for internal ‘secure’ networks; •Monthly for externally-facing networks used for customer data transfer. Sites should monitor vendor and industry sources for announcements of vulnerabilities and patches. Local policies should be in place that define target timescales for implementation of patches based on the level of risk. The level of risk may be determined based on:

Requirement Statements			Guidelines	
				•The severity of the vulnerability; •The context of the system where the vulnerability exists. Critical vulnerabilities should always be prioritised for implementation. Critical vulnerabilities in externally facing system components should always be remediated as an immediate priority (e.g. within 7 days). Critical vulnerabilities in system components within secure networks should be remediated as high priority (e.g. within 30 days).
	(vi)	Comprehensive measures for prevention and detection of malware and viruses shall be deployed across all vulnerable systems.		The malware control strategy should always emphasise prevention of infection as the primary control. Detection mechanisms should be used as a final line of defence in the event that prevention measures fail. Response mechanisms should be in place where possible infections occur. The prevention strategy should consider general best practice through a combination of: •Regular application of security patches and updates. •Appropriate network segmentation and separation. •Restrictions on the use of uncontrolled external media. •Definition of a malware perimeter for the Site. All incoming data (including application software) crossing the perimeter should be explicitly checked, including: ○ Email; ○ Direct data transfer (e.g. FTP); ○ Physical media (e.g. CD/DVD-ROM, external USB storage device, USB memory key). Detection mechanisms (e.g. anti-virus software) should be: •Installed on all vulnerable systems. •Updated regularly with virus definitions. •Subject to regular checks to identify systems that have not been updated. Where systems cannot support anti-virus software, controls should be in place to ensure viruses cannot be introduced. Such controls should include:

Requirement Statements			Guidelines	
				•Scanning of data and applications software prior to introduction to the system. •Isolation of network segments containing such systems. Where possible infections are detected, mechanisms should be in place to ensure that these are reported and escalated quickly. Clear response procedures should be in place. Possible infections in systems and networks used for the processing of Sensitive Data should always be treated as security incidents. Root-cause of infections should always be identified, and the anti-virus strategy reviewed and updated as appropriate.
	(vii)	Unattended terminals shall timeout to prevent unauthorised use and appropriate time limits shall be in place.		Configuration of timeouts should be controlled by the administrator; users should be prevented from changing timeout settings.
	(viii)	Decertification/decommissioning of assets (such as IT systems) used as part of the SP shall be documented and performed in a secure manner.		The requirements of section 9.4 should be applied to network devices (routers, firewalls etc.)
	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.		A programme of regular back-ups should be defined. Back-up frequency and retention period should be defined based on the importance of the data contained. Sensitive Data should be appropriately protected in accordance with the Site's security classification and data handling guidelines. Such controls should normally include encryption of data and physical security of storage media. Storage media used for back-ups should be selected, implemented, managed and maintained to ensure adequate protection from: •Environmental threats (e.g. fire, flood, temperature extremes, electrical and electro-magnetic effects); •Accidental or deliberate corruption; •Unauthorised access.

Requirement Statements			Guidelines	
				Typically, media should be stored separately from the systems themselves. Back-ups retained on-site should be stored away from server rooms in a data / media fire safe. Off-site storage of one generation of back-ups should be considered. Procedures for restoration of data from back-up should be checked periodically (typically once or twice per year). Procedures should be in place to ensure that production status can be reinstated to the correct point when/if such data is restored from back-up.
	10.7	Audit and monitoring		
	10.7.1	Audit trails of security events shall be maintained and procedures established for monitoring use.		Systems and applications on the secure network should implement logging of security relevant events including: •Logon attempts (successful and unsuccessful); •Logoff; •Password changes; •Attempts to exceed permissions; •Changes to audit logs. Audit logs should be reviewed regularly (e.g. weekly) to identify suspicious behaviour. Specific applications on the secure networks (e.g. data processing, Personalisation) should implement full logging of all events relevant to the Sensitive Process, as described in section 7.4.1.
	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.		Where operations are outsourced, Auditees should demonstrate that appropriate controls are in place to enforce the IT security policy. Auditees should take responsibility for auditing and controlling external facilities management partners. See also 2.4.2.

Requirement Statements			Guidelines	
SM	10.9	Software Development		
	10.9.1	The software development processes for the SM-DP, SM-SR, SM-DP+, SM-DS or eIM shall follow industry best practices for development of secure systems.		The development processes for the software/cloud services available for use for hosting the SM service should be resistant against the top 10 security flaws described by the OWASP (www.owasp.org).
DC	10.9.2	The software development processes for applications and bespoke software deployed within the SM Environment shall follow industry best practices for development of secure systems.		The software development processes should follow recognised industry standards; for example, the W3C standard (www.w3c.org).
DC	10.10	Multi-tenancy Environments		
	10.10.1	Multi-tenant solutions must prevent cross-contamination of assets between different customers.		Prevention should be ensured by assigning access rights for each tenant to their own environment only, with no possibility for any tenant to access any other tenant's environment.
	10.10.2	Multi-tenant solutions on the same physical hardware shall ensure customer data is logically segregated between different customers.		Logical segregation refers to utilisation of the same hardware and the same instance, with separation enforced through different logical access rights.
	10.10.3	Each tenant running their own applications must use a unique tenant ID for the running of all application processes.		All processes running on shared infrastructure should be run using unique IDs for each tenant, including: •Applications; •Common Gateway Interface (CGI) scripts. Controls should be in place that prevent: •Processes from running that do not have a recognised tenant ID; •Tenant processes from being initiated with IDs not associated within the tenant.

Requirement Statements			Guidelines	
	10.10.4	Use of shared infrastructure shall by controlled to ensure appropriate availability of shared system resources for all tenants.		Controls should be established to ensure that SAS-SM customer SLAs can be adhered to, and monitored internally, to ensure suitable restrictions on utilization of shared system resources (i.e. to prevent one customer monopolizing resources).
DC SM	10.10.5	The Auditee shall ensure that customer data is only stored within SAS-certified physical locations meeting all requirements detailed in section 5 of this document, including any Sites to which data is, or may be, replicated as part of Business Continuity plans.		The Auditee should prevent any data replication or other form of backup to outside of the certified Sites or regions. Controls should ensure that all SM data is only stored at SAS-SM certified data centre location(s), that are specifically permitted under customer SLAs.
	10.11	Internal audit and control		
	10.11.1	IT security controls shall be subject to a rigorous programme of internal monitoring, audit and maintenance to ensure their continued correct operation.		A programme of internal audits/controls should be defined that demonstrates appropriate consideration of: •The frequency of checks required for each area addressed by the internal audit/control mechanism. •The structure of the audits/controls themselves, including clear guidance on what should be checked and how. •The recording / documentation and follow-up process for audits/controls undertaken and actions identified. The Auditors will expect to see evidence that processes and systems are working correctly, and that internal audits/controls have been carried out according to the schedule. There should be appropriate coverage of all aspects of the system; the audit/control programme should be defined around the need to provide appropriate coverage, rather than the availability of resource. In particular, there should be evidence that the internal audit/control system has been designed to consider the different IT systems in use and the sensitivity of the data stored or processed. All IT systems should be audited against application of the IT security policy.

Requirement Statements				Guidelines	
					Auditors should have received appropriate training in the structure and content of internal audits/controls.

Requirement Statements			Guidelines	
11 Two-Step Personalisation Process				
UP	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).			Requirements for the two-step Personalisation process are not intended to apply where the full Personalisation process takes place in the same physically secure EUM Environment. Requirements in this section have been added to enable SAS-UP to support products, such as eUICC, where the two Personalisation steps may be carried out at different times, potentially in different Environments under the control of different entities. Production processes for product types other than those listed in this requirement are not currently supported for SAS-UP certification, although this may change in the future. Auditees involved in the eUICC production chain will be expected to demonstrate that the combined solution is secure.
	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.		Auditees should demonstrate controls for preventing Duplicate production. Personalisation Data for each eUICC should exist and be used in exactly one instance. A mechanism should be implemented to prevent the Duplicate use of Personalisation Data.
	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.		Auditees must demonstrate that hardware credentials are generated and provisioned in a secure manner. Credentials should be generated using security modules (HSM) that are FIPS or Common Criteria certified as required by section 6.4.3 of this document. Where generation and provisioning to eUICC hardware occur in separate facilities, a secure exchange mechanism should be in place.

Requirement Statements			Guidelines	
	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.		Auditees should demonstrate that hardware credentials are provisioned in a secure manner.
	11.3.2	Perso_SC can occur only once within the device lifecycle.		Auditees should demonstrate that hardware credentials can be used only once.
	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 in section 7 of this document.		Auditees should demonstrate that OS credentials are generated and in a secure manner. Credentials should be generated using security modules (HSM) that are FIPS or Common Criteria certified as required by section 6.4.3 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.		Auditees should demonstrate that OS credentials are to be provisioned only to authenticated eUICC hardware that has been personalised at an SAS-UP certified Site. Auditee may include in such demonstration mechanisms based on cryptographic means and legal obligations.
	11.5.2	Personalisation of UICC OS credentials to a device shall be carried out by establishing a secure channel that:		[10] 7.3.2, Package 2: Loader defines a set of security requirements as part of a protection profile.
	(i)	Utilises unique security credentials personalised to the device in the Perso_SC step.		Auditees should demonstrate that:

Requirement Statements				Guidelines	
	(ii)	Can only be initiated by an appropriately authorized entity in possession of the security credentials.			•OS credentials provisioning process, combined with capabilities provided by the eUICC hardware manufacturer, satisfy requirements equivalent to those described in Package 2: Loader; principally that: •The means to establish a secure channel is rooted in a certified part of the target hardware; •The communication channel itself is secure; •The service it provides is secure; •The combined solution is secure; •Hardware includes the additional authentication requirements of [10] 7.2 Authentication of the Security IC. It is not the role of the SAS-UP Audit to test or validate the product. Auditees should demonstrate compliance through evidence of testing of the target product.
	(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 (Normative) Limited interactive remote access from non-certified locations

As described in 10.4.4, limited interactive remote access is permitted to take place from non-certified locations to specified systems for specified activities only. The permitted systems and activities are documented below. These lists may be updated from time-to-time to add systems and activities as required. Auditees should not assume that other systems or purposes will be permitted unless they have been added to these lists.

A.1 Systems

The following systems / classes of systems are permitted to be included within limited interactive remote access arrangements in 10.4.4. In all cases, systems may only be accessed for the mapped purposes defined in this Annex.

System		Description
S1	Jump Host / Bastion Host	The servers that provide a mechanism of authenticating a user connecting from a lower security zone (e.g. Auditee's Corporate Network) to a higher security zone (e.g. DMZ/frontend zone).
S2	Data transfer servers	Servers (e.g. Secure File Transfer Protocol (SFTP)) that are used to enable secure data transfer between external networks (e.g. customers or corporate) and the target network.
S3	Management servers	Servers that are used for management activities within the target network, such as DNS, virtualization hosts, WSUS, AV, NTP, etc.). These servers do not hold Sensitive Data.
S4	Application servers	Servers that are used to host the eSIM solution.
S5	Database server	Servers used to host the databases that will hold the eSIM solution data.

A.2 Activities

The following activities are permitted to be included within limited interactive remote access arrangements as part of 10.4.4. In all cases, activities may only be applied for the defined systems / classes of system defined in this Annex.

Activity		Description
A1	Initial deployment	The initial deployment of a server into the environment, which would include the build and hardening.
A2	Patch management	Applying approved patches/updates to the servers (patch must be already present in the target environment)

A3	Rebooting the server	Rebooting of a server, such as following a patch/update
A4	Customer creation and management	Setting up and managing customers access on the application server
A5	Profile Management	Management of Profile data on the application.
A6	Database management	Management of database setup and configuration where there is no access to Sensitive Data (even if encrypted) held in the database.

A.3 Mapping

The following table defines which activities may be applied for each system. A ✓ indicates that the particular activity is permitted to be carried out for the corresponding system/class of system. Where a mapping is not explicitly indicated as accepted then Auditees should consider that the activity is not permitted for the system. Activities and systems that are not explicitly included within this annex should be considered to be not permitted.

		Activity					
		A1: Initial deployment	**A2: Patch management**	**A3: Rebooting the server**	**A4: Customer creation and management**	**A5: Profile Management**	**A6: Database Management**
System	**S1: Jump Host / Bastion Host**	✓	✓	✓			
	S2: Data transfer servers	✓	✓	✓			
	S3: Management servers	✓	✓	✓			
	S4: Application servers	✓	✓	✓	✓	✓	
	S5: Database server	✓	✓	✓			✓

Annex B Document Management

B.1 Document History

Version	Date	Brief Description of Change	Editor / Company
1.0	26 Jul 2016	Created based on SAS-UP Guidelines document v5.0. Added Certificate Management requirements and PKI Certificate Policy security requirements.	James Messham, FML
2.0	31 Mar 2017	Incorporated SAS-SM requirements, including SM-DP+ and SM-DS.	RSPSAS subgroup
2.1	2 Jan 2018	Updated guidelines on external network connections (section 10.4.2)	SAS subgroup
3.0	26 Jun 2019	Added two-step personalisation process (Integrated eUICC) guidelines. Added guidance on use of a single HSM platform for EUM and SM functions and network separation at such sites. Added guidance on SM solution demonstration expectations.	Or Elnekaveh, Qualcomm James Messham, FML Neil Shepherd, NCC Group
4.0	25 Jul 2019	Added guidelines for transfer of sensitive assets between sites.	SAS subgroup
5.0	18 Jun 2020	Development of remote user access guidelines	SAS subgroup
6.0	20 Nov 2020	Add specific guidelines for auditing of cloud service providers.	SAS subgroup
7.0	2 Jul 2021	Add guidelines for new requirement at 2.4.2 – clarify subcontractor responsibilities	James Messham, FML & Neil Shepherd, SRC
7.1	22 Sep 2021	Clarifications to HSM guidelines. Addition of SAS-UP definitions.	Saïd Gharout, Kigen
8.0	1 April 2022	Enable auditing and certification of certain cloud service provider-managed HSMs used in SM solutions. Make this PRD the single source of SAS requirements and guidelines, allowing withdrawal of PRD FS.17.	David Maxwell, GSMA
8.1	1 Jun 2022	Clarification to guidelines for HSM as a managed service.	Vincent Bourdaraud, Idemia; James Messham, FML; David Maxwell, GSMA.
9.0	1 Oct 2022	Permit access to Class 2 assets remotely using a secure connection under the control of the auditee. Extend two-step personalisation to all eUICC types	Saïd Gharout, Kigen

Version	Date	Brief Description of Change	Editor / Company
9.1	22 Feb 2023	CR1015: General review and updates	James Messham, FML
10.0	5 Jul 2023	CR1016: Updated remote user access requirements and guidelines.	SAS group
11.0	6 Dec 2023	CR1017: Add eSIM IoT Remote Manager CR1018: Update HSM certification requirement.	SAS group
11.1	18 Sep 2024	CR1019: Clarify key management responsibility requirements	SAS group

B.2 Other Information

Type	Description
Document Owner	GSMA SAS group
Editor / Company	David Maxwell, GSMA

It is our intention to provide a quality product for your use. Comments, corrections and suggestions are always welcomed. Please contact us at sas@gsma.com.