Cloud Deployment of Subscription Management Solutions - Guidance for SAS-SM Auditees

Version 1.0

31 August 2021

Security Classification: Non-Confidential

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

Copyright Notice

Copyright © 2021 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   Introduction

1.1   Overview

The growth and development of subscription management (SM) deployments has led to the use of cloud service providers (CSPs) services for SM solution hosting. In such deployments, both the SM service provider and the CSP need to be SAS-SM certified for the activities within scope of SAS-SM that they are responsible for.

To assist SM service providers and CSPs in preparing for an SAS audit of such deployments, this document provides guidance on what is likely to be in scope for SAS-SM audits of the CSP and of the SM service provider. The final scope of such audits will depend on the activities performed by each auditee type, and shall be agreed between the auditee, the audit team and the GSMA in advance of an audit.

The contents of this document are based on SAS-SM audit team experience in applying the requirements to different auditee activities and environments, and discussions with SM service provider and CSP stakeholders to date.

As the use of CSP for SM deployments grows and develops, the SAS auditors, with the support of the GSMA SAS subgroup will continue to work with the SM service provider and CSP community to enhance these guidelines, and consider incorporating them into the official SAS documentation as needed.

1.2   Scope

The guidance in this document assumes that the CSP is providing data centre operations and management (DCOM) services to the SM service provider. As specified in [4], DCOM does not include management of the SM application or SM application data.

If a CSP is seeking to obtain SAS-SM certification for services that include management of the SM application or SM application data, then it would need to be audited with scope SM-SR, SM-DP, SM-DP+ and/or SM-DS as applicable.

1.3   Abbreviations

Term	Description
CSP	Cloud Service Provider
CSR	Consolidated Security Requirements (i.e. FS.17)
DCOM	Data Centre Operations and Management
HSM	Hardware Security Module
IaaS	Infrastructure as a service
PaaS	Platform as a service
SaaS	Software as a service
SAS	Security Accreditation Scheme
SM	Subscription Management

1.4   References

Ref	Doc Number	Title
[1]	PRD FS.09	GSMA SAS Methodology for Subscription Manager Roles, latest version available at www.gsma.com/sas
[2]	PRD FS.17	GSMA SAS Consolidated Security Requirements, latest version available at www.gsma.com/sas
[3]	PRD FS.18	GSMA SAS Consolidated Security Guidelines, latest version available on request from sas@gsma.com
[4]	SAS-SM Scope Definitions	SAS for Subscription Management (SAS-SM) Scope Definitions https://www.gsma.com/security/wp-content/uploads/2020/07/GSMA-SAS_SM-Scope-Definitions-v1.pdf

2   Responsibilities for Compliance with CSRs

2.1   Defining Responsibilities

For all cloud deployments, it is important for both the SM service provider and CSP in a relationship to understand their own responsibilities, and each other's responsibilities, for compliance with the GSMA SAS Consolidated Security Requirements [2] across the cloud service model. This understanding will help each party to effectively scope, prepare for and undergo their SAS-SM audits and to use their certification, as described in section 3.
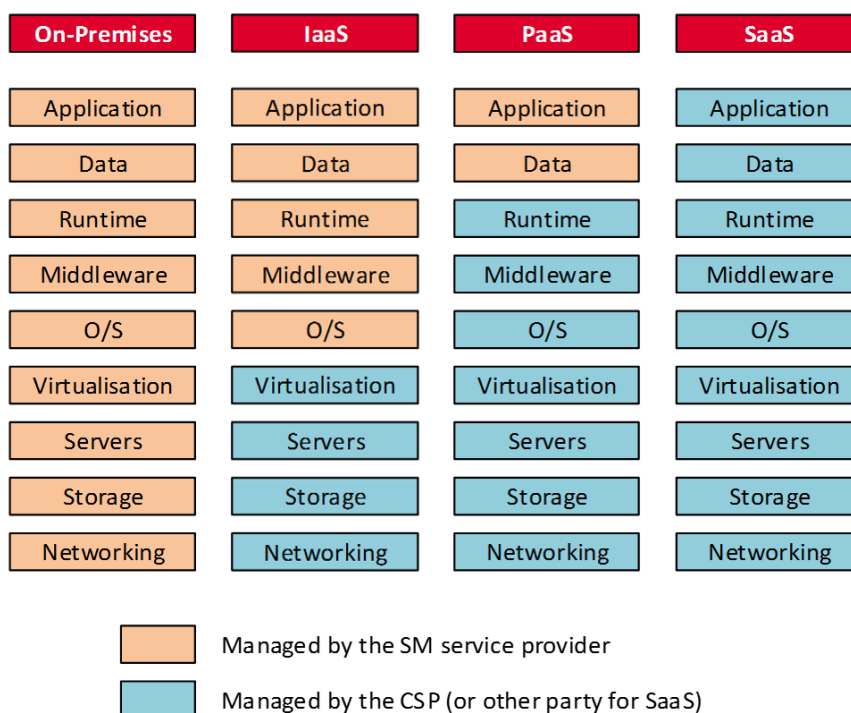

Figure 1: Traditional split of responsibilities for services

Figure 1 shows a typical split of responsibilities for the different types of cloud services with a comparison to a traditional on-premises model. A SM service provider using a CSP for DCOM services would normally use a hybrid of the IaaS or PaaS models. However, the

exact services to be used and the associated division of responsibilities will be agreed between the parties.

3   Scoping the SAS-SM Certification and Audits

3.1   Defining the Scope

The GSMA and SAS-SM auditing companies have provided guidance in section 4 of this document on the sections of the GSMA SAS Consolidated Security Requirements [2] that would normally fall within the scope of SAS-SM audits of:

- a CSP providing DCOM services to an SM service provider, and
- an SM service provider that is hosting its SM solution on a CSP's infrastructure..

The intention of this guidance is to enable a CSP or an SM service provider, together with the SAS auditors, to effectively scope a planned SAS-SM audit.

The CSP services used by the SM service provider, and the division of responsibilities between a CSP and a SM service provider will vary for different parties and deployments, so the audit scope will be agreed between the auditee (CSP or SM service provider), GSMA, and the audit team as part of the audit planning process.

3.1.1   CSPs

3.1.1.1   CSP Options For Certification

There are two options available to CSPs seeking to host SAS-SM certified services, as defined in FS.09 SAS-SM Methodology [1].

1. **Independent CSP SAS-SM Certification:** The CSP can seek its own independent SAS-SM certification (with scope DCOM) to allow multiple SM service providers to use its services (section 11 of FS.09)**Error! Reference source not found.**.
2. **Non-Independent CSP SAS-SM Certification:** The CSP can be included within a SM service provider's certification as a subcontractor (section 10.7 of FS.09).

3.1.1.2   Independent CSP SAS-SM Certification

Where the CSP chooses to pursue independent SAS-SM certification, the audit will be planned to cover:

- Cloud services, including the core infrastructure supporting the cloud services;
- Remote access and management of cloud services operated by CSP staff;
- Data centres.

The applicable sections of FS.17 for this audit type are specified in Table 1 below.

FS.17 Section	Cloud Services	CSP Remote Access	Data Centres
1 – Policy, Strategy, and Documentation	In Scope	In Scope	In Scope
2 – Organisation and Responsibility	In Scope	In Scope	In Scope
3 – Information	In Scope	In Scope	In Scope
4 – Personnel Security	In Scope	In Scope	In Scope
5 – Physical Security	N/A	In Scope	In Scope
6 – Certificate and Key Management	N/A	N/A	N/A
7 – Sensitive Process Data Management	N/A	N/A	N/A
8 – SM-DP, SM-SR, SM-DP+, and SM-DS Service Management	N/A	N/A	N/A
9 – Logistics and Production Management	N/A	N/A	N/A
10 – Computer and Network Management	In Scope	In Scope	In Scope
11 – Two-Step Personalisation Process	N/A	N/A	N/A

Table 1: Overview of CSP Audit Scope

Where CSP policies and procedures are shared (e.g. global) across all services and locations, for remote access and data centres, the audit will review these as part of a centralised audit as described in section 11 of FS.09.

For these audit types, separate audit reports will normally be provided for the following:

- Central policies and cloud services;
- Data centre cloud regions (as necessary).

3.1.1.3   Non-Independent CSP SAS-SM Certification

If a CSP is seeking to be included within the scope of a client SM service provider's certification as a subcontractor, the same control areas under the responsibility of the CSP (as per Table 1 above) will be included as part of the SM service provider's audit, but the scope of auditing of the CSP activities is limited to the services provided by the CSP to that SM service provider client only. The SM service provider is ultimately responsible for compliance with the SAS-SM requirements by its subcontractor (the CSP). The same audit will also cover all in-scope activities performed directly by the SM service provider.

For these audits, a single audit report describing compliance by the SM service provider and its CSP subcontractor will be prepared.

3.1.2   SM Service Providers

There are two options available to SM service providers seeking to use SAS-SM certified cloud hosting services:

1. **Independent CSP SAS-SM Certification:** The SM service provider can deploy its SM application within a CSP cloud region that holds independent SAS-SM certification.
2. **Non-Independent CSP SAS-SM Certification:** The SM service provider can seek SAS-SM auditing and certification with a scope that includes both its own management

of the SM application and cloud hosting services provided to it by the CSP (considered as its subcontractor).

3.1.2.1   Independent CSP SAS-SM Certification

In this scenario, the security controls related to the services and facilities offered by a CSP to SM service providers are subject to independent SAS-SM auditing and certification. Auditing of those security controls (e.g. physical security controls at the CSP site(s) hosting the SM application, logical controls of the CSP service offerings) are therefore excluded from the SM service provider's audit.

The SM service provider's audit shall include assessment of the SM service provider's activities under all relevant sections of FS.17 related to local hosting of sensitive assets and processes (e.g. HSM, key management) and its management of the cloud-hosted SM application.

The applicable sections of FS.17 for this audit type are specified in Table 2, below:

CSR Section	HSM /Key Mgmt. Location	SM Service Provider Management of Cloud Deployment
1 – Policy, Strategy, and Documentation	In Scope	In Scope
2 – Organisation and Responsibility	In Scope	In Scope
3 – Information	In Scope	In Scope
4 – Personnel Security	In Scope	In Scope
5 – Physical Security	In Scope	In Scope
6 – Certificate and Key Management	In Scope	N/A
7 – Sensitive Process Data Management	N/A	In Scope
8 – SM-DP, SM-SR, SM-DP+, and SM-DS Service Management	N/A	In Scope
9 – Logistics and Production Management	N/A	N/A
10 – Computer and Network Management	In Scope	In Scope
11 – Two-Step Personalisation Process	N/A	N/A

Table 2: Overview of SM Service Provider Audit Coverage

For these audits, the SM service provider audit report will cover the in-scope activities performed by the SM service provider only. However, the CSP's SAS-SM certified cloud region will be specified as a supporting site on the audit report and SAS-SM certificate granted to the SM service provider.

3.1.2.2   Non-Independent CSP SAS-SM Certification:

As per section 3.1.1.3.

4   GSMA SAS-SM Scope of Audit & Certification when using Cloud Service Provider

4.1   Key

Term	Description
	Requirement is applicable
	Requirement is not applicable

4.2   Presentation of Information

In some cases below where the same applicability category and/or comment applies to multiple sequential requirements within a section or subsection, the rows have been merged and lower requirement statements have been removed to reduce duplication and improve readability. Unless otherwise indicated, the applicability category and comment apply to all requirement statements of lower depth in the numbering scheme. Refer to FS.17 [2] for the complete contents of the CSR.

4.3   Details

Statements from CSR			SM Provider	Comment	CSP	Comment
1	**Policy, strategy and documentation**					
All	The security policy and strategy provides the business and its employees with a direction and framework to support and guide security decisions within the company and at the location where the SP takes place.					
	1.1	Policy		Applies to the SM environment including local hosting of sensitive assets and processes (e.g. HSM, key management) and the SM provider's		Applies to the CSP's data centre operations and management (DCOM) services and facilities provided by the CSP to one or more SM service providers to host SM applications.
	1.2	Strategy				
	1.3	Business Continuity Planning				

Statements from CSR			SM Provider	Comment	CSP	Comment
	1.4	Internal audit and control		management of the cloud-hosted SM application.		

Statements from CSR			SM Provider	Comment	CSP	Comment
2	**Organisation and responsibility**					
All	A defined organisation shall be responsible for ownership and operation of the security management system.					
	2.1	Organisation		Applies to the SM environment including local hosting of sensitive assets and processes (e.g. HSM, key management) and the SM provider's management of the cloud-hosted SM application.		Applies to the CSP's data centre operations and management (DCOM) services and facilities provided by the CSP to one or more SM service providers to host SM applications.
	2.2	Responsibility				
	2.3	Incident response and reporting				
	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.		Applies to the SM environment including local hosting of sensitive assets and processes (e.g. HSM, key management) and the SM provider's management of the cloud-hosted SM application.		Applies to the CSP's data centre operations and management (DCOM) services and facilities provided by the CSP to one or more SM service providers to host SM applications.
	2.4.2	Where activities within scope of SAS certification are outsourced or sub-contracted, partners providing or operating these services shall be contractually responsible to ensure an appropriate level of compliance with the SAS requirements.				
	(i)	Responsibilities that fall within the scope of the auditee's SAS certification shall be clearly documented and agreed.				
	(ii)	Contracts shall include a "right-to-audit" clause (or equivalent mechanism) to:				

Statements from CSR			SM Provider	Comment	CSP	Comment
		• Enable auditees to confirm that contractual responsibilities and obligations are maintained at the required level by the outsourcing partner / sub-contractor. • Include the right of the auditee to require the outsourcing partner / sub-contractor to participate in the SAS audit process, where applicable.	🟩		🟩	
UP CM	2.4.3	For eUICC production, transfer of class 1 assets between sites must enforce integrity of SAS-UP certification throughout the production chain.	🟨	Not applicable to SAS-SM.	🟨	Not applicable to SAS-SM.

Statements from CSR			SM Provider	Comment	CSP	Comment
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	🟩	Applies to the SM environment including local hosting of sensitive assets and processes (e.g. HSM, key management) and the SM provider's management of the cloud-hosted SM application.	🟩	Applies to the CSP's data centre operations and management (DCOM) services and facilities provided by the CSP to one or more SM service providers to host SM applications.
	3.2	Data and media handling	🟩		🟩	

Statements from CSR			SM Provider	Comment	CSP	Comment
4	**Personnel security**					
All	A number of security requirements shall pertain to all personnel working within the SP and those with trusted positions.					
	4.1	Security in job description	🟩	Applies to the SM environment including local hosting of sensitive assets and processes (e.g. HSM, key management) and the SM provider's management of the cloud-hosted SM application.	🟩	Applies to the CSP's data centre operations and management (DCOM) services and facilities provided by the CSP to one or more SM service providers to host SM applications.
	4.2	Recruitment screening	🟩		🟩	
	4.3	Acceptance of security rules	🟩		🟩	
	4.4	Incident response and reporting	🟩		🟩	
	4.5	Contract termination	🟩		🟩	

Statements from CSR			SM Provider	Comment	CSP	Comment
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	🟩	Applies to the SM environment including local hosting of sensitive assets and processes (e.g. HSM, key management) and the SM provider's management of the cloud-hosted SM application. Physical security of remote access endpoints will be considered as may be required under FS.17 section 10.4.	🟩	Applies to data centres within the cloud region seeking certification.
	5.2	Physical protection	🟩		🟩	
	5.3	Access control	🟩		🟩	
	5.4	Security staff				
	5.4.1	Security staff are commonly employed by suppliers. Where this is the case the duties shall	🟩	Applies when physical security staff are employed by SM service provider as a security control for local hosting of	🟩	Applies to the security staff (in-house or outsourced / sub-

Statements from CSR			SM Provider	Comment	CSP	Comment
		be clearly documented and the necessary tools and training shall be supplied.		sensitive assets and processes (e.g. HSM, key management, and remote access locations).		contracted) deployed at data centres.
	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.		Applies to the SM environment including local hosting of sensitive assets and processes (e.g. HSM, key management) and the SM provider's management of the cloud-hosted SM application. Physical security of remote access endpoints will be considered as may be required under FS.17 section 10.4.		Applies to data centres within the cloud region seeking certification.

Statements from CSR			SM Provider	Comment	CSP	Comment
6	**Certificate and key management**					
UP SM CM I	Technical and procedural controls shall be applied to cryptographic keys and certificates related to the SP at the site. Applicable requirements will vary according to the level of SP. Specific requirements applying to Root CA(s) are highlighted where applicable.					
	6.1	Classification	🟩	Applies to the SM environment including local hosting of sensitive assets and processes (e.g. HSM, key management) and the SM provider's management of the cloud-hosted SM application.	🟧	Not applicable to CSP
	6.2	Roles and responsibilities	🟩		🟧	
	6.3	Cryptographic key specification	🟩		🟧	
	6.4	Cryptographic key management	🟩		🟧	
	6.5	Auditability and accountability	🟩		🟧	
CM SM	6.6	GSMA Public Key Infrastructure (PKI) Certificates				
	6.6.1	Supplier certificates used as part of any GSMA PKI shall be signed by a CA authorized by and acting on behalf of the GSMA	🟩	Applies to the SM environment including local hosting of sensitive assets and processes (e.g. HSM, key management) and the SM provider's	🟧	Not applicable to CSP
	6.6.2	PKI certificate private keys shall only ever be installed and used for signing at sites:	🟩		🟧	

Statements from CSR			SM Provider	Comment	CSP	Comment
	(i)	That are agreed with the GSMA.		management of the cloud-hosted SM application.		
	(ii)	That are SAS certified with the appropriate scope.				
	(iii)	In accordance with the certificate policy.				
6.6.3		PKI certificate key pairs shall only ever be transferred and installed to a different operational site:				
	(i)	With the prior agreement of the GSMA.				
	(ii)	Where the new operational site is SAS certified with the appropriate scope.				
	(iii)	In accordance with the certificate policy.				
	(iv)	By a mechanism that ensures an appropriate level of security for the transfer of the sensitive assets.				
6.6.4		Where auditees make use of the same PKI certificate private key at multiple sites, in addition to the requirements of 6.6.2 and 6.6.3:				
	(i)	A single, nominated, site within the auditee organization shall be responsible for control and issue of the certificate key pair.				
	(ii)	All transfer of certificate private keys shall originate from the nominated site.				
	(iii)	Controls shall be in place to prevent certificate private keys being transferred except under the control of the nominated site.				

Statements from CSR			SM Provider	Comment	CSP	Comment
	(iv)	All transfer of certificate private keys shall be recorded and auditable.	🟩		🟧	
UP	6.6.5	Where auditees make use of the same EUM PKI certificate private key at multiple sites, in addition to the requirements of 6.6.4:	🟧	Not applicable to SAS-SM.	🟧	Not applicable to SAS-SM.
	(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			SM Provider	Comment	CSP	Comment
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	🟩	Applies to the SM environment including local hosting of sensitive assets and processes (e.g. HSM, key management) and the SM provider's management of the cloud-hosted SM application.	🟨	Not applicable to CSP.
	7.2	Sensitive data access, storage and retention	🟩		🟨	
UP	7.3	Data generation	🟨	Not applicable to SAS-SM.	🟨	Not applicable to SAS-SM.
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:	🟩	Applies to the SM environment including local hosting of sensitive assets and processes (e.g. HSM, key management) and the SM	🟨	Not applicable to CSP.
	(i)	all assets created, processed and deleted are completely accounted for				

Statements from CSR			SM Provider	Comment	CSP	Comment
	(ii)	access to sensitive data is auditable	🟩	provider's management of the cloud-hosted SM application.	🟨	
	(iii)	responsible individuals are traceable and can be held accountable				
	7.4.2	The audit trail shall be protected in terms of integrity and the retention period must be defined. The audit trail shall not contain sensitive data.	🟩		🟨	
	7.4.3	Auditable dual-control and 4-eyes principle shall be applied to sensitive steps of data processing.	🟩		🟨	
UP	7.4.4	For UICC production the audit trail shall include:	🟨	Not applicable to SAS-SM.	🟨	Not applicable to SAS-SM.
	(i)	data generation and processing				
	(ii)	personalisation				
	(iii)	re-personalisation				
	(iv)	access to sensitive data				
	(v)	Production of customer output files				
	7.5	Duplicate production	🟩	Applies to the SM environment including local hosting of sensitive assets and processes (e.g. HSM, key management) and the SM provider's management of the cloud-hosted SM application.	🟨	Not applicable to CSP.
UP SM	7.6	Data integrity	🟩		🟨	
	7.7	Internal audit and control	🟩		🟨	

Statements from CSR			SM Provider	Comment	CSP	Comment
8		**SM-DP, SM-SR, SM-DP+ and SM-DS Service Management**				
SM	8.1	SM-DP, SM-SR, SM-DP+ and SM-SR Service		Applies to the SM environment including local hosting of sensitive assets and processes (e.g. HSM, key management) and the SM provider's management of the cloud-hosted SM application.		Not applicable to CSP.
	8.2	Remote Entity Authentication				
	8.3	Audit trails				

Statements from CSR				
9	**Logistics and production management**	🟧	Not applicable to SAS-SM.	🟧 Not applicable to SAS-SM.

Statements from CSR			SM Provider	Comment	CSP	Comment
10	**Computer and network management**					
All	The secure operation of computer and network facilities is paramount to the security of data. In particular, the processing, storage and transfer of Class 1 information, which if compromised, could have serious consequences, must be considered. Operation of computer systems and networks must ensure that comprehensive mechanisms are in place to preserve the confidentiality, integrity and availability of data.					
	10.1	Policy	■	Applies to the SM environment including local hosting of sensitive assets and processes (e.g. HSM, key management) and the SM provider's management of the cloud-hosted SM application.	■	Applies to the CSP's data centre operations and management (DCOM) services and facilities provided by the CSP to one or more SM service providers to host SM applications.
	10.2	Segregation of roles and responsibilities	■		■	
	10.3	Access control				
	10.3.1	Physical access to sensitive computer facilities shall be controlled.	■	Applies to the SM environment including local hosting of sensitive assets and processes (e.g. HSM, key management) and the SM provider's management of the cloud-hosted SM application. Physical security of remote access endpoints will be considered as may be required under FS.17 section 10.4.	■	Applies to data centres within the cloud region seeking certification.

Statements from CSR			SM Provider	Comment	CSP	Comment
	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.		Applies to the SM environment including local hosting of sensitive assets and processes (e.g. HSM, key management) and the SM provider's management of the cloud-hosted SM application.		Applies to the CSP's data centre operations and management (DCOM) services and facilities provided by the CSP to one or more SM service providers to host SM applications.
	10.3.3	Passwords shall be used and managed effectively.				
	10.4	Remote Access Remote access for a user to connect to a network, system or service from a location other than as part of the certified secure area(s) at the site shall only be permitted in accordance with the requirements of 10.4. Remote access requirements shall be applied to any environment containing assets (networks, systems or information) within the scope of SAS certification. The remote access requirements describe connection from a remote **endpoint** via a secure **channel** to the **target** environment.		Applies to the controls over remote access to the cloud-hosted SM application.		Applies to the controls over remote access to core services and infrastructure.
	10.5	Network security		Applies to the SM environment including local hosting of sensitive assets and processes (e.g. HSM, key management) and the SM provider's		Applies to the service offerings and core infrastructure provided by the CSP to one or more SM service providers to host SM applications.
	10.6	Systems security				
	10.7	Audit and monitoring				

Statements from CSR			SM Provider	Comment	CSP	Comment
	10.8	External facilities management	🟩	management of the cloud-hosted SM application.	🟩	
	10.9	Internal audit and control	🟩		🟩	
SM	10.10	Software Development	🟩		🟩	
	10.10.1	The software development processes for the SM-DP, SM-SR, SM-DP+ or SM-DS shall follow industry best practices for development of secure systems.	🟩	Applies to the SM environment including local hosting of sensitive assets and processes (e.g. HSM, key management) and the SM provider's management of the cloud-hosted SM application.	🟧	Not applicable to CSP.
DC	10.10.2	The software development processes for applications and bespoke software deployed within the SM environment shall follow industry best practices for development of secure systems.	🟩		🟩	Applies to the service offerings and core infrastructure provided by the CSP to one or more SM service providers to host SM applications.
DC	10.11	Multi-Tenancy Environments				
	10.11.1	Multi-tenant solutions must prevent cross-contamination of assets between different customers.	🟧	Not applicable to SM service provider deploying SM application in cloud environment	🟩	Applies to the service offerings and core infrastructure provided by the CSP to one or more SM service providers to host SM applications.
	10.11.2	Multi-tenant solutions on the same physical hardware shall ensure customer data is logically segregated between different customers.	🟧		🟩	
	10.11.3	Each customer running their own applications must use a unique ID for that customer for the running of these application processes	🟧		🟩	

Statements from CSR			SM Provider	Comment	CSP	Comment
	10.11.4	Restrictions shall be put in place for all customers on shared infrastructure by restricting use of shared system resources.				
DC SM	10.11.5	The auditee shall ensure that customer data is only stored within SAS certified physical locations, including any Sites where data may be replicated to as part of business continuity plans, meeting all requirements detailed in section 5 of this document.		Applies to the SM environment including local hosting of sensitive assets and processes (e.g. HSM, key management) and the SM provider's management of the cloud-hosted SM application.		

Statements from CSR		
11 Two-step personalisation process	Not applicable to SAS-SM.	Not applicable to SAS-SM.

Annex A   Document History

A.1   Document History

Version	Date	Brief Description of Change	Editor / Company
1.0	31/08/2021	First version	Neil Shepherd, SRC GmbH Andrew Hutchins, NCC Group David Maxwell, GSMA