

GSMA SAS Guidelines for Subscription Manager Roles

Version 1.0

13 October 2014

This is a Non-binding Permanent Reference Document of the GSMA

Security Classification: Non-confidential

Access to and distribution of this document is restricted to the persons permitted by the security classification. This document is confidential to the Association and is subject to copyright protection. This document is to be used only for the purposes for which it has been supplied and information contained in it must not be disclosed or in any other way made available, in whole or in part, to persons other than those permitted under the security classification without the prior written approval of the Association.

Copyright Notice

Copyright © 2014 GSM Association

Disclaimer

The GSM Association ("Association") makes no representation, warranty or undertaking (express or implied) with respect to and does not accept any responsibility for, and hereby disclaims liability for the accuracy or completeness or timeliness of the information contained in this document. The information contained in this document may be subject to change without prior notice.

Antitrust Notice

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

Table of Contents

1 General 3
1.1 Introduction 3
1.2 Audits 3
1.3 Definitions 4
1.4 Abbreviations 4
1.5 References 5
2 Guidelines 6
9.2 Policy, Strategy and Documentation 6
9.3 Organisation and Responsibility 8
9.4 Information 10
9.5 Personnel Security 11
9.6 Physical Security 13
9.7 SM-DP and SM-SR Data Management 19
9.8 SM-DP and SM-SR Service Management 22
9.9 IT System and Network Management 23
9.10 Control, Audit and Monitoring 28
9.11 Incident Response and Reporting 31
Annex A Document Management 32
A.1 Document History 32
A.2 Other Information 32

1 General

1.1 Introduction

This document provides guidelines on compliance with the GSMA Security Accreditation Scheme for Subscription Management Roles (SAS-SM), a scheme through which Subscription Manager – Secure Routing (SM-SR) and Subscription Manager – Data Preparation (SM-DP) suppliers subject their operational sites to a comprehensive security audit to ensure security measures to protect the interests of mobile network operators (MNO).

The guidelines help these suppliers understand how to interpret and apply the SGP.07 GSMA SAS Standard for Subscription Manager Roles [1] operationally. The guidelines should be read and used in conjunction with the SAS standard [1] and are not intended to replace or supersede the SAS-SM standard.

1.2 Audits

SAS-SM audit processes and participants are described in SGP.09 GSMA SAS Methodology for Subscription Manager Roles [2]. The SAS-SM audit itself will remain the basis by which compliance with the SAS-SM standard [1] is assessed. Certification by the GSMA will be based on an assessment and recommendation by an Audit Team.

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 on-going successful application
- They comply with the basic principles of the SGP.07 [1]
- 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 of their practical effectiveness. When scheduling audits, sites are 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 this guidelines document may also be acceptable to the Audit Team if they do satisfy the above criteria.

1.3 Definitions

Term	Description
Actor	Person who is involved in, or can affect, the Sensitive Process.
Audit Team	Two auditors, one each from different auditing companies, jointly carrying out the audit on behalf of the GSMA.
Auditees	SM-SR or SM-DP suppliers subject of the audit
Authorised	Permitted by the Supplier
Business Continuity	Capability of the entity performing the role of an SM-DP or SM-SR to continue delivery of SM-DP or SM-SR functionality at acceptable predefined levels following a failure incident. According to SM-DPs or SM-SRs customer requirements.
Environment	Environment of use of the Sensitive Process limited to the security aspects
eUICC Management	A set of functions related to the registration of a eUICC to a SM-SR and the change of SM-SR for a eUICC.
High Security Area	Restricted areas off-limits to unauthorised personnel in which assets are stored and processed
Key	Refers to any logical key for example, a cryptographic key
Physical Keys	The keys and/or combinations used for vaults, safes and secure cabinets
Platform Management	A set of functions related to the transport, enabling, disabling and deletion of a Profile on a eUICC.
Profile	Combination of a file structure, data and applications to be provisioned onto, or present on, a eUICC and which allows, when enabled, access to a specific mobile network infrastructure.
Profile Management	A set of functions related to the downloading, installation and content update of a Profile in a dedicated eUICC.
Sensitive Process	The Sensitive Process represents the security evaluation field, covering the processes and the assets within those processes
Restricted area	A physical area where access is controlled but is not necessarily on a one by one basis.
SM-DP	An entity that provides SM-DP functionality to its customers.
SM-SR	An entity that provides SM-SR functionality to its customers.
Supplier	SM-SR or SM-DP

1.4 Abbreviations

Term	Description
BCP	Business continuity plan
eUICC	Embedded UICC
FIPS	Federal Information Processing Standard
GSMA	GSM Association
HSA	High security area
HSM	Hardware security module

Term	Description
IT	Information Technology
MNO	Mobile network operator
SAS-SM	Security Accreditation Scheme for Subscription Management Roles
SGP.nn	Prefix identifier for official documents belonging to GSMA SIM Group
SLA	Service level agreement
SM-DP	Subscription Manager – Data Preparation
SM-SR	Subscription Manager – Secure Routing
SP	Sensitive Process

1.5 References

Ref	Doc Number	Title
[1]	SGP.07	GSMA SAS Standard for Subscription Manager Roles
[2]	SGP.09	GSMA SAS Methodology for Subscription Manager Roles
[3]	SGP.01	Embedded SIM Remote Provisioning Architecture
[4]	SGP.02	Remote Provisioning Architecture for Embedded UICC Technical Specification

2 Guidelines

Reference	*Statements from SAS-SM Standard*	*Guidelines*
9.2 Policy, Strategy and Documentation		
	The security policy and strategy provides the business and its employees with a direction and framework to support and guide security decisions within the company.	
9.2.1	Policy	
9.2.1.1	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.
9.2.1.2	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.
9.2.2	Strategy	
9.2.2.1	A coherent security strategy must be defined based on a clear understanding of the risks. The strategy shall use periodic risk assessment as the basis for defining, implementing and updating the site security system. The strategy shall be reviewed regularly to ensure that it reflects the changing security Environment through on-going re-assessment of risks.	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 risk assessments taking place. Results of risk assessment should be used to drive revisions to the security strategy and security management system. Risk assessments shall include as a minimum all sensitive assets identified as being in the scope for SM-SR/SM-DP processes.
9.2.3	Business Continuity Planning	

Reference	Statements from SAS-SM Standard	Guidelines
9.2.3.1	Business Continuity measures must be in place in the event of disaster, according to customers' service level agreements.	The Business Continuity plan (BCP) should be documented as a working business document covering; • Definition of service affecting incidents based on a risk assessment and impact analysis • Processes for management of service-affecting scenarios focusing on customer data protection. • Maintenance of the integrity of the security system and production processes. • The BCP test should be reviewed as per the service level agreements (SLA) with the customer defining the continuity objectives.

Reference	Statements from SAS-SM Standard	Guidelines
9.3 Organisation and Responsibility		
9.3.1	Organisation	
9.3.1.1	To successfully manage security, a defined organisation structure shall be established with appropriate allocation of security responsibilities.	The security organization should be clearly defined and documented as part of the security management system.
9.3.1.2	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.
9.3.2	Responsibility	
9.3.2.1	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.
9.3.2.2	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 (for example, physical and IT security), suppliers should be able to demonstrate an overall co-ordinated / integrated approach to security management with responsibilities clearly defined.
9.3.2.3	Asset protection procedures and responsibilities shall be documented throughout the SP	Employees shall be made responsible and accountable for sensitive information within their care throughout the service process. Procedures for documenting handover of assets should be clearly defined. An asset list and asset protection mechanisms applicable at each processing stage should be documented as part of the service process and supporting documentation. Detailed requirements are described in SGP.07 section 6.1 and appendix A.
9.3.3	Contracts and Liabilities	
9.3.3.1	In terms of contractual liability responsibility for loss shall be documented. Appropriate controls and	Contracts with customers should clearly define responsibility and liability for data loss.

Reference	Statements from SAS-SM Standard	Guidelines
	insurance shall be in place.	Where contracts with customers are not standardised (that is, 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 data, and for consequential loss where defined within contracts. Normally it will be expected that insurance will be in place to cover such losses.

Reference	Statements from SAS-SM Standard	Guidelines
9.4 Information		
	The management of sensitive information, including its storage, archiving, deletion and transmission, can vary depending on the classification of the asset involved.	
9.4.1	Classification	
9.4.1.1	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 SGP.07 [1] . The classification structure should not exist in isolation. Evidence should exist that the classification structure is: • Linked to a set of asset protection requirements / standards • Mapped onto business processes to identify where sensitive assets are handled, and the asset protection standards are applied • Specifying the treatment during the entire lifecycle (that is, creation, processing, storage, transmission and disposal) The Audit Team will expect to see evidence of the classification and treatment being applied throughout the operation during the audit.
9.4.2	Data and Media Handling	
9.4.2.1	Access to sensitive information and assets must always be governed by an overall ‘need to know’ principle.	A clear documented process should exist defining the physical and logical individual access rights. The ‘need to know’ principle should be ensured that an individual is granted no more than sufficient access to perform his or her job.
9.4.2.2	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. Specific controls should be in place for the secure handling of all media during the entire lifecycle. Of particular importance is the treatment of sensitive data in electronic form stored on old or faulty equipment.

Reference	Statements from SAS-SM Standard	Guidelines
9.5 Personnel Security		
	A number of security requirements shall pertain to all personnel working within the SP.	
9.5.1	Security in Job Description	
9.5.1.1	Security responsibilities shall be clearly defined in job descriptions.	An individual having access to sensitive assets should have a job description in which security tasks are defined. For all other individuals a general security declaration should be defined.
9.5.2	Recruitment Screening	
9.5.2.1	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 • Validation of education and employment history 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 annual basis.
9.5.3	Acceptance of Security Rules	
9.5.3.1	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. Temporary employees, contractors and visitors should sign confidentiality agreements.
9.5.3.2	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 acceptance 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 9.5.3.3).

Reference	Statements from SAS-SM Standard	Guidelines
9.5.3.3	Adequate training in relevant aspects of the security management system shall be provided on an on-going basis.	All new employees should be provided with induction training covering basic security principles applicable throughout the plant. Employees should receive refresher training in security principles on a regular basis for example, annually. 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 security training; auditable records should exist of training taking place, and those employees trained. Specific, focused, security training should be conducted for employees with specific security responsibilities.
9.5.4	Contract Termination	
9.5.4.1	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 (for example, physical and logical access) have been revoked. Procedures should exist to escort employees from the premises where appropriate. Employees should be reminded of their obligations under the confidentiality agreement prior to leaving the company.

Reference	Statements from SAS-SM Standard	Guidelines
9.6 Physical Security		
	A building is part of the site where SM-DP or SM-SR functionality is provided, SM-DP or SM-DP systems are deployed and eUICCs information, MNO information and Profile information are stored. Buildings in which sensitive assets are processed shall be strongly constructed. Constructions and materials shall be robust and resistant to outside attack as manufacturers must ensure assets are stored within high security areas and restricted areas by using recognised security control devices, staff access procedures and audit control logs.	Strongly constructed means precast or masonry blocks or materials with equivalent strength. External windows and doors must be protected by mechanisms such as motion or magnetic contact detector. High security area (HSA) means an area where access is controlled on a strict person by person basis including anti-pass back mechanisms and equipped with security devices. Restricted Area means an area where access is controlled by an access control system.
9.6.1	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.	Risk assessments should be conducted / updated on a regular basis (for example, annually). Risk assessment findings should be used to drive continuous improvement and modification of controls.
9.6.1.1	The strategy shall be encapsulated in a security plan that:	
	• 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.

Reference	Statements from SAS-SM Standard	Guidelines
	• 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 the HSA. 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 create partitions within the HSA, to segregate assets as per of their sensitivity.
	• Defines physical security protection standards for each level of secure area.	The expected, or required, physical protection standard for HSA and restricted area should be defined, to consider elements defined in 9.6.2.1.
9.6.2	Physical Protection	
9.6.2.1	The protection standards defined in the security plan shall be appropriately deployed throughout the site, to include:	
◦	• deterrent to attack or unauthorized entry,	Sites should make use of visible security mechanisms to act as a deterrent, which may include: • Fences at the site boundary • CCTV • Access control • Guard presence / Site monitoring
◦	• physical protection of the building and secure areas capable of resisting attack for an appropriate period,	Response and escalation times for secure areas shall be defined. Requirements for secure areas shall as a minimum include: • Walls should be strongly constructed • Points of access (windows and doors) to HSAs should be minimised • Doors and windows giving direct access into secure areas from outside (for example, emergency exit doors) should be physically hardened and include for example, multi-point locking mechanisms so that removal or cutting of hinges should not allow doors to be opened.

Reference	Statements from SAS-SM Standard	Guidelines
◦	• 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 shall include Movement detection sensors and may also include barrier systems and/or seismic and vibration sensors
◦	• 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.
◦	• 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 HSAs are cleared of all personnel during evacuation • Attempts to restrict unauthorised re-entry to buildings and HSAs, including: • 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 (for example, damaged security systems or physical controls).
◦	• 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. Alarms should be recorded to a system-generated log. Controls should be in place to enforce the integrity of the log.

Reference	Statements from SAS-SM Standard	Guidelines
◦	• 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 when legally authorised. 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: • Cameras must record as minimum 4 frames per second. • 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.

Reference	Statements from SAS-SM Standard	Guidelines
9.6.3	Access Control	
9.6.3.1	Clear entry procedures and policies shall exist which cater for the rights of employees, visitors and deliveries to enter the SP. These considerations should 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 mobile network operator (MNO) making the change. 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 secure areas should be controlled. All Physical Keys used for HSA and restricted area should be catalogued. Issue of keys to employees should be tracked according to an auditable system. Keys to secure areas should be under strict control and subject to regular audit.
9.6.3.2	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. Regular audits shall be undertaken to monitor access control to the secure area.	All access to secure areas should be strictly controlled and auditable using the access control system. All employees, visitors and contractors to the secure areas should be uniquely identifiable to the access control system. Access to sensitive locations within the HSAs should make use of dual control (where 2 people are present within the area). Sensitive locations may include: • Key ceremony rooms • Server rooms Movements into, and out of, the secure areas, and between defined zones within the

Reference	Statements from SAS-SM Standard	Guidelines
		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 areas where sensitive information is created, stored and processed should be on a strict 'need to be there' basis, covering employees, contractors and visitors to the site.
9.6.4	Security Staff	
9.6.4.1	Security staff are commonly employed or sub-contracted by suppliers. Duties for security staff 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 Audit Team expect that security staff will demonstrate a basic competence in their operation during the audit.

Reference	Statements from SAS-SM Standard	Guidelines
9.7 SM-DP and SM-SR Data Management		
	SM-DPs or SM-SRs will be responsible for lifecycle management of data used for remote provisioning, management of eUICCs and management of Profiles. 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.	
9.7.1	Data Transfer	
9.7.1.1	SM-DPs or SM-SRs shall take responsibility to ensure that electronic data transfer to other entities in the Embedded UICC eco-system is appropriately secured.	A document should identify the relevant data transfer and their associated protection. Appropriate electronic data transfer mechanisms including encryption of sensitive data should be compliant with SGP.02 Remote Provisioning Architecture for Embedded UICC Technical Specification [4] when applicable or agreed with external third parties when not applicable.. In that case suppliers should demonstrate that they have worked to ensure data transfer mechanisms are appropriate to the sensitivity of the data concerned. Where demanding insecure data transfer mechanisms, suppliers should formally notify (in writing) third parties of the unsuitability of the data transfer mechanism.
9.7.2	Access to Sensitive Data	
9.7.2.1	SM-DPs or SM-SRs shall prevent direct access to sensitive SM-DP or SM-DR data. User access to sensitive data shall be possible only where absolutely necessary. All access must be auditable to identify the date, time, activity and person responsible, where audit data must be protected in	Sensitive data should be protected as per the definition in the asset classification at all stages of storage, processing and transmission, except where decrypted data is specifically required to complete the processing stage. Appropriate data encryption technologies should be used to protect sensitive data as per the recommendation set in SGP.02 [4]. Keys should be managed securely. Sensitive data should be deleted as per a documented data retention policy. Sensitive

Reference	Statements from SAS-SM Standard	Guidelines
	terms of integrity.	data should always be deleted using a secure wipe mechanism. 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 data is possible or required it must always be auditable. Control of the audit trail must be independent of personnel with access to data. Accessing to the data should be recorded in an audit trail file (date, time, activity, person) that is not able to be tampered by the non-privileged users
9.7.3	Cryptographic Keys	That section applies to the keys defined in the asset classification list in the document SGP.07 [1]
9.7.3.1	Cryptographic keys used for data protection shall be generated, exchanged and stored securely	Key management must be governed by the two principles that are split knowledge and dual control
9.7.3.2	The cryptographic computation (derivations, random generations) and storage of keys involved in the protection of the sensitive data shall rely on high security modules (HSM) that are FIPS 140-2 level 3 certified.	The service provider must provide a copy of the FIPS certification with a clear identification of the hardware board and associated firmware of the cryptographic device. This equipment should be subject to a documented commissioning and /or decommissioning process. The HSMs in use must be dedicated to the SM services. Any activity on HSM's should be logged. Integrity of audit trails must be ensured
9.7.3.3	The cryptographic key management process shall be documented and cover the full lifecycle of the keys.	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). Any activity on keys should be logged. Integrity of audit trails must be ensured.
9.7.3.4	The key lengths defined in SGP.02 [4] shall be used	
9.7.4	Data Integrity	
9.7.4.1	Controls shall be in place to ensure that the same, authorized, data from the correct source is used for the SM-DP or SM-SR processes and supplied to the	Control of authentication should be done between Actors as per the functional specifications (for example, the certificate chain in the reference document SGP.02 [4]) when applicable.

Reference	Statements from SAS-SM Standard	Guidelines
	SM-DP's or SM-SR's customer.	When non applicable, there must be a specific authentication mechanism with the third party (for example, specific communication link or specific data transfer process)

Reference	*Statements from SAS-SM Standard*	*Guidelines*
9.8 SM-DP and SM-SR Service Management		
9.8.1	Personnel	
9.8.1.1	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.	Please refer to the section 9.5 Personnel Security
9.8.2	SM-DP and SM-SR Service	
9.8.2.1	Systems used for the remote provisioning and management of Profiles shall be compliant with the security requirements defined in SGP.01 [3] and SGP.02 [4].	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
9.8.2.2	SM-DPs or SM-SRs must prevent cross-contamination of assets between different MNO customers.	SM-SR/SM-DP services shall be logically segregated from other services and SM-SR and SM-DP shall be logically segregated from each other. Applications used to support multiple tenants shall ensure appropriate segregation between individual tenants. For example by using key segregation and access rights allocation.
9.8.3	Remote Entity Authentication	
9.8.3.1	All authorized entities in the SM-DP or SM-SR processes shall be authenticated by appropriate authentication protocols. for example, SM-SR, SM-DP, 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 [4]) when applicable. When not applicable, there must be a specific authentication mechanism with the third party (for example, specific communication link or specific data transfer process)

Reference	Statements from SAS-SM Standard	Guidelines
9.9 IT System and Network Management		
9.9	Secure operation of IT system and network facilities is paramount to the security of data and services. In particular, the processing, storage and transfer of information, which if compromised, could have serious consequences for the MNO, must be considered. Operation of IT systems and networks must ensure that comprehensive mechanisms are in place to preserve the confidentiality, integrity and availability of data and services. The software implemented on the SM-DP or SM-SR IT systems must implement the Profile and Platform Management protocols in terms of security as specified in SGP.01 [3] and SGP.02 [4].	
9.9.1	Policy	
9.9.1.1	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.
9.9.2	Segregation of Roles and Responsibilities	
9.9.2.1	Responsibilities and procedures for the management and operation of IT systems and networks shall be established. Security related duties shall be segregated from operational activities to minimise risk.	Roles and responsibilities for administration of computer systems should be clearly defined. Administration of production systems and networks should not be carried out by users who have security related duties. Users whose function it is to handle and process production data shall not have the capability to administer the production systems. Roles for review of audit logs for systems employed in the SM-SR and/or SM-DP solution should be separated from privileged users (for example, administrators)

Reference	Statements from SAS-SM Standard	Guidelines
9.9.3	Access Control	
9.9.3.1	Physical access to sensitive IT system facilities shall be controlled	Servers and sensitive computer facilities (for example, data processing servers) shall be located in a restricted area within the HSA. Different HSAs can exist to host the system components. The HSA should be protected by the site alarm system when not occupied.
9.9.3.2	An access control policy (including remote access) 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 processes 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.
9.9.3.3	Passwords shall be managed effectively and strong authentication shall be deployed where remote access is granted.	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 • Validity • History Where systems are not capable of enforcing the policy, additional procedural controls should be used to ensure the policy is applied. Remote access mechanisms should employ enhanced authentication mechanisms. (two factor mechanism)
9.9.3.4	Remote access shall only be permitted from an authorised site.	Remote access must be done from an authorised Restricted Area

Reference	Statements from SAS-SM Standard	Guidelines
9.9.4	Network Security	
9.9.4.1	Systems and data networks used for the processing and storage of sensitive data should be housed in an appropriate Environment and logically or physically separated from insecure networks. Data transfer between secure and insecure networks must be strictly controlled according to a documented policy defined on a principle of minimum access.	Network configuration should be clearly documented; an up to date network diagram that indicates in-scope data flows shall be available. All processing of customer data shall take place on secure networks. Processing of secure data shall take place on dedicated networks different from the insecure networks (office, accounting, human resources). Virtual LANs are not considered a secure segregation mechanism. The secure network should be protected using one or more firewalls: • Firewalls should be managed from the protected (that is, 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. • 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. • Firewalls should be configured to log key events; logs should be reviewed regularly (for example, weekly) Systems used for data exchange between the secure network and uncontrolled, third-party, networks (for example, customers), should be positioned on de-militarized zones (DMZs). When web applications are used, web application firewall shall be implemented.
9.9.4.2	The system shall implement a 3 tier dedicated security architecture.	There should be an architecture document introducing systems components.
9.9.4.3	The system shall be implemented using appropriately configured and managed firewalls incorporating appropriate intrusion detection	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.

Reference	Statements from SAS-SM Standard	Guidelines
	systems.	It must be demonstrated that intrusion detection systems are implemented and alerts are treated, including an escalation process.
9.9.5	IT Security	
9.9.5.1	Data Management	
9.9.5.1.1	Multi-tenant SM-DP or SM-SR 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.
9.9.5.1.2	Database administration must be strictly controlled and managed. Each access to databases shall be authenticated, authorized and irreversibly logged.	Data base administration activity must be recorded in an audit trail file that is protected in terms of integrity.
9.9.5.1.3	Data shall be stored encrypted in the database according to the asset classification	Refer to the asset classification list to identify the data to be encrypted when at rest
9.9.5.1.4	Exchange of sensitive data within the SM-DP or SM-SR IT systems shall be end to end encrypted.	Refer to SGP.02 [4] to identify sensitive data exchanges.
9.9.5.1.5	A data retention policy shall be defined.	Data retention policy must be defined in line with the customers' requirements.
9.9.5.2	System configuration and maintenance	
9.9.5.2.1	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 shall be available including their configurations.
9.9.5.2.2	Ensure that all system components and software are protected from known vulnerabilities by having the latest vendor-supplied security	The entire IT system Environment shall be maintained with the latest vendor supplied security patches that guarantee the IT components are up to date.

Reference	Statements from SAS-SM Standard	Guidelines
	patches installed.	
9.9.5.2.3	System components configuration shall be hardened in accordance with industry best practice.	Hardening configuration shall be demonstrated.
9.9.5.2.4	Change control processes and procedures for all changes to system components shall be in place.	Any change to IT systems shall be subject to a documented change management process with a formal validation process
9.9.5.2.5	Processes and procedures to identify newly discovered security vulnerabilities and to test all system components for security vulnerabilities shall be in place.	Vulnerability scan should be in place in the entire Environment (internal / external) and shall be done on a regular basis (at least on a monthly basis and after any major change). It is important to monitor vendor announcements for news of vulnerabilities and patches related to their products, it is equally important to monitor common industry vulnerability news groups and mailing lists for vulnerabilities and potential workarounds that may not yet be known or resolved by the vendor. Critical vulnerabilities related to any internet facing system components shall be remediated within 7 days, 30 days otherwise.
9.9.5.2.6	Comprehensive virus detection and prevention measures shall be deployed across all systems vulnerable to viruses and other malicious software.	Anti-virus clients should be installed on all vulnerable systems Anti-virus clients should be updated regularly with virus definitions Mechanisms should be in place 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 scanning of data and applications software prior to introduction to the system.
9.9.5.2.7	Unattended terminals shall timeout to prevent unauthorised use and appropriate time limits shall be in place.	Employees having individual accounts shall lock or log out of their terminals when not in attendance. This excludes service accounts. Timeouts should be controlled by the administrator and set to a maximum of 15 minutes. Users should be prevented from changing timeout settings.
9.9.5.3	System back-up	
9.9.5.3.1	Back-up copies of critical business data shall be taken regularly. Back-ups shall be stored appropriately to ensure confidentiality and	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

Reference	Statements from SAS-SM Standard	Guidelines
	availability.	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 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 depending on the customer SLA. Procedures for restoration of data from back-up should be checked periodically (typically once or twice per year).
9.9.6	Software Development	
9.9.6.1	The software development processes for the SM-DP or SM-SR shall follow industry best practices for development of secure systems.	The Auditee shall ensure that the software is protected against the top 10 security flaws described by the OWASP (www.owasp.org).The Auditee shall provide evidence of the security of the software development process. The software development processes shall follow industry best practice, for example, W3C standard (The World Wide Web Consortium (W3C) is an international community that develops open standards to ensure the long-term growth of the Web)
9.9.7	External Facilities Management	
9.9.7.1	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.
9.10 Control, Audit and Monitoring		
9.10.1	General Principals	
9.10.1.1	Controls deployed shall be clearly documented and up-to-date.	A programme of internal audits should be defined that demonstrates appropriate consideration. The Audit Team should have received appropriate training in the structure and content of internal audits.

Reference	Statements from SAS-SM Standard	Guidelines
9.10.1.2	Controls shall be subject to a rigorous programme of internal monitoring, audit and maintenance to ensure their continued correct operation.	The program shall include: • 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 Audit Team will expect to see evidence that processes and systems are working correctly, and that internal audits 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.
9.10.1.3	The controls apply to the different sections 9.6, 9.7 and 9.9.	All elements of the protection should be checked regularly to ensure their correct operation. The frequency of checks should be defined based on the importance and reliability of each security control. The list below is the minimal one (and not exhaustive): • Controls of the keys (usage and storage) • Controls of physical access • Controls on security equipment • Controls of the access to the security area • Controls of firewall and any IDS alert treatment • Controls of efficiency of antivirus and patch management • Controls of users access rights • Controls of data deletion as per the data policies • Controls of administration activities (local or remote)
9.10.2	Audit Trails	
9.10.2.1	The SP shall be logged in an audit trail that provides a complete record of, and individual accountability for:	

Reference	Statements from SAS-SM Standard	Guidelines
9.10.2.1.1	• Profile Management, Platform Management, IT system and eUICC Management procedures;	The minimum information related to the application (Profile Management, Platform Management, and eUICC Management) that have to be logged are: • Initiator of the request • ID of the request • Type of the request • Timestamp of the request • Timestamp for the completion • Profile identifier (if applicable) • eUICC ID (if applicable) • MNO_ID (if applicable) • SM-SR ID (if applicable) • SM-DP ID (if applicable) The minimum information related to the IT system that have to be logged are: • Users login (successful/unsuccessful) • Resource access • Activity description
9.10.2.1.2	• Access to sensitive data;	The minimum information gathered in relation to each access to sensitive data is: • Users login (successful/unsuccessful) • List of sensitive data accessed • Timestamp of the log in and log out Reason for accessing sensitive data shall also be documented.
9.10.2.2	The audit trail shall:	
9.10.2.2.1	• ensure that all assets created, processed and deleted are completely accounted for.	Based on the asset lists, a log should exist for the entire lifecycle of the asset.

Reference	Statements from SAS-SM Standard	Guidelines
9.10.2.2.2	• ensure that the responsible individuals are traceable and can be held accountable.	A log should exist for the entire user access lifecycle.
9.10.2.3	The audit trail shall be protected in terms of integrity and the retention period must be defined. The audit trail shall not contain sensitive data.	Audit trails should not be modified via technical or procedural processes. Retention period guidelines shall be defined with maximum or minimum retention period either in line with the customer SLA or Auditee default policy.
9.11 Incident Response and Reporting		
9.11.1	An escalation process shall be in place where a security breach is revealed on SM-DP and SM-SR process.	An escalation process / mechanism should be in place where security breaches are identified. It is expected that all such security breaches are tracked and reported. When any security breach happens, an incident management process shall be started including impact analysis, setup of remediation plan and notification to external third party impacted.
9.11.2	Reporting procedures shall be in place.	Mechanisms should be in place for employees to make confidential reports of security incidents or suspicions.

Annex A Document Management

A.1 Document History

Version	Date	Brief Description of Change	Editor / Company
1.0	13 October 2014	PSMC approved, first release	Arnaud Danree, Oberthur

A.2 Other Information

Type	Description
Document Owner	SIM Group
Editor / Company	Arnaud Danree, Oberthur

It is our intention to provide a quality product for your use. If you find any errors or omissions, please contact us with your comments. You may notify us at PRD@gsma.com.

Your comments or suggestions & questions are always welcome.