



# **GSMA SAS Methodology for Subscription Manager Roles**

## **Version 5.0**

### **25 July 2019**

*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 © 2019 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

<b>1</b>	<b>Introduction</b>	<b>4</b>
1.1	Overview	4
1.2	Scope	4
1.3	Definitions	4
1.4	Abbreviations	5
1.5	References	5
<b>2</b>	<b>Audit Process</b>	<b>6</b>
2.1	Audit Setup	6
2.1.1	Audit Request	6
2.1.2	Confirmation of Audit Date	7
2.1.3	Contract	7
2.2	Audit Preparation (Off-Site)	7
2.2.1	Audit Agenda	7
2.2.2	Audit pre-requisites	7
2.3	Audit Process (On-Site)	7
2.3.1	Presentation and Documentation for the Audit Team	7
2.3.2	Audit Performance	8
2.3.3	Audit Report	8
2.3.4	Presentation of Results	8
2.4	Following the Audit	8
2.5	Appeals	8
2.6	Notification and Publication of Certification	9
2.7	Language	9
<b>3</b>	<b>Provisional certification</b>	<b>10</b>
3.1	Provisional certification process	10
3.2	Provisional certification period	10
3.3	Duration of provisional certification	11
3.4	Duration of Provisional Certification Audits	11
<b>4</b>	<b>Certification Renewal</b>	<b>11</b>
4.1	Certification Renewal Process	11
4.2	Certification Period	12
4.3	Duration of Certification	13
<b>5</b>	<b>SAS-SM Participants</b>	<b>13</b>
5.1	Auditee	14
5.2	Audit team	14
5.2.1	Observing Auditor	14
5.3	SAS subgroup	15
5.4	Audit Management	16
5.5	Participant Relationships	16
<b>6</b>	<b>Audit Report Scoring and Assessment</b>	<b>16</b>
6.1	Audit Result	17
<b>7</b>	<b>Maintaining SAS Compliance</b>	<b>18</b>

7.1	Examples of notifiable events	18
7.1.1	What should be notified	18
7.1.2	What would not normally require notification:	19
<b>8</b>	<b>Costs</b>	<b>19</b>
8.1	First Dry Audit or Renewal Audit	19
8.2	Audit of sites with limited scope	19
8.3	Audit of Central / Corporate Functions	20
8.4	Repeat Audit	20
8.5	Off-Site Review of Improvements	20
8.6	Scope Extension Audits	21
8.7	Cancellation Policy	21
8.8	Appeals	21
<b>9</b>	<b>Final Report</b>	<b>22</b>
<b>10</b>	<b>Auditing and Certification of Supporting Sites</b>	<b>22</b>
10.1	Definition	22
10.2	Auditing and Certification Approach	22
10.3	Data Centres hosting SM solutions	22
10.4	SM Backup Sites	23
10.5	Centralised or Outsourced IT Services	24
10.6	SM Remote Administrative Access Sites	25
10.7	Cloud Service Providers (CSP)	26
10.8	Audit Reports	27
10.9	SAS Certificates	27
<b>Annex A</b>	<b>Final Audit Report Structure</b>	<b>28</b>
A.1	First Page:	28
A.2	Subsequent Pages:	28
<b>Annex B</b>	<b>Standard Audit Agenda</b>	<b>31</b>
<b>Annex C</b>	<b>Standard Document List</b>	<b>34</b>
C.1	Document List	34
<b>Annex D</b>	<b>Subscription Management Processing Audit</b>	<b>35</b>
D.1	Before the Audit	36
D.1.1	Preparation	36
D.1.2	Certificate Enrolment	36
D.1.3	Further Preparation for Audit (SM-SR)	36
D.1.4	During the Audit (SM-SR)	37
D.1.5	Further Preparation for Audit (SM-DP)	38
D.1.6	During the Audit (SM-DP)	39
D.1.7	Further Preparation for Audit (SM-DP+)	39
D.1.8	During the Audit (SM-DP+)	40
D.1.9	During the Audit (SM-DS)	41
D.2	After the Audit	41
<b>Annex E</b>	<b>Scope of Audit &amp; Certification when using Cloud Service Provider</b>	<b>42</b>
E.1	Document History	43
E.2	Other Information	43

# 1 Introduction

## 1.1 Overview

The GSMA Security Accreditation Scheme for Subscription Management Roles (SAS-SM) is a scheme through which Subscription Manager – Secure Routing (SM-SR), Subscription Manager – Data Preparation (SM-DP), Subscription Manager – Data Preparation+ (SM-DP+) and Subscription Manager – Discovery Server (SM-DS) solution providers subject their operational sites to a comprehensive security audit. The purpose of the audit is to ensure that these entities have implemented adequate security measures to protect the interests of mobile network operators (MNO).

Audits are conducted by specialist auditing companies over a number of days, typically in a single site visit. The auditors will check compliance against the GSMA SAS Standard for Subscription Manager Roles [1] and its supporting documents ([2], [3]) by various methods such as document review, interviews and tests in specific areas.

Subscription Management entities that are found to be compliant with the requirements in the SAS-SM Standard are certified by the GSMA. This document describes the SAS-SM methodology and processes.

## 1.2 Scope

This scope of this document covers:

- SAS-SM participating stakeholders and their roles
- Processes for arrangement and conduct of SAS-SM audit
- Audit scoring and report structure
- Certification and provisional certification processes
- SAS-SM costs

## 1.3 Definitions

Term	Description
Audit management	A GSMA team which: <ul style="list-style-type: none"> <li>• Administers SAS-UP</li> <li>• Appoints the auditor companies</li> <li>• Monitors and assures the quality and consistency of the audit process and audit team</li> <li>• Issues certificates to those sites that the audit team assesses as compliant with the requirements.</li> </ul>
Appeals Board	Two auditors, one each from different GSMA selected auditing companies who consider and rule on appealed audit results.. Auditors for the SAS-UP appeals board will be drawn from the SAS-SM audit companies and vice versa.separate from the auditing companies that performed the audit that may be the subject of an appeal, who consider and rule on appealed audit results.
Audit team	Two auditors, one each from different GSMA-selected auditing companies, jointly carrying out the audit on behalf of the GSMA.

Term	Description
Auditee	The site that is the subject of the audit.
Auditing Company	Company appointed by the GSMA that provides Auditors.
Auditor	A person qualified to perform audits
eUICC	A UICC which is not easily accessible or replaceable, is not intended to be removed or replaced in a device, and enables the secure changing of profiles. Note: The term originates from "embedded UICC".
SAS subgroup	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 Consolidated Security Guidelines;

See section 4 for more detailed explanations of each role.

## 1.4 Abbreviations

Term	Description
CSG	Consolidated Security Guidelines
CSR	Consolidated Security Requirements
eUICC	Embedded UICC
EUM	Embedded UICC Manufacturer
FS.nn	Prefix identifier for official documents belonging to GSMA Fraud and Security Group
GSMA	GSM Association
MNO	Mobile Network Operator
PKI	Public Key Infrastructure
PRD	Permanent Reference Document
RSP	Remote SIM Provisioning
SAS-SM	Security Accreditation Scheme for Subscription Management Roles
SAS-UP	Security Accreditation Scheme for UICC Production
SGP.nn	Prefix identifier for official documents belonging to GSMA SIM Group
SM-DP	Subscription Manager – Data Preparation
SM-DP+	Subscription Manager – Data Preparation (Enhanced compared to the SM-DP)
SM-DS	Subscription Manager – Discovery Service
SM-SR	Subscription Manager – Secure Routing
SP	Sensitive Process
UICC	Universal Integrated Circuit Card (e.g. a SIM card)

## 1.5 References

Ref	Doc Number	Title
[1]	PRD FS.08	GSMA SAS Standard for Subscription Manager Roles

Ref	Doc Number	Title
[2]	PRD FS.17	GSMA SAS Consolidated Security Requirements, latest version available at <a href="http://www.gsma.com/sas">www.gsma.com/sas</a>
[3]	PRD FS.18	GSMA SAS Consolidated Security Guidelines, available to participating sites from <a href="mailto:sas@gsma.com">sas@gsma.com</a>
[4]	N/A	GSMA SAS-SM Standard Agreement (available from <a href="mailto:sas@gsma.com">sas@gsma.com</a> )

## 2 Audit Process

The audit process is described below.

### 2.1 Audit Setup

#### 2.1.1 Audit Request

If a SM-SR, SM-DP, SM-DP+ or SM-DS provider (auditee) wants to be audited it must make a request to the audit management (GSMA) by completing and submitting an SAS application form. The auditee shall specify on the application form the scope of activities being performed for which certification is being requested.

**NOTE:** It is possible for an auditee to be audited for a subset of subscription management activities (e.g. data centre operations and management in the case of a cloud service provider). The scope of certification should be agreed with the audit management and audit team in advance (see Annex E for details). The agreed scope will be specified in the audit report and on the SAS-SM certificate. See sections 8.2 and 8.3 for associated cost considerations.

The auditee shall also specify the location of the site to be audited (or multiple site locations if processes are distributed across multiple sites). On receipt of the request the audit management will log the details.

First SAS-SM audits of SM-SR, SM-DP, SM-DP+ and SM-DS services are always dry audits leading to provisional certification – see section 3 for details.

Audit applications should be submitted to GSMA several months in advance to increase the likelihood of the SAS audit teams being available to conduct an audit on or near the dates requested by the auditee. As a guide:

<b>If SAS audit application is submitted ...</b>	3 months before requested audit dates,	<b>then GSMA will try to schedule audit within ...</b>	4 weeks of requested dates
	2 months before requested audit dates		6 weeks of requested dates
	1 month before requested audit dates		8 weeks of requested dates

**Table 1 - Audit Scheduling Guidance**

It is the responsibility of the auditee to ensure that certification is in place to satisfy the requirements of any specific contract, customer or bid.

### **2.1.2 Confirmation of Audit Date**

After logging the details of the audit request, the information is sent to the audit team. The audit team will contact the auditee to agree audit dates.

### **2.1.3 Contract**

The auditee enters into a standard agreement [4] with GSMA and pays GSMA in advance for the audit.

## **2.2 Audit Preparation (Off-Site)**

After audit dates have been agreed the audit team and auditee will liaise to agree arrangements for the audit.

### **2.2.1 Audit Agenda**

A provisional agenda will normally be agreed one week before the audit team travel to the site to be audited. The agenda should include guidance for auditees on information that should be prepared for each element of the audit. A sample agenda is included in Annex B.

Changes to the agenda may need to be made during the audit itself as agreed between the audit team and auditee.

### **2.2.2 Audit pre-requisites**

To assist in the auditing of processes and systems the audit team will make arrangements with the auditee to prepare a eUICC and mobile network operator (MNO) data to be used during the audit. The following options may be considered:

1. Use an existing eUICC and MNO data
2. Contract with a temporary eUICC and MNO data
3. Use a test tool (permitted for first dry audit and any associated re-audit(s) only) to simulate, eUICC, EUM and MNO

The auditee is expected to prepare their systems to enable subscription management functionality within the scope of the audit.

The audit team will liaise with the auditee to ensure that pre-requisites are in place.

A more detailed guide to this process for auditees is included in Annex D.

## **2.3 Audit Process (On-Site)**

### **2.3.1 Presentation and Documentation for the Audit Team**

On the first day of the audit the auditee presents to the audit team the information and documentation specified in the audit agenda. A list of the required documentation is included in Annex C. Documentation must be available to the audit team in English.

Having reviewed the documentation the audit team identifies the individuals to be interviewed during the audit. It is the responsibility of the auditee to ensure the availability of these individuals.

### **2.3.2 Audit Performance**

The audit team assesses performance according to the agreed agenda, by various methods such as:

- Document review,
- Interviewing the key individuals
- Testing in the key areas based on a review of sample evidence of compliance.

### **2.3.3 Audit Report**

The audit team summarises the results in a report which is structured as follows:

- Audit summary and overall assessment
- Actions required
- Auditors' comments
- Scope of certification
- Detailed results

Detailed results are given in an annex in the audit report.

The audit report is completed during the audit.

The audit report is restricted to the auditors, auditee and the audit management, save for the auditee's right to release a copy to its customers. In case of an appeal (see below), the audit report will also be provided to the Appeals Board.

### **2.3.4 Presentation of Results**

The final half day of the audit is used to finalise the audit report. The audit team will present the audit results to the auditee focussing on the key points identified in the audit report. It is not deemed necessary to have a slide presentation.

The audit results include the audit team's decision on certification of the site, which is passed to the audit management.

## **2.4 Following the Audit**

The audit management checks the report to confirm that the audit has been carried out in accordance with this Methodology document and that the report meets GSMA quality requirements.

In the event of a successful audit the audit management issues a certificate to the auditee within fifteen (15) business days of completion of the audit.

## **2.5 Appeals**

In the event that the certification decision and/or duration of certification are disputed, the auditee may lodge a submission with the audit management within twenty (20) business

days of completion of the audit. The audit management will refer the appeal to the Appeals Board.

The Appeals Board is comprised of two auditors, one each from different GSMA selected auditing companies and separate from the auditing companies that performed the audit that is the subject of the appeal. For SAS-SM, the Appeals Board is comprised of representatives of the SAS-UP auditing companies, and vice versa. The individual auditors from each auditing company that serve on the Appeals Board may be assigned by those auditing companies from a pool of suitably experienced auditors pre-approved by GSMA, and may change per appeal.

The Appeals Board will consider and rule on appealed audit results. The process to be followed by the Appeals Board will include:

- Review of the audit report, focussing on the appealed assessment(s)
- Discussion with the audit team and the auditee

The Appeals Board should not need to visit the auditee site.

The auditee may request the members of the Appeals Board to sign an NDA prior to receiving a copy of the audit report and other information about the site.

The Appeals Board will seek to rule on appeals within twenty (20) business days of lodgement of the appeal, subject to the availability of the audit team and the auditee and the prompt provision of any information requested from either party.

The auditee and the audit team agree to accept the decision of the Appeals Board as final.

See section 7 for a description of costs associated with the appeals process.

## **2.6 Notification and Publication of Certification**

The GSMA will list certified and provisionally certified production sites on the [SAS website](#), with an explanation of provisional certification.

It is anticipated that interested parties may ask the GSMA to explicitly confirm certification/provisional certification status of sites and the GSMA is willing to support and respond to such requests.

## **2.7 Language**

The language used in the course of the audit for all SAS documentation and presentations is English.

The documents described in Annex C, or their equivalents, should be available to the auditors in English.

Other documents may be in a language other than English but translation facilities should be available during the conduct of the audit.

Where it is difficult to conduct audit discussions with key personnel in English, auditees should arrange for one or more translators to be available to the audit team.

### 3 Provisional certification

Auditee sites seeking SAS-SM certification for this first time for a SM service must undergo a two-stage certification process for that SM service. This is required in order to satisfy the remote SIM provisioning (RSP) compliance process and gain eligibility to receive GSMA public key infrastructure (PKI) certificates. This certification process will initially lead to provisional certification, and later lead to full certification.

#### 3.1 Provisional certification process

The provisional certification process requires two audits to be conducted at the site.

The first, referred to as a 'dry audit', takes place before live subscription management services using GSMA PKI certificates and live customer data commence at the site. For a 'dry audit' to take place, the site must have a complete set of operational systems, processes and controls in place in all areas of the SAS-SM standard. The site should be in a position to begin subscription management services for a customer immediately when a GSMA PKI certificate and a customer order is received. See Annex D for more details.

If the site demonstrates compliance with the Standard [1] provisional certification is granted that remains valid for a period of nine months. A non-compliant result at a 'dry audit' requires the auditee to remedy identified non-compliances within three months. Successful provisional certification will be valid from the date of the repeat 'dry audit'.

A follow up 'wet audit' is required to upgrade the provisional certification to full certification. This audit can only be undertaken if the site has been in continuous live production using GSMA PKI certificates for a minimum period of four to six weeks and it must be undertaken within nine months of the successful 'dry audit'.

Successful completion of a 'wet audit' leads to full certification. The period of full certification runs from the date of the successful 'dry audit'. Provisional certification will be withdrawn if:

- The 'wet audit' is not conducted within nine months of the successful 'dry audit'
- The 'wet audit' result is non-compliant, and a successful repeat audit is not completed within three months
- Live auditee services for a continuous period of four to six weeks cannot be demonstrated within nine months of the successful 'dry audit'
- The auditee chooses to withdraw from the certification process

#### 3.2 Provisional certification period

The nine month provisional certification period begins when the site is first certified..

**NOTE:** The provisional certification period extends from the date of the successful 'dry audit' regardless of whether it is a first or repeat 'dry audit'. This differs from the normal certification process, which backdates certification to the first audit. An exception is made in the case of provisional certification because the three month period to make any improvements necessary after a first 'dry audit' would reduce the window of opportunity within the nine month provisional certification period to ramp-up subscription management services.

The provisional certification period ends at the date specified on the site's SAS-SM provisional certificate or when the site is fully certified following the successful completion of a 'wet audit'.

### **3.3 Duration of provisional certification**

The duration of provisional certification is fixed at nine months. It is the responsibility of the auditee to ensure the 'wet audit' necessary to achieve full certification is undertaken within the nine month period of provisional certification.

If a provisionally-certified site receives a non-compliant result at a 'wet audit', its provisional certification will not be withdrawn immediately and it will retain its provisional certification status until the end of the nine month provisional certification period.

Full certification will normally run for one year, in accordance with the provisions set out in section 4.3, and this will be back dated to the date on which the first 'wet audit' was concluded. If the wet audit extends the scope of existing full certification for a site, and there is significant overlap in controls between the existing and new scope elements, the audit team may extend the full certification expiry date for the new scope element to match the expiry date of the existing certification (if later).

### **3.4 Duration of Provisional Certification Audits**

The first 'dry audit' is conducted over the same period as a full audit and all controls will be audited. Auditee processes will also be examined but in the absence of live processes, the audit team will sample test controls. The duration of a repeat 'dry audit' will depend on the areas to be repeat audited to be agreed with the auditee in accordance with section 8.4 below.

The 'wet audit' is normally conducted over a two day period to review the controls in operation. If the wet audit is conducted together with a renewal audit for other fully certified scope elements, some time savings on the total audit duration may be possible.

## **4 Certification Renewal**

The certification renewal process is applicable to sites holding full SAS-SM certification as is described below.

### **4.1 Certification Renewal Process**

The full certification renewal process begins with the conduct of a renewal audit at a site.

The certification renewal process ends when:

- A new certificate is issued based on the decision of the audit team.
- or
- The site withdraws from the certification renewal process by either:

Indicating that it does not intend to continue with the certification renewal process

or

Not complying with the audit team’s requirements for continuing with the certification renewal process following a non-compliant audit result. (Typically, the audit team requires the site to arrange a repeat audit or to provide evidence of improvement).

The certification renewal process can begin up to 3 months before the expiry of the current certificate.

## 4.2 Certification Period

The certification period begins when a certificate is issued based on the decision of the audit team.

The certification period ends at the date specified on the site’s SAS Certificate of compliance.

The certification period will be determined by the audit team based on the following criteria:

- If the certification renewal process begins up to 3 months before the expiry of the existing certificate

and

the certification is awarded before the expiry of the existing certificate

then

the certification Period will begin at the expiry of the existing certificate

In all other cases the certification period will begin at the time that the certificate is issued.



**Figure 1 - Certification Renewal**

Under the terms of their contract with the GSMA, all sites must be aware of their obligations relating to notification of significant changes at certified sites within the certification period. See section 7 for more details.

### 4.3 Duration of Certification

The duration of certification is determined by the audit team.

The standard duration of certification for sites gaining full certification for the first time is one year.

The standard duration of certification of sites renewing full certification is two years. This duration will be applied in most cases.

The audit team may, at its discretion, decide that certification should be for a shorter duration, for reasons including:

- Significant planned changes at the site related to security-critical processes or facilities
- Significant reliance on recently introduced processes or systems where there is little or no history of successful operation of similar or equivalent controls
- Repeated failure to maintain security controls at an appropriate level for the full certification period (as evidenced by significant failure to meet the standard [1] at a renewal audit).

The audit team may also, at its discretion, decide that certification should be for two years for sites that perform exceptionally well at their dry and wet audits.

The audit management will review decisions made on exceptional circumstances as part of its control of scheme quality and consistency.

Sites gaining full certification for the first time following one or more repeat wet audits shall, in all cases, be granted certification for a minimum of seven months from the month during which a certificate is issued. This allowance reduces the likelihood that the next renewal audit at the site resulting in 2-year certification is influenced by the most recent wet re-audit rather than being an assessment of steady-state controls in operation at the site.

The SAS-SM Methodology does not normally allow the GSMA to extend a site's period of certification. Sites with an existing certificate that are planning or making major changes in advance of a renewal audit, which could affect the ability to demonstrate the necessary period of evidence, are encouraged to contact the GSMA as early as possible. On an exceptional basis, the GSMA may allow a short extension to the existing certificate to accommodate the change process, ensuring that there is sufficient evidence of controls/operations available in their final form prior to the renewal audit. In such cases, the subsequent certificate would be issued to the original renewal date; no advantage will be gained, beyond the site's ability to schedule the SAS renewal audit effectively around the site changes.

## 5 SAS-SM Participants

The following section describes the roles of the participants during the standard audit process. The role of the Appeals Board is not considered here (see section 2.5 for details instead).

## 5.1 Auditee

The auditee is the site that is the subject of the audit. The auditee is responsible for supplying all necessary information at the beginning of the audit. The auditee must ensure that all key individuals are present when required. At the beginning of the audit the auditee makes a short presentation describing how it believes that it is compliant with the Standard [1] and the relevant documentation is made available to the audit team.

The auditee is responsible to disclose to the audit team all areas of the site where assets related to sensitive processes may be created, stored or processed. The auditee may be required by the audit team to demonstrate that other areas of the site are not being used to create, store or process relevant assets, and should honour any reasonable request to validate this.

## 5.2 Audit team

The audit team consists of two independent auditors, one from each of the auditing companies selected by GSMA following a competitive tender for the supply of SAS auditing services and in accordance with selection criteria defined by the GSMA. The audit team conducts the audit by reviewing documentation, conducting interviews with key individuals and carrying out tests in specific areas. After the audit is conducted, the audit team writes a report (see 2.3.3).

The independence of the audit team is of paramount importance to the integrity of SAS-SM. It is recognised that the chosen audit companies are professional in the conduct of their business. Where the audit companies previously supplied consultancy services to an auditee, the audit management should be informed of this fact prior to commencement of the audit, and the auditors performing the audit should be different individuals to those who have provided the consultancy services.

### 5.2.1 Observing Auditor

On some audits, an additional observing SAS auditor may accompany the audit team, in order to:

- Support the development of a common understanding of audit schemes between the audit companies
- Ensure consistency in standards and the audit process
- Facilitate sharing of best practice in the audit approach

Audit observation will be carried out at no additional cost to the auditee, and subject to the following guidelines:

- A maximum of one observer will be present on any one audit, except by the prior agreement with the auditee. Auditees will be under no obligation to agree to any requests for participation of more than one observer.
- The observer will comply with all requirements of the auditee:
  - Prior to the audit (e.g. signing NDAs, providing personal information for visitor authorisation).
  - On-site (e.g. behaviour and supervision).

- The role of the observer is observe. The observation process should not interfere with the conduct of the audit. Specifically, the observing auditor:
  - Should not normally engage directly with the auditee during the audit process to ask audit questions.
  - Should only engage in discussion with the auditee about the observer's own SAS scheme when such discussion will not interfere with the audit process.
  - Should not present or participate in any discussions during the closing meeting.
  - Should not contribute to the preparation of the audit report.

To maximise the benefits of the observation process the observer and audit team are expected to discuss elements of the audit process and approach. Such discussions:

- Should only take place outside of the audit process, and not in the presence of the auditee.
- Should include an opportunity for the observer to read the audit report.
- May include a post-audit discussion, either on- or off-site to discuss any questions or observations. The post-audit discussion may be extended to include other auditors if appropriate.

Members of the audit management may also seek to attend and observe audits from time to time. The guidelines above will also apply to them.

### **5.3 SAS subgroup**

The SAS subgroup is a committee comprised of GSMA staff (including the audit management) and members, and representatives of the auditing companies. It is responsible for maintenance of the following SAS-SM documentation:

- The Standard [1] which contains the security objectives for SAS-SM.
- The Consolidated Security Requirements (CSR) [2] which provide requirements for all sensitive processes (SPs) within the scope of the different SAS schemes. Many of the requirements are common across all schemes, however some requirements are specific to individual SPs, including subscription management. The requirements that apply to subscription management are indicated in that document. These are the requirements that the auditee must satisfy in order to be certified.
- The Consolidated Security Guidelines [3] to guide interpretation and operational application of the CSR, and
- The Methodology (this document)

Updates will normally arise from an annual review meeting of the SAS subgroup. Where acute issues are identified ad hoc meetings may be convened to discuss updates to the SAS-SM documentation.

The SAS subgroup also contributes to the development of auditing company selection criteria when GSMA is procuring SAS auditing services from time to time. Operator members of the SAS subgroup that do not offer any products or services within the scope of SAS will be invited by GSMA to participate in the review of tender responses and the selection of auditing companies.

## 5.4 Audit Management

The Audit Management comprises a team of GSMA staff members responsible for administering the scheme, including:

- Selecting suitably qualified auditing companies to carry out the audits, in conjunction with the SAS subgroup as indicated in section 5.3, and ensuring that they provide a high-quality service.
- Ensuring that audits are conducted in accordance with the SAS-SM Methodology and that audit reports meet GSMA quality requirements.
- Managing audit lifecycle tasks, pre and post audit, for example maintenance of the audit log and list of certified and provisionally certified sites
- Contract and financial management between the GSMA and auditees and the GSMA and auditing companies
- Distribution of SAS-SM documentation (this document, the Standard [1], the Consolidated Security Requirements [2], and the Consolidated Security Guidelines[3]) to auditees and auditors.
- Handling general queries about the scheme via [sas@gsma.com](mailto:sas@gsma.com).

## 5.5 Participant Relationships

The relationships between SAS-SM participants are indicated in Figure 2.

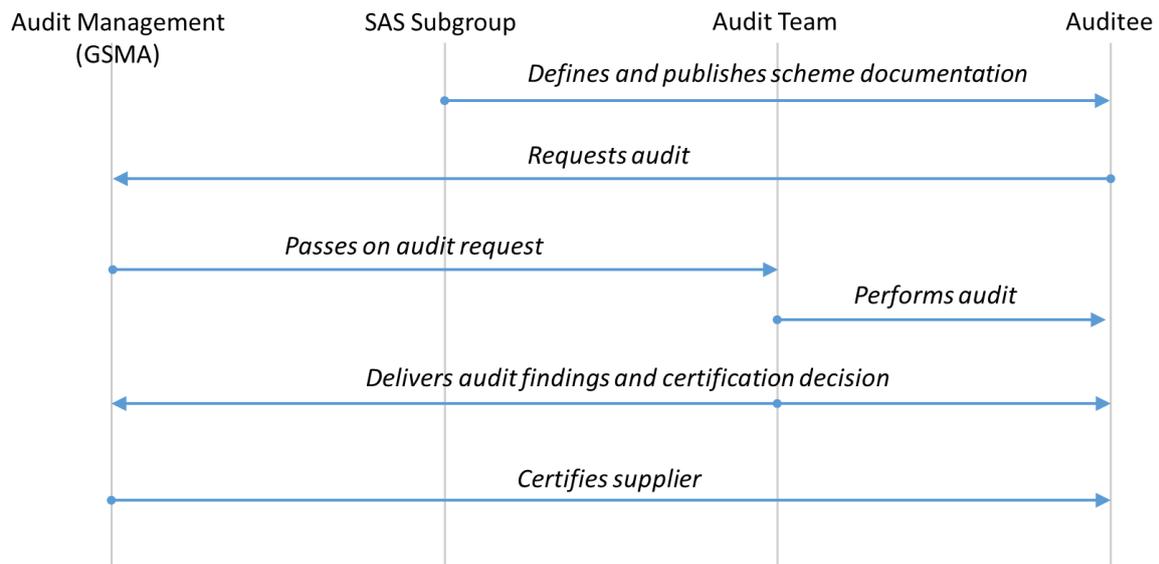


Figure 2 - SAS-SM Participant Relationships

## 6 Audit Report Scoring and Assessment

The audit report (see section 2.3.3) contains detailed audit results. An indexed matrix of requirements is used as a means to structure and standardise recording of compliance. Possible assessments are described in Table 2.

<b>Compliant (C)</b>	Indicates that the auditors' assessment of the site has found that a satisfactory level of compliance with the standard has been demonstrated during the audit. To assist auditees in assessing their audit performance, and to plan improvements, the auditors may, at their discretion, indicate the level of compliance as follows:
	<p><b>Compliant (C):</b></p> <p>In the auditors' assessment the auditee has met the standard to an acceptable level. Comments for further improvement may be offered by auditors.</p>
	<p><b>Substantially compliant (C-):</b></p> <p>In the auditors' assessment the auditee has just met the standard, but additional improvement is thought appropriate to bring the auditee to a level at which compliance can easily be maintained. An assessment of C- will be qualified with comments indicating the improvements required. Future audits will expect to see improvement in areas marked as C-.</p>
<b>Non-compliant (NC)</b>	In the auditors' assessment the auditee has not achieved an acceptable level of compliance with the standard due to one or more issues identified. The issues identified require remedial action to be taken to ensure that an acceptable level of compliance is achieved. Remedial action is compulsory to ensure continued certification.

**Table 2 - Assessments Possible Under SAS-SM**

Non-compliances and required actions will be summarised at the front of the audit report, and described further in the detailed findings.

Comments will normally be provided, marked as (+) and (-) in the *Auditor* remarks to indicate positive and negative implications of the comments. Comments with no symbol represent general comments. The number of (+) or (-) comments bears no relation to the section or sub-section score.

## 6.1 Audit Result

The audit result will be determined based on the level of compliance achieved in all sections of the audit report.

In the event that no sections of the audit report are assessed as non-compliant by the auditors then the audit result will specify that certification will be awarded by GSMA without further improvement.

In the event that one or more sections of the audit report are assessed as non-compliant then the auditee will be required to submit to further assessment in those areas. The assessment may be carried out:

- On-site during a repeat audit
- Off-site through presentation of evidence

The re-assessment method will be determined by the number and nature of issues identified and will be indicated in the audit summary.

Certification will not be awarded where one or more areas of non-compliance are identified.

Once the auditee has submitted to successful re-assessment of the issues identified an updated audit report will be issued specifying that certification will be awarded.

## 7 Maintaining SAS Compliance

SAS certification is awarded based on an assessment by the audit team that the site met the requirements of the SAS Standard during the audit, and that it demonstrated an ability and intent to sustain compliance during the certification period. Continued site compliance with the SAS Standard during the certification period, including the implementation of SAS-compliant controls following any changes to the certified environment, is the responsibility of the site.

Certified sites are required, under their agreement with the GSMA, to notify the GSMA of any major change planned or proposed within the audited domain at the auditee's site, and to host within three months any audits deemed necessary by the GSMA to verify the continued compliance of the site with the SAS Standard as a result of such change. Major changes to the auditee's site that require notification include but shall not be limited to significant production, process or relevant policy changes, and sale of the auditee's site.

### 7.1 Examples of notifiable events

The following examples are provided to help auditees understand what level of change should be notifiable. The list is provided to help guide auditees only. Auditees are always encouraged to contact the GSMA in the event of any uncertainty about whether an event is notifiable.

#### 7.1.1 What should be notified

- Revisions to policy or procedure that change controls audited within the scope of the SAS audit, e.g.:
  - Removal of a procedure or control of sensitive assets
  - Removal of a security screening step for new employees.
  - Reduction in the frequency of a risk assessment process, security awareness training programme or IT vulnerability scan.
- Changes to the responsibility for physical security management, such as site security manager.
- Changes to the responsibility for logical security management, such as key manager, IT security manager.
- Changes to the physical environment where sensitive processes are located or housed, e.g.:
  - Relocation of sensitive processes to new premises or alternative locations within the existing certified site.
  - Enlargement or other physical change to a room or workshop containing a sensitive process
  - Changes to the physical construction of areas of the site where sensitive processes are carried out.

- Changes to the architecture of the networks used for sensitive processes, or to the security level of networks where sensitive processes take place.

### **7.1.2 What would not normally require notification:**

- Replacement or implementation like-for-like of a data processing, production or infrastructure supporting system, e.g.:
  - Replacing a firewall with a new device implementing an identical policy
  - Implementing a new instance of an existing platform with a configuration that applies the same policies.
- Changes to layout of existing certified areas where CCTV visibility and other controls are maintained at an equivalent standard, e.g. changing the positions of:
  - Systems in a server room

## **8 Costs**

The audit fees for an audit are determined by the audit duration, which depends on the audit type (e.g. first dry audit, wet audit, renewal audit, repeat audit or scope extension audit). Costs may also depend on the logistics involved in carrying out the audit, that is, if more than one site is included in each visit the presentations, document reviews and audit performances may take longer than normal. Costs guidance will be sent by the audit management to the auditee in advance of the audit.

### **8.1 First Dry Audit or Renewal Audit**

The audit duration will depend on the logistics involved but will normally take eight person days for an SM-SR, SM-DP, SM-DP+ or SM-DS audit, and nine person-days for a combined SM-SR and SM-DP audit. Detailed costs will be quoted in the GSMA SAS standard agreement [4] which is sent to the auditee in advance of each audit.

Variable costs such as accommodation and travel will be incurred by the auditors with a view to minimising costs while maintaining reasonable standards (see the agreement [4] for more information. The auditors or the auditee may book and pay for travel and accommodation as agreed between the parties on a case by case basis. Where audits are conducted at long haul destinations during consecutive weeks every effort will be made to minimise costs by conducting several audits during one trip and allocating the travel and accommodation costs proportionately between multiple auditees where applicable.

### **8.2 Audit of sites with limited scope**

First audits for sites with a very limited scope of certification (e.g. sites only providing data centre operations and management) may be conducted over a period different to the standard audit duration. Auditees should notify the audit management of the reduced scope at the time of application for first audit. A proposed audit duration will be agreed in advance of the first audit. The proposed duration for subsequent renewal audits will be documented by the auditors in the audit report.

### 8.3 Audit of Central / Corporate Functions

Subscription management entities may be group companies that have a number of sites. In some cases some functions, knowledge or expertise may be centralised, with common solutions deployed at multiple sites.

Auditees may request that common solutions are audited in detail, centrally. In such a case, successful audits will result in approval of such solutions for deployment across multiple SAS-SM certified sites within the corporate group. Audits will be undertaken by the audit team to a scope agreed in advance between the auditee, audit management and audit team. Approval will be granted via an audit report prepared by the audit team, issued to the audit management, and notified in writing to the auditee.

Subsequent audits at sites dependent on centralised functions deployed elsewhere will ensure that the centrally-approved solutions are deployed appropriately, but will not consider the detail of the solutions themselves.

Certification of all sites deploying such solutions will become dependent on renewal of approval of centralised solutions. Renewal will be required every two years.

Audits of centralised functions will be agreed on a case-by-case basis with auditees. The duration of audits at individual sites may be reduced where appropriate.

### 8.4 Repeat Audit

The costs for a repeat audit will depend on the required duration of the repeat audit, which in turn depends on the number of areas assessed as non-compliant during the preceding audit. The repeat audit duration is agreed between the audit team and the auditee at the end of the preceding audit and the fixed cost is the daily rate quoted in the contract between GSMA and the auditee, multiplied by the number of auditor days required to conduct the repeat audit.

Repeat audits must be conducted within three months of the original non-compliant audit and the auditee must certify that no significant changes have taken place to affect the site security during the time period between the original and the repeat audits.

### 8.5 Off-Site Review of Improvements

Where the auditors' recommendation at audit is non-compliant with an off-site reassessment method, it is likely that additional time will be required to review evidence of changes provided by auditees. Such time may be chargeable to auditees in addition to the cost of the audit itself.

Where an off-site reassessment method is recommended by the auditors, the audit report will include an estimate of the time required to review the evidence and update the audit report. This estimate will be used as the basis for charging.

The estimate will be based on the following structure:

**Total units = Administration + Minor items + Major items**

where:

<b>Administration</b>	1 unit	Applies to all off-site reassessment. Covers updates to report, general communication with auditee and GSMA
<b>Minor items</b>	1 unit per item	Applies to each audit report sub-section assessed as NC where the scope of improvement is limited to: <ul style="list-style-type: none"> <li>• Minor changes to individual documents</li> <li>• Changes to individual controls, where changes can be illustrated by simple photographs, plans or updated documents</li> </ul>
<b>Major items</b>	4 units per item	Applies to each audit report sub-section assessed as NC where the scope of improvement is: <ul style="list-style-type: none"> <li>• Significant changes to processes (new or existing) with multiple documents or elements to be reviewed</li> <li>• Changes to individual controls, where changes require detailed review or analysis of multiple documents, photographs, plans or video</li> <li>• Changes to multiple linked controls</li> </ul>

**Table 3 - Estimating Auditor Time for Off-Site Review of Improvements**

For each audit, charging will be based on the total applicable units:

- 0-3 units (one or two minor issues, plus admin) – no charge,
- 4-6 units (three or more minor items or one major item) – half-day charge per auditor,
- >6 units – full day charge per auditor.

### **8.6 Scope Extension Audits**

If a site is already certified for one or more SM services and wishes to extend certification to include other SM services, it needs to hold dry and wet audits for the additional SM services for which SAS-SM certification is being sought. The duration of scope extension dry and wet audits will normally be reduced compared to the audits that have previously taken place at the site to gain initial SAS-SM certification. The duration will be agreed on a case-by-case basis with auditees.

### **8.7 Cancellation Policy**

An audit cancellation fee shall be payable by the auditee to each (of the two) auditors for each scheduled audit day where less than fourteen (14) business days notice of cancellation, from the date that an audit is due to commence, is given by the auditee.

The auditee shall also be liable for certain unavoidable and non-recoverable expenses (e.g. visa application fees) incurred by the auditors where less than 60 days notice of cancellation, from the date than an audit is due to commence, is given by the auditee, or where GSMA cancels the audit as a result of non-compliance by the auditee with the terms of the SAS-SM standard agreement. Such expenses shall be evidenced by receipts. More details are contained in the SAS-SM standard agreement [4].

### **8.8 Appeals**

Charges for each appeal will be based on the same principles as for estimating charges for off-site review of improvements, as specified in section 8.5.

If an appeal results in a change to the certification decision for an auditee site, then no fee shall be payable by the auditee and the Appeals Board cost will be borne by GSMA. If an appeal results in no change to the certification decision for an auditee site, then the costs of the appeal shall be payable by the auditee.

## 9 Final Report

In the course of each audit, the auditors will make observations which will be recorded in the audit report. Various details will also be recorded in the course of the audit that will result in the production of a final audit report, the content of which is described in Annex A.

## 10 Auditing and Certification of Supporting Sites

SAS provides auditing and certification on a site-by-site basis. However, sites that participate in the scheme may use additional physical sites owned and operated by themselves or by third party subcontractors to provide some supporting infrastructure or services within the scope of certification. This document proposes how such additional supporting sites should be formally handled within the scheme.

### 10.1 Definition

A supporting site is one that meets all of the following criteria:

- Provides supporting infrastructure and/or services within the scope of SAS certification to the primary site seeking certification.
- Does not wish to hold its own SAS certification, or is not eligible to do so.
- To be eligible for SAS-SM certification, a site must operate, or be planning to operate, live and primary (not just backup) production or services that fulfil at least one of the primary SAS- SM scope elements.
- Exceptional applications for SAS certification by sites that do not meet these criteria will be considered by GSMA on a case-by-case basis.

In most cases the supporting site is primarily accountable (via internal or contractual agreements) to the primary site rather than to GSMA for its compliance with the SAS requirements. However, a supporting site must still be subject to the terms of SAS participation, and therefore must be named on an SAS agreement signed by the primary site or the primary site's parent company.

A secondary site is a supporting site that is included as part of the same audit process and audit report as the primary site.

### 10.2 Auditing and Certification Approach

The auditing and certification process to be followed is slightly different depending on the type of supporting site, as follows:

### 10.3 Data Centres hosting SM solutions

Data centres hosting SM solutions typically provide the SM service provider with a secure room or cage within the data centre, electrical power, air conditioning, connectivity and

building security controls. The focus of the SAS-SM audit is the room or cage within which the SM platform is contained, which is under the control of the SM service provider. The data centre provider is responsible as a subcontractor to the SM service provider for the services that it provides within SAS-SM scope.

The primary site and the supporting site in this case are the same. On the SAS-SM certificate, this will be represented by specifying the auditee name, with a site location as the data centre name and address. In practice, part of the SAS-SM audit (documentation review, meetings, interviews) will be performed outside of the SM server room/cage. This may be in a different room, building, city or even a different country, depending on the corporate office facilities provided by the SM service provider and the locations of key personnel. If there are no sensitive processes within SAS-SM scope occurring at these corporate offices, the location(s) of these offices will usually not be specified on the SAS-SM certificate. If sensitive processes are occurring at these locations, these will be specified as described (e.g. the location of remote administrative access would be specified as per section 10.6)

Item	Description
Application form	SAS-SM applicants should indicate on the SAS application form if an external data centre is being used.
Audit scheduling and duration	Although their focus is to provide supporting services, SM data centres (DCs) are considered as primary sites, given that they host SM servers and assets and are used for activities such as key ceremonies. The SAS-SM audit duration is not affected solely by the use of a DC. However, in practice, if part of the SAS-SM audit (e.g. documentation review, meetings, interviews) is performed outside of the DC, the distance between the DC and other site(s) may affect the overall audit duration. If the necessary transfer time between the DC and other site(s) is significant and is expected to extend the overall audit duration, this should be highlighting by the auditee when the audit is being scheduled.
SAS agreement and invoicing	SM data centres do not sign an SAS-SM participation agreement directly with GSMA. Their involvement in the scheme is indirect and through the SM service provider. However, the name and address of the DC should be specified in the agreement. The SM service provider is invoiced for the audit.
Audit report	A single audit report should be prepared covering the in-scope activities performed by the auditee and/or relevant to the SM DC.
SAS Certificate and website listing	The SAS certificate will contain specifying the auditee name, with a site location as the data centre name and address. A single certification expiry date applies and will be specified on the certificate.

#### 10.4 SM Backup Sites

Item	Description
Application form	If use of a backup site is part of the business continuity plan for the primary site, then SAS-SM applicants should provide backup site details on the SAS application form.
Audit scheduling and duration	SM backup site audits may be conducted back-to-back or with some period between them, depending on auditee preference.

Item	Description
	<ul style="list-style-type: none"> <li>• Back-to-back audits of primary and backup sites provides the fastest means to certification of the primary site, as there is no delay waiting for the backup site audit and outcome. It is likely to also result in lower overall auditor travel expenses, and means that the certification periods for both sites remain aligned.</li> <li>• Independent scheduling (primary site first) allows the participant to improve controls at the backup site based on any non-compliances found during the audit of the primary site, improving the chance of a compliant result at the first audit of the backup site and therefore avoiding the need for a re-audit.</li> </ul> <p>The standard audit duration for SM backup sites is 3 days, given the overlap in controls in many areas. For back-to-back audits, transfer time between primary and backup sites will need to be considered when scheduling the audits and will determine whether the standard 1 day chargeable travel time applies to the audit of the backup site.</p>
SAS agreement and invoicing	<p>The backup site (whether owned by primary site applicant or a third party subcontractor) must be subject to the terms of the SAS participation agreement. The backup site should be specified in the primary site's agreement. If the backup site audit request is received after the primary site's agreement has already been executed, then another instance of the agreement specifying the backup site will need to be signed.</p> <p>The primary site applicant is invoiced for the audit.</p>
Audit report	<p>Controls and observations common to the primary and backup sites made at a single point in time (i.e. back-to-back or closely scheduled audits) can be documented once only, but need to be highlighted as being common. The audit team can decide whether to report their findings in a single document (but clearly distinguishing which site their observations refer to) or in two documents (with references in relevant sections to the observations and assessments on common controls described in the other report). If there is a significant time interval between primary and backup site audits, separate reports are recommended.</p>
SAS Certificate and website listing	<p>The backup site name and address are mentioned on the SAS certificate of the primary site(s) to which they provide support.</p>
Provisional certification	<p>It may occur that the primary site holds full certification while the backup site holds provisional certification. This will be highlighted on the SAS certificate.</p> <p>If the certification of a backup site lapses, GSMA may withdraw the SAS certification of the associated primary site(s).</p>

### 10.5 Centralised or Outsourced IT Services

Item	Description
Examples	<p><u>Centralised IT administration, network operations centre, server farm, firewall management</u></p>
Application form	<p>The application form provides space to provide supporting site details and to outline the site activities.</p>

Item	Description
Audit scheduling and duration	<p>Supporting sites providing centralised or outsourced IT services may host initial audits scheduled back-to-back or closely scheduled with primary site audits. Audits of additional primary sites that depend on the supporting site's certification are scheduled independently.</p> <p>The audit duration depends on the supporting site activities, and should be agreed on a case by case basis with the audit team. For back-to-back audits, transfer time between sites should also be agreed.</p>
SAS agreement and invoicing	<p>The supporting site (whether owned by the primary site applicant or a third party subcontractor) must be subject to the terms of the SAS participation agreement. The site should be specified in the primary site's agreement. If the supporting site audit request is received after the primary site's agreement has already been executed, then another instance of the agreement specifying the supporting site will need to be signed.</p> <p>The primary site applicant or its parent company is invoiced for the audit.</p>
Audit report	<p>Only the sections of the audit report relevant to the activities performed by the site need to be completed by the audit team.</p>
SAS Certificate and website listing	<p>The supporting site name and address are mentioned on the SAS certificate of the primary site(s) to which they provide support.</p>

### 10.6 SM Remote Administrative Access Sites

This applies to sites that have routine remote administrative access to SM applications and systems, i.e. access to unencrypted sensitive data assets and functions within audit scope.

Remote customer access to an SM application that does not enable administrative access to or control of any sensitive assets or infrastructure does not require SAS-SM certification of the remote access site.

Item	Description
Application form	<p>The application form provides space to provide supporting site details and to outline the site activities.</p>
Audit scheduling and duration	<p>Flexible scheduling (scheduled independently of primary site audit or conducted back-to-back).</p> <p>The audit duration depends on the supporting site activities, and should be agreed on a case by case basis with the audit team. For back-to-back audits, transfer time between sites should also be agreed.</p>
SAS agreement and invoicing	<p>The supporting site (whether owned by primary site applicant or a third party subcontractor) must be subject to the terms of the SAS participation agreement. The site should be specified in the primary site's agreement. If the remote access site audit request is received after the primary site's agreement has already been executed, then another instance of the agreement specifying the remote access site will need to be signed.</p> <p>The primary site applicant is invoiced for the audit.</p>
Audit report	<p>Only the sections in the audit report relevant to the activities performed by the site need to be completed.</p>

Item	Description
	The audit team can decide whether to add their findings to the primary site audit report (but clearly distinguishing which site their observations refer to) or produce a second report (with references in relevant sections to the observations and assessments on common controls described in the other report). If there is a significant time interval between primary and remote access site audits, separate reports are recommended.
SAS Certificate and website listing	The supporting site name and address are mentioned on the SAS certificate of the primary site(s) to which they provide support.
Provisional Certification	Not applicable. Certification type is determined by primary site only.

## 10.7 Cloud Service Providers (CSP)

This applies where a CSP is a subcontractor to an SM service provider, i.e.

- CSP does not hold its own SAS certification. It is listed as subcontractor on its client's SAS certificate.
- It is only audited and certified for services that it provides to the specific client.
- It does not engage or contract directly with GSMA.

If a CSP applies directly to GSMA for its own SAS-SM certification with scope "Data Centre Operations and Management", then it should be handled as a primary site.

Item	Description
Application form	The application form should specify all CSP sites where SM service provider data may be held, via multiple application forms if necessary.
Audit scheduling and duration	Although their focus is to provide supporting services, CSP data centres (DCs) may be considered and treated as primary sites as described in section 10.2, given that they host SM servers and assets. Scheduling is flexible (scheduled independently of primary site audit or conducted back-to-back). Audit duration depends on the number of CSP sites to be audited, the activities performed and the consistency of controls at each site, and should be agreed on a case by case basis with the audit team. For back-to-back audits, transfer time between sites should also be agreed.
SAS agreement and invoicing	The CSP sites must be subject to the terms of the SAS participation agreement. The sites should be specified in the primary site's agreement.
Audit report	Usually a separate report to primary site, but will depend on services provided. Only the sections in the audit report relevant to the activities performed by the site need to be completed.
SAS Certificate and website listing	The CSP site name(s) and address(es) are specified on the SAS certificate of the SM service provider to which they provide support. If multiple CSP sites provide support, a customised SAS certificate may be created to list these.
Provisional Certification	Not applicable to CSPs, as their activities are already live. First audits of these sites lead to full certification.

## **10.8 Audit Reports**

Relevant contextual information about the audit should be provided within all audit reports (within “Auditors’ Comments” section or other standardised tables/subsections within template). This is especially important if a supporting site is being audited. The information provided should include site location(s), dates and duration, audit type and approach, summary of activities performed at each site, any relevant audit history, and explanatory notes in relation to how the report has been prepared and any deviations from standard audit practice if necessary.

## **10.9 SAS Certificates**

If the certification expiry dates of a primary site and a backup site are different, GSMA will include both expiry dates on the certificate. Note that this approach will trigger reissue of certificates to primary site(s) by GSMA each time a supporting site renews certification.

If the certification of a supporting site lapses, GSMA may withdraw the SAS certification of the associated primary site(s).

## Annex A Final Audit Report Structure

### A.1 First Page:

- **Headline:** Security Accreditation Scheme for Subscription Manager Roles Qualification Report
- **Scope of Audit:**
  - SM-SR only
  - SM-DP only
  - SM-DP+ only
  - SM-DS only
  - Multiple SM roles (specify)
- **Type of Audit (within SAS certification lifecycle):**
  - “First-Audit” for the first audit at the site
  - “Renewal Audit” in the following years after a first audit
  - “Repeat Audit” because the result of the “First Audit” or the “Renewal Audit” was unsatisfactory
  - Dry audit / wet audit, if applicable
  - Scope extension audit
- **Type of Audit (if a provisional audit):**
  - Dry audit
  - Wet audit
- Name of the auditee and location of the audited site
- Date of the audit
- Audit number
- Audit team participants

### A.2 Subsequent Pages:

- Audit result and summary
- Auditors’ comments
- Actions required
- Appendix A – Detailed Results

Section	Result of Sub-Section	Auditor Remarks
<b>Policy, Strategy and Documentation Result</b>		
Strategy	C	+ comment
Documentation	C	
Business continuity planning	NC	- comment
Internal audit and control	C	

Section	Result of Sub-Section	Auditor Remarks
<b>Organisation and Responsibility Result</b>		
Organisation	C	
Responsibility	NC	
Incident response and reporting	C	+ comment
Contracts and Liabilities	NC	
<b>Information Result</b>		
Classification	NC	- comment - comment
Data and media handling	C-	
<b>Personnel Security Result</b>		
Security in job description	C	Comment
Recruitment screening	C	+ comment
Acceptance of security rules	C	
Incident response and reporting	C	
Contract termination	C-	
<b>Physical Security Result</b>		
Security plan	C	
Physical protection	NC	
Access control	NC	- comment
Security staff	NC	
Internal audit and control	C	+ comment
<b>Certificate and Key Management Result</b>		
Classification	C	+ comment
Roles and Responsibilities	C	
Cryptographic key specification	C	
Cryptographic key management	C	- comment
Audit and accountability	NC	
GSMA PKI Certificates	NC	- comment
<b>Sensitive Process Data Management Result</b>		
Data transfer	C	
Sensitive data access, storage and retention	C	
Data Generation	C-	- comment
Auditability and accountability	C	+ comment - comment
Duplicate production	C	+ comment
Data integrity	C	+ comment

Section	Result of Sub-Section	Auditor Remarks
Internal audit and control	C	
<b>SM-DP, SM-SR, SM-DP+ and SM-DS Service Management Result</b>		
SM-DP, SM-SR, SM-DP+ and SM-DS service	NC	
Remote entity authentication	C	
Audit trails	C	
<b>Computer and Network Management Result</b>		
Policy	C	
Segregation of roles and responsibilities	NC	
Access control	C	
Network security	C	
Systems security	C	
Audit and monitoring	C	
External facilities management	C	- comment
Internal audit and control	C-	- comment
Software Development	C	

- Appendix C: SAS Scoring Mechanism (that is, a copy of Table 2 of this document)

## Annex B Standard Audit Agenda

The following agenda is proposed for all audits (first and renewal audits) as a guide for auditees. Non-standard audits (principally repeat audits) may have shorter duration and a specific agenda will be agreed.

The standard agenda for a four-day audit is split into eight half-day segments which will normally be carried out in the sequence set out below.

The audit agenda may be adjusted based on production schedules or availability of personnel. The auditors may also wish to change the amount of time spent on different aspects during the audit itself.

Half-day Segment	Outline Agenda	Suggested Auditee Preparation
1	<ul style="list-style-type: none"> <li>• Company / site introduction and overview</li> <li>• Overview of changes to site and security management system</li> <li>• Description of security management system</li> <li>• Review of security policy and organisation</li> <li>• IT infrastructure</li> <li>• Subscription management architecture and infrastructure</li> </ul>	<p>Preparation of introductory presentations to include:</p> <ul style="list-style-type: none"> <li>• Company/corporate background and overview</li> <li>• Site introduction/overview</li> <li>• Production and audit scope</li> <li>• Security management organisation, responsibility and system</li> <li>• IT and information security overview</li> </ul> <p>Preparation of copies of appropriate documents for review by the auditors during the audit.</p> <p>A high-level network diagram of the entity's networking typography showing the overall architecture of the environment being assessed. It should include all components used, connections in and out of the network</p>
2a	<ul style="list-style-type: none"> <li>• <b>For SM-SR</b></li> <li>• SM-SR system                             <ul style="list-style-type: none"> <li>○ eUICC registration</li> <li>○ Platform management</li> <li>○ SM-SR change</li> <li>○ Control</li> <li>○ Audit trails</li> </ul> </li> </ul>	<p>Preparation of detailed data flow diagram showing end-to-end lifecycle of remote management, to include:</p> <ul style="list-style-type: none"> <li>• Certificate enrolment</li> <li>• eUICC Registration</li> <li>• Management of requests and eUICC status during the SM-SR process</li> </ul> <p>Diagrams should include detailed description of controls in place to preserve the confidentiality, integrity and availability of data throughout the process and its auditability.</p> <ul style="list-style-type: none"> <li>• Preparation of detailed description of SM-SR mechanism used for sensitive data (for example, individual eUICC keys)</li> </ul>

2b	<ul style="list-style-type: none"> <li>• <b>For SM-DP or SM-DP+</b></li> <li>• SM-DP / SM-DP+ system                         <ul style="list-style-type: none"> <li>○ Platform management (Only for SM-DP)</li> <li>○ Data Preparation</li> <li>○ Profile management</li> <li>○ Control</li> <li>○ Audit trails</li> </ul> </li> </ul>	<p>Preparation of detailed data flow diagram showing end-to-end lifecycle of remote management, to include:</p> <ul style="list-style-type: none"> <li>• Certificate enrolment</li> <li>• Data Preparation and Profile Management                         <ul style="list-style-type: none"> <li>○ Profile Description management and generation of Un-personalised Profile</li> <li>○ Generation of Personalisation Data for the targeted profile (for example, Network Access Credentials and other data) based upon input data from the MNO</li> <li>○ Generation of Personalised Profiles for the targeted eUICC</li> </ul> </li> <li>• Management of requests during the SM-DP. SM-DP+ process (for example, Platform Management for SM-DP, Profile Download Initiation for SM-DP+, )</li> <li>• Preparation of detailed description of SM-DP / SM-DP+ mechanism used for sensitive data (for example, individual MNO keys)</li> <li>• Diagrams should include detailed description of controls in place to preserve the confidentiality, integrity and availability of data throughout the process and its auditability.</li> </ul>
3	<ul style="list-style-type: none"> <li>• Key management and data protection                         <ul style="list-style-type: none"> <li>○ Asset control</li> </ul> </li> </ul>	<p>Description of how asset is protected during its full lifecycle</p>
4	<ul style="list-style-type: none"> <li>• IT infrastructure and security</li> <li>• Systems development and maintenance</li> </ul>	<p>Preparation of detailed description of system maintenance procedures, to include:</p> <ul style="list-style-type: none"> <li>• Patch management</li> <li>• System Configuration</li> <li>• Security vulnerabilities management</li> </ul>
5	<ul style="list-style-type: none"> <li>• Physical security concept</li> <li>• Physical security                         <ul style="list-style-type: none"> <li>○ External and internal inspection</li> <li>○ Control room</li> </ul> </li> </ul>	<p>Preparation of printed copies of site plans and layouts of security systems for use by the auditors.</p> <p>Plans will be used as working documents for annotation by the auditors during the physical security review.</p> <p>Plans will only be used during the audit and will not be removed from the site at any time.</p>
6	<ul style="list-style-type: none"> <li>• Detailed review of security</li> </ul>	<p>Preparation of printed copies of documents</p>

	<p>management system documentation, including (but not limited to):</p> <ul style="list-style-type: none"> <li>○ Asset classification</li> <li>○ Risk assessment</li> <li>○ Business continuity plan</li> <li>○ Human resources</li> </ul>	<p>for review by the auditors (see also document list). Documents will only be used during the audit and will not be removed from the site at any time.</p>
7	<ul style="list-style-type: none"> <li>• Internal audit system</li> <li>• Finalise report, present findings</li> </ul>	

## Annex C Standard Document List

The auditors will normally require access to the documents listed below during the audit, where such documents are used by the auditee. Copies of the current version of these documents must be available in English for each auditor.

Additional documentation may be requested by the auditors during the audit; where such documents are not available in English, translation facilities must be provided by the auditee within a reasonable timescale. The auditors will seek to minimise such requests, whilst still fulfilling the requirements of the audit.

### C.1 Document List

- Subscription Management system description

This should specify which subscription management roles that the entity provides at the site. It shall include a high-level network diagram of the entity's networking topography, showing the overall architecture of the environment being assessed. This high-level diagram should summarize all locations and key systems, and the boundaries between them and should include the following.

- Connections into and out of the network including demarcation points between the subscription management environment and other networks/zones
  - Critical components within the subscription management environment, including systems, databases, firewalls, HSM and web servers, as applicable
  - Clear and separate identification of respective components for separate systems if the site is operating multiple processes (e.g. SM-SR and SM-DP). Description of associated processes and responsibilities.
- Overall security policy
  - IT security policy
  - Security handbook
  - Security management system description
  - Security management system documentation as provided to employees
  - Business continuity plan
  - Job descriptions for all employees with security responsibilities
  - Confidentiality agreement for employees
  - Standard employment contract
  - Employee exit checklists

It is accepted that in some cases not all of these documents will be used by auditees, or that one document may fulfil multiple functions.

All documents shall be used on-site during the audit only; the auditors shall not remove documents from the site during the audit and shall return all materials at the end of each audit day.

## Annex D Subscription Management Processing Audit

As part of the audit of the site's Subscription Management system and supporting processes it is preferred that auditees prepare a SM-SR, SM-DP, SM-DP+ or SM-DS SAS-specific audit scenario in advance of the audit date. The audit scenario may use test data (for a dry audit) or live data (for a full or wet audit). This document provides a suggested approach; the auditee and audit team will agree the precise approach for each audit.

The purpose of these audit scenarios is to allow the audit to be carried out in a consistent way to consider:

For SM-SR

- SM-SR interaction with other roles in the embedded SIM ecosystem (ES1, ES3, ES4, ES5, ES7)
- Profile download and installation with SM-DP
- Platform and eUICC management operations
- Data protection
- Log files

For SM-DP

- SM-DP interaction with other roles in the embedded SIM ecosystem (ES2, ES3, ES8)
- Profile creation, download and installation with SM-SR
- Profile management operations
- Data protection
- Log files

For SM-DP+

- SM-DP+ interaction with other roles in the embedded SIM ecosystem (ES2+, ES8+/ES9+, ES12)
- Profile creation, download and installation
- Local profile management notification
- Data protection
- Log files

For SM-DS

- SM-DS interaction with other roles in the embedded SIM ecosystem (ES11, ES12, ES15)
- Event Registration
- Event Deletion
- Event Retrieval
- Data protection
- Log files

The audit scenarios are intended to be transparent and will not deliberately involve any form of system intrusion.

Note: For the performance of an audit scenario in a dry audit, interactions between entities can be simulated. For a wet or full audit, evidence of interactions with other production entities must be available.

## **D.1 Before the Audit**

### **D.1.1 Preparation**

The auditee should make arrangements to prepare the relevant other roles (e.g. EUM, MNO, SM-DP, SM-SR, SM-DP+, SM-DS, eUICC) that will be needed by the auditee to demonstrate its compliance with the Standard. The roles may be set up for simulation only (for dry audits). Existing connected entities used in production must be used for wet or full audits.

It is recognised that different configurations may be used for different roles. One should be selected that is representative of the current scope of activities at the site. The audit will focus on those security processes that are typically practiced and/or recommended by the auditee to mobile operator customers. It is the auditee's responsibility to select appropriate, representative processes.

If more than one SM-SR, SM-DP, SM-DP+ or SM-DS solution is offered to customers (excluding any customer-specific solutions) then the number of different solutions and the nature of the differences should be confirmed with the audit team before setting up the audit scenarios.

### **D.1.2 Certificate Enrolment**

The auditee should initiate its process for certificate enrolment, to include:

- Exchange of certificates

If the Certificate Issuer (CI) does not exist at the time of an audit, the auditee will need to self-certify or utilise the GSMA's test certificates.

### **D.1.3 Further Preparation for Audit (SM-SR)**

#### **D.1.3.1 eUICC Registration**

Two input eUICC information files (eUICC-1 and eUICC-2) will be prepared by the auditee and supplied to the audit team in advance of the audit. See below for a description of how these files will be used. Test data will be used for a dry audit, and live data will be used for a wet or full audit. The input eUICC information will be submitted electronically by the auditee's nominated mechanism or an alternative mechanism if set-up cost is implied.

The auditee will prepare the input file which will include test data and structure to be used in the audit and supply this in advance to the audit team.

#### **D.1.3.2 Processing of eUICC Registration eUICC-1**

Auditees should carry out eUICC registration for the first eUICC in advance of the audit.

NOTE: Registration for eUICC-2 should not be processed before the audit

### D.1.3.3 Profiles

Personalised profiles for the targeted eUICCs will normally be created by the auditee and made available to the audit team in advance of the audit. The personalised profile will be submitted electronically by the auditee’s nominated SM-DP in the profile download and installation procedure or an alternative mechanism (for example, using test data) in the case of a dry audit.

### D.1.3.4 Processing of Profile Download and Installation for eUICC-1

Auditees should carry out profile installation and download for a personalised profile for the first eUICC in advance of the audit.

NOTE: Profile download and installation for eUICC-2 should not be processed before the audit

### D.1.3.5 Timescales

Exact timescales for the process will be agreed between the audit team and auditee, but would typically involve:

Time before audit	Actions
Week –4	Opening discussions regarding process
Week –3	Auditee to conduct internal preparations for SM-SR audit
Week –2	Auditee to communicate requirements for certificate enrolment and message protocols to other roles in the embedded SIM ecosystem
Week –1	Auditee to maintain eUICC information available for review by the audit team Auditee to process first eUICC Registration and Profile Installation and Download Auditee to maintain output responses for first eUICC for review by the audit team.

## D.1.4 During the Audit (SM-SR)

### D.1.4.1 Review of Certificate Enrollment and Verification

The audit team will discuss and review the certificate enrolment and verification process with the auditee, including reference to relevant logs and records.

### D.1.4.2 Review of eUICC Registration Processing

The audit team will discuss and review the processing of registration of eUICC-1 with the auditee, including reference to relevant logs and records.

### D.1.4.3 Demonstration of Input eUICC 2 Processing

The audit team shall request that auditees use input information for eUICC-2 to provide a live demonstration of the eUICC registration processing flow.

#### **D.1.4.4 Review of Profile Download and Installation Processing**

The audit team will discuss and review the processing of profile download for eUICC-1 with the auditee, including reference to relevant logs and records.

#### **D.1.4.5 Demonstration of Profile Download and Installation Processing**

The audit team shall request that auditees provide a live demonstration of the profile download and installation processing flow using a personalised profile for eUICC-2.

#### **D.1.4.6 Demonstration of Enabling, Disabling and Deletion of Profile**

The audit team shall request that auditees provide a live demonstration of the profile enabling, disabling and deletion processing flow using a personalised profile for eUICC-1 or eUICC-2.

#### **D.1.4.7 Demonstration of SM-SR Change**

The audit team shall request that auditees provide a detailed plan of the process to perform an SM-SR change.

### **D.1.5 Further Preparation for Audit (SM-DP)**

#### **D.1.5.1 Unpersonalised Profile Creation**

The unpersonalised profile is created by the auditee taking into account the MNO's profile description and the eUICC type. For the dry audit, a sample profile description and sample eUICC type chosen by the auditee may be used.

#### **D.1.5.2 Profile Ordering and Personalisation**

Two operator input files (IF-1 and IF-2) containing for example, IMSI, ICCID, POL1, will be prepared by the auditee and supplied to the audit team in advance of the audit. See below for a description of how these files will be used. Test data (may be generated by the audit team in a format agreed with the auditee) will be used for a dry audit, and live data will be used for a wet or full audit. The input files will be submitted electronically by the auditee's nominated mechanism or an alternative mechanism if set up cost is implied.

The auditee will prepare the input file which will include test data and structure to be used in the audit and supply this in advance to the audit team.

The auditee will use the input file IF-1 to personalise profiles in advance of the audit, including generation of the operator keys (Ki), and use IF-2 to personalise profiles and generate operator keys (Ki) during the audit.

#### **D.1.5.3 Profile Download and Installation**

The auditee will ensure that there is a personalised profile ready to be downloaded and install.

#### **D.1.5.4 Timescales**

Exact timescales for the process will be agreed between the audit team and auditee, but would typically involve:

Time Before Audit	Actions
Week –4	Opening discussions regarding process
Week –3	Auditee to conduct internal preparations for SM-DP audit
Week –2	Auditee to communicate requirements for certificate enrolment and message protocols to other roles in the embedded SIM ecosystem
Week –1	<p>Auditee to maintain profile ordering information available for review by the audit team</p> <p>Auditee to process the IF-1, profile creation and profile download and Installation.</p> <p>Auditee to maintain output responses for first IF-1 for review by the audit team.</p>

## **D.1.6 During the Audit (SM-DP)**

### **D.1.6.1 Review of Certificate Enrollment and Verification**

The audit team will discuss and review the certificate enrolment and verification process with the auditee, including reference to relevant logs and records.

### **D.1.6.2 Demonstration of Input IF-1 Processing**

The audit team will review the data flow of the input file (IF-1) that has been received and processed and it will check the protection of the sensitive assets and logs involved in this process.

### **D.1.6.3 Review of Profile Download and Installation Processing**

The audit team will discuss and review the processing of profile download for IF-1 with the auditee, including reference to relevant logs and records.

### **D.1.6.4 Demonstration of Profile Download and Installation Processing**

The auditee may provide a live demonstration of the profile download and installation processing flow using a personalised profile for IF-2.

### **D.1.6.5 Demonstration of Enabling, Disabling and Deletion of Profile**

The auditee may provide a live demonstration of the profile enabling, disabling and deletion processing flow using a loaded profile.

## **D.1.7 Further Preparation for Audit (SM-DP+)**

### **D.1.7.1 Unpersonalised Profile Creation**

The unpersonalised profile is created by the auditee taking into account the MNO's profile description and the eUICC type. For the dry audit, a sample profile description and sample eUICC type chosen by the auditee may be used.

Note: this current process if done for SM-DP is to be applicable for SM-DP+.

### D.1.7.2 Profile Ordering and Personalisation

Two operator input files (IF-1 and IF-2) containing for example, IMSI, ICCID will be prepared by the auditee and supplied to the audit team in advance of the audit. See below for a description of how these files will be used. Test data (may be generated by the audit team in a format agreed with the auditee) will be used for a dry audit, and live data will be used for a wet or full audit. The input files will be submitted electronically by the auditee’s nominated mechanism or an alternative mechanism if set up cost is implied.

The auditee will prepare the input file which will include test data and structure to be used in the audit and supply this in advance to the audit team.

The auditee will use the input file IF-1 to personalise profiles in advance of the audit, including generation of the operator keys (Ki), and use IF-2 to personalise profiles and generate operator keys (Ki) during the audit.

Note: this current process if done for SM-DP is to be applicable for SM-DP+.

### D.1.7.3 Profile Download and Installation

The auditee will ensure that there is a personalised profile ready to be downloaded and install.

### D.1.7.4 Timescales

Exact timescales for the process will be agreed between the audit team and auditee, but would typically involve:

Time Before Audit	Actions
Week –4	Opening discussions regarding process
Week –3	Auditee to conduct internal preparations for SM-DP+ audit
Week –2	Auditee to communicate requirements for certificate enrolment and message protocols to other roles in the embedded SIM ecosystem
Week –1	<p>Auditee to maintain profile ordering information available for review by the audit team</p> <p>Auditee to process the IF-1, profile creation and profile download and Installation.</p> <p>Auditee to maintain output responses for first IF-1 for review by the audit team.</p>

## D.1.8 During the Audit (SM-DP+)

### D.1.8.1 Review of Certificate Enrollment and Verification

The audit team will discuss and review the certificate enrolment and verification process with the auditee, including reference to relevant logs and records.

#### **D.1.8.2 Demonstration of Input IF-1 Processing**

The audit team will review the data flow of the input file (IF-1) that has been received and processed and it will check the protection of the sensitive assets and logs involved in this process.

#### **D.1.8.3 Review of Profile Download and Installation Processing**

The audit team will discuss and review the processing of profile download for IF-1 with the auditee, including reference to relevant logs and records.

#### **D.1.8.4 Demonstration of Profile Download and Installation Processing**

The auditee may provide a live demonstration of the profile download and installation processing flow using a personalised profile for IF-2.

The auditee must demonstrate the download and installation on all 3 modes from the specification: (activation code, default SM-DP+, service discovery).

#### **D.1.8.5 Demonstration of Enabling, Disabling and Deletion of Profile**

The auditee may provide a live demonstration of the profile enabling, disabling and deletion processing flow using a loaded profile via LPA and ensure the SM-DP+ gets the proper notification.

### **D.1.9 During the Audit (SM-DS)**

#### **D.1.9.1 Review of Certificate Enrollment and Verification**

The audit team will discuss and review the certificate enrolment and verification process with the auditee, including reference to relevant logs and records.

#### **D.1.9.2 Demonstration of event registration and retrieval**

The auditee must demonstrate the download and installation in a service discovery mode including event registration, retrieval and deletion.

Note: the operation can use simulation for SM-DP+ and LPA.

### **D.2 After the Audit**

Following the audit the audit team will confirm that requests and records are no longer required and can be removed/archived as appropriate by the auditee and deleted by the audit team.

## **Annex E Scope of Audit & Certification when using Cloud Service Provider**

It is possible that a subscription management service provider may outsource operation and management of the data centre hosting the subscription management application to a third party (referred to as a cloud service provider). To provide assurance to other parties in the remote provisioning ecosystem that the overall solution is secure, the cloud service provider site hosting the application and the subscription management service provider managing the subscription management must be SAS-SM certified for the activities that they perform within the scope of the scheme.

The table embedded below indicates what is likely to be in scope for SAS-SM audits at the cloud service provider and the subscription management service provider. It should be considered as a starting point for discussion. The final scope of such audits will depend on the activities performed by each auditee, and shall be agreed between the auditee, the audit team and the GSMA in advance of an audit.



SAS\_SM scope CSP  
v2.xlsx

## Document Management

### E.1 Document History

Version	Date	Brief Description of Change	Editor / Company
1.0	13 October 2014	PSMC approved, first release	Arnaud Danree, Oberthur
2.0	13 May 2015	Transferred ownership to FASG	Arnaud Danree, Oberthur
2.1	16 May 2016	Clarify dry audit prerequisites. Update provisional certification duration to 9 months. Specify minimum certification duration for new sites.	David Maxwell, GSMA
3.0	31 Mar 2017	Updated to reflect use of Consolidated Security Requirements (CSR) and Consolidated Security Guidelines (CSG) for SAS-SM, and extension of SAS-SM to support audit and certification of SM-DP+ and SM-DS solution providers, plus associated cloud service providers.	RSPSAS subgroup
4.0	16 Feb 2018	Remove Certification Body. Specify that audit team makes certification decision. Introduce Appeals Body. Revise cancellation policy. New section on maintaining SAS compliance.	David Maxwell, GSMA
4.1	18 Feb 2019	Clarify that provisional certification is a necessary step towards full SAS-SM certification. Minor general updates in other sections.	David Maxwell, GSMA
5.0	25 Jul 2019	Added process for auditing and certifying supporting sites	David Maxwell, GSMA

### E.2 Other Information

Type	Description
Document Owner	GSMA Fraud and Security Group
Editor / Company	David Maxwell, GSMA

It is our intention to provide a quality product for your use. If you find any errors or omissions, please contact us with your comments. You may notify us at [sas@gsma.com](mailto:sas@gsma.com). <mailto:sas@gsma.com> Your comments or suggestions and questions are always welcome.