SAS Methodology for Subscription Manager Roles

Version 1.0

13 October 2014

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

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 5
1.1 Overview 5
1.2 Scope 5
1.3 Role Definitions 5
1.4 Abbreviations 6
1.5 References 6
2 Audit Process 6
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 Language 9
3 Certification Process 9
3.1 Certification Process 9
3.2 Certification Period 9
3.3 Duration of Certification 11
4 Provisional Certification Process 11
4.1 Provisional Certification Process 11
4.2 Provisional Certification Period 12
4.3 Duration of Provisional Certification 12
4.4 Duration of Provisional Certification Audits 12
4.5 Notification and Publication of Provisional Certification 13
5 SAS-SM Participants 13
5.1 Audit Team 13
5.2 Auditee 13
5.3 Certification Body 13
5.3.1 Oversight of Audits 14
5.3.2 Maintenance of SAS-SM Documentation 14
5.3.3 Appointment and Oversight of Audit Teams 14
5.4 Audit Management 14
5.5 Participant Relationships 14
6 Audit Report Scoring and Assessment 15
6.1 Audit Result 16
7 Costs 17

7.1 First Audit or Renewal Audit 17
7.2 Audit of Central / Corporate Functions 17
7.3 Repeat Audit 18
7.4 Off-Site Review of Improvements 18
7.5 Cancellation Policy 19
8 Final Report 19
Annex A Final Audit Report Structure 20
A.1 First Page: 20
A.2 Subsequent Pages: 20
Annex B Standard Audit Agenda 23
Annex C Standard Document List 26
C.1 Document List 26
Annex D Subscription Management Processing Audit 27
D.1 Before the Audit 27
D.1.1 Preparation 27
D.1.2 Certificate Enrolment 28
D.1.3 Further Preparation for Audit (SM-SR) 28
D.1.3.1 eUICC Registration 28
D.1.3.2 Processing of eUICC Registration eUICC-1 28
D.1.3.3 Profiles 28
D.1.3.4 Processing of Profile Download and Installation for eUICC-1 28
D.1.3.5 Timescales 28
D.1.4 During the Audit (SM-SR) 29
D.1.4.1 Review of Certificate Enrollment and Verification 29
D.1.4.2 Review of eUICC Registration Processing 29
D.1.4.3 Demonstration of Input eUICC 2 Processing 29
D.1.4.4 Review of Profile Download and Installation Processing 29
D.1.4.5 Demonstration of Profile Download and Installation Processing 29
D.1.4.6 Demonstration of Enabling, Disabling and Deletion of Profile 29
D.1.4.7 Demonstration of SM-SR Change 29
D.1.5 Further Preparation for Audit (SM-DP) 30
D.1.5.1 Unpersonalised Profile Creation 30
D.1.5.2 Profile Ordering and Personalisation 30
D.1.5.3 Profile Download and Installation 30
D.1.5.4 Timescales 30
D.1.6 During the Audit (SM-DP) 31
D.1.6.1 Review of Certificate Enrollment and Verification 31
D.1.6.2 Demonstration of Input IF-1 Processing 31
D.1.6.3 Review of Profile Download and Installation Processing 31
D.1.6.4 Demonstration of Profile Download and Installation Processing 31
D.1.6.5 Demonstration of Enabling, Disabling and Deletion of Profile 31
D.2 After the Audit 31
Annex E Document Management 32
E.1 Document History 32

E.2 Other Information 32

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) and Subscription Manager – Data Preparation (SM-DP) solution providers subject their operational sites to a comprehensive security audit. The purpose of the audit is to ensure that SM-SRs and SM-DPs 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 a prescribed GSMA SAS Standard for Subscription Manager Roles [1] and GSMA SAS Guidelines for Subscription Manager Roles [2] by various methods such as document review, interviews and tests in specific areas.

SM-SRs and SM-DPs that achieve a successful audit are certified by the GSMA. This document describes the SAS-SM methodology and processes.

1.2 Scope

SAS-SM audits cover the following areas:

- Security policy, strategy and documentation
- Security organisation and responsibility
- Information security
- Personnel security
- Physical security
- Production data management
- Logistics and production management
- Computer and network management

1.3 Role Definitions

Role	Description
Auditor	A person qualified to perform audits
Auditing Company	Company appointed by the GSMA that provides Auditors.
Audit Team	Two auditors, one each from different auditing companies, jointly carrying out the audit on behalf of the GSMA.
Audit Management	A GSMA team, which administers SAS-SM under the governance of the Certification Body
Certification Body	A committee comprised of GSMA staff and mobile network operator representatives.
Auditee	SM-SR or SM-DP

See section 5. SAS-SM Participants for more detailed explanations

1.4 Abbreviations

Term	Description
eUICC	Embedded UICC
EUM	Embedded UICC Manufacturer
GSMA	GSM Association
MNO	Mobile Network Operator
SAS-SM	Security Accreditation Scheme for Subscription Management Roles
SGP.nn	Prefix identifier for official documents belonging to GSMA SIM Group
SM-DP	Subscription Manager – Data Preparation
SM-SR	Subscription Manager – Secure Routing

1.5 References

Ref	Doc Number	Title
[1]	SGP.07	GSMA SAS Standard for Subscription Manager Roles
[2]	SGP.10	GSMA SAS Guidelines for Subscription Manager Roles
[3]	N/A	GSMA SAS-SM Standard Agreement (from sas@gsma.com)

2 Audit Process

The audit process is described below.

2.1 Audit Setup

2.1.1 Audit Request

If a SM-SR or SM-DP (*Auditee*) wants to be audited it must make a request to *Audit Management.*

The *Auditee* shall specify the scope of assessment (whether SM-SR, SM-DP or both) and the site (or sites if processes are distributed across multiple sites) of assessment. On receipt of the request the *Audit Management* will log the details.

To ensure that the audit can be carried out in the desired timescale, the *Auditee* should give sufficient notice. As a guide:

Notice provided for requested dates	Scheduling target
3 months	within 4 weeks of requested date
2 months	within 6 weeks of requested date
1 month	within 8 weeks of requested date

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 [3] 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 the MNO to be used during the audit. The following options may be considered:

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

The *Auditee* is expected to prepare their systems to enable SM-DP and/or SM-SR 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,
- interview 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*, the *Certification Body* and the *Audit Management,* save for the *Auditee's* right to release a copy to its customers.

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 *Auditors'* recommendations which will be passed to the *Certification Body* for consideration.

2.4 Following the Audit

Following the audit the report is sent to the *Certification Body* by the *Audit Team*. The *Certification Body* checks the report and reviews the *Auditors*' recommendation to decide whether the *Auditee* should be accredited. In the event of a successful audit the GSMA issues a certificate to the *Auditee* within twenty (20) business days of completion of the audit. The *Audit Management*, when informed of the result, will update the audit log.

The audit log is a confidential document maintained within the GSMA.

In the event that the audit findings are disputed, the *Auditee* may lodge a submission with the *Certification Body* within twenty (20) business days of completion of the audit.

2.5 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 Certification Process

The certification process is described below.

3.1 Certification Process

The certification process begins with the first audit or renewal audit at a site.

The certification process ends when:

- Certification is approved by the *Certification Body*.

  or

- The site withdraws from the certification process by either:
  - indicating that it does not intend to continue with the certification process

    or

  - not complying with the Certification Body's requirements for continuing with the certification process following a non-compliant audit result. (Typically, the Certification Body requires the site to arrange a repeat audit or to provide evidence of improvement).

For an existing certified site the certification process can begin up to 3 months before the expiry of the current certificate.

3.2 Certification Period

The certification period begins when the site is certified by the *Certification Body*.

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

The certification period will be determined by the *Certification Body* based on the following criteria:

- For sites with an existing valid certificate:

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

  and

- the certification is approved 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 certification is approved.

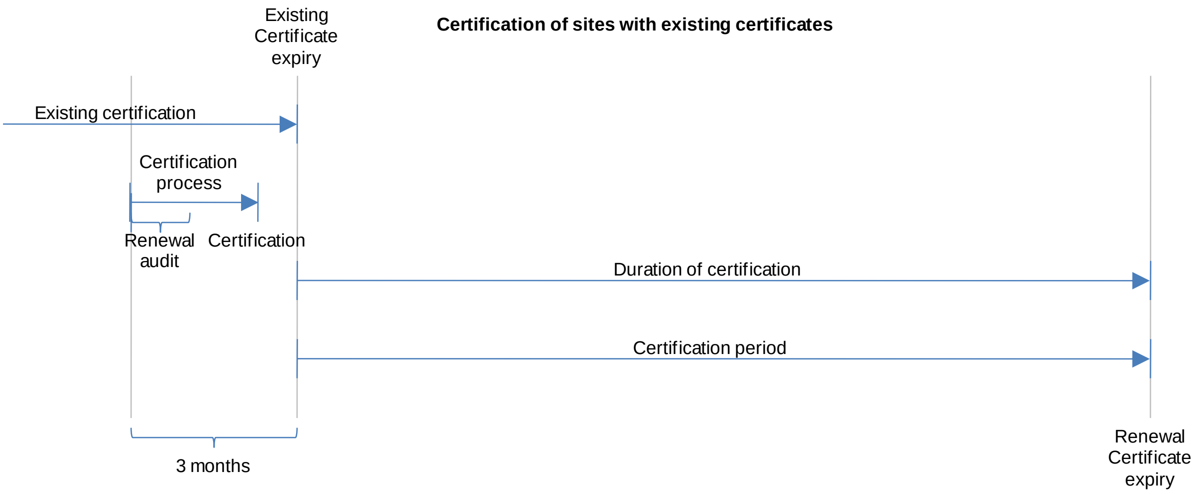
Existing Certificate expiry
Certification of sites with existing certificates
Existing certification
Certification process
Renewal audit
Certification
Duration of certification
Certification period
3 months
Renewal Certificate expiry

Figure 1: Certification of Sites With Existing Certificates

- For sites without an existing valid certificate (new sites, sites where certification has lapsed):
  - the certification period will begin at the time that certification is approved

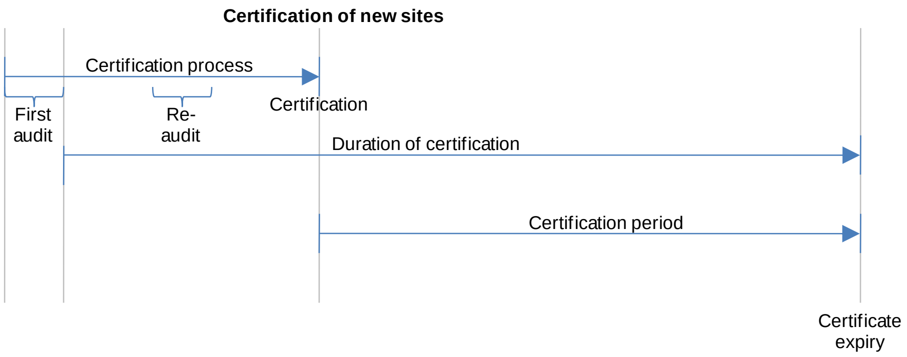

Figure 2: Certification of New Sites

Under the terms of their contract with the GSM Association, all sites must be aware of their obligations relating to notification of significant changes at certified sites within the certification period.

3.3 Duration of Certification

The duration of certification is determined by the *Certification Body* at the time that certification is approved.

The standard duration of certification for sites without an existing valid certificate (new sites, sites where certification has lapsed) is one year.

The standard duration of certification of sites with an existing valid certificate is two years. This duration will be applied in most cases.

The *Certification Body* may, at its discretion, approve certification 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 the first renewal audit).

The *Certification Body* may also, at its discretion, approve certification for two years for sites without an existing valid certificate that perform exceptionally well at the first audit.

4 Provisional Certification Process

SAS-SM is open to both established and new SM-SRs and SM-DPs. The certification process requires that reasonable evidence exists of continued operation of controls. (The guidelines [2] recommend four to six weeks of continuous operation).

To help newly-established sites to achieve certification, two options are offered:

1. Undergo a full audit once SM-SR and/or SM-DP systems and processes are in place at the site,
2. Undergo a provisional certification process (specifically designed for new sites that do not have sufficient operational volumes to submit to a full certification audit).

The *Auditee* will be responsible for choosing their preferred approach.

4.1 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 remote provisioning and management services commence at the site. If the site demonstrates compliance with the security requirements defined in the standard [1] a provisional certification is granted that remains valid for a period of eight months. A non-compliant result at a ‘dry audit’ requires the SM-SR and/or SM-DP 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 for a minimum period of six weeks and it must be undertaken within eight 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 eight 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 SM-SR and/or SM-DP services for a continuous period of six weeks cannot be demonstrated within eight months of the successful ‘dry audit’
- The SM-SR and/or SM-DP chooses to withdraw from the certification process

4.2 Provisional Certification Period

The eight month provisional certification period begins when the site is first certified by the *Certification Body* following the successful ‘dry audit’ or repeat ‘dry audit’ within three months, whichever is later.

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 eight month provisional certification period to ramp-up production.

The provisional certification period ends at the date specified on the site’s SM-SR and/or SM-DP SAS Provisional Certificate of compliance or when the site is fully certified following the successful completion of a ‘wet audit’.

4.3 Duration of Provisional Certification

The duration of provisional certification is fixed at eight months. It is the responsibility of the *Auditee* to ensure the ‘wet audit’ necessary to achieve full certification is undertaken within the eight 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 eight month provisional certification period.

Full certification will run for the normal period, subject to the provisions set out at 3.3 above, and this will be back dated to the date on which the audit to achieve successful provisional certification was concluded.

4.4 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. SM-SR and/or SM-DP processes will also be examined but in the absence of live SM-SR and/or SM-DP 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 7.3 below.

The ‘wet audit’ is conducted over a two day period to review the controls in operation.

4.5 Notification and Publication of Provisional Certification

The GSMA will list provisionally certified production sites at SAS web pages, with an explanation of “provisional certification”.

It is anticipated that operators may ask the GSMA to explicitly confirm certification/provisional certification status of sites and *Audit Management* is willing to support such requests.

5 SAS-SM Participants

The following section describes the roles of the participants during the audit process.

5.1 Audit Team

The *Audit Team* consists of two independent *Auditors*. 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.

5.2 Auditee

The *Auditee* is the SM-SR and/or SM-DP entity to be audited. 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 SM-SR and/or SM-DP 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.

5.3 Certification Body

The *Certification Body* is a committee comprised of GSMA staff and mobile network operator representatives. It has a number of responsibilities.

5.3.1 Oversight of Audits

The *Certification Body* will ensure that audits are properly conducted. The *Certification Body* receives the audit report from the *Audit Team* in order to make decisions on certification of SM-SR and SM-DP entities. These decisions must be notified to the *Audit Management*.

5.3.2 Maintenance of SAS-SM Documentation

The SAS-SM documentation is comprised of the following;

- The standard [1] which contains the security requirements the SM-SR and SM-DP must satisfy in order to be certified.
- The guidelines [2] to guide interpretation and operational application of the standard and
- The Methodology (this document)

These documents are defined and maintained by the *Certification Body*.

Updates will normally arise from an annual review meeting which will involve the *Audit Management*, *Auditors* and subscription manager service provider representatives. Where acute issues are identified ad hoc meetings may be convened to discuss updates to the SAS-SM documentation.

5.3.3 Appointment and Oversight of Audit Teams

The *Certification Body* is responsible for selecting suitably qualified auditing companies to carry out the audits and to ensure that they provide a high-quality service.

5.4 Audit Management

Audit Management is the GSMA (staff) team, which administers SAS-SM under the governance of the *Certification Body*. *Audit Management comprises a number of different tasks such as;*

- Managing audit lifecycle tasks, pre and post audit, for example maintenance of the audit log and list of list of certified and provisionally certified sites
- Contract and financial management between the GSMA and *Auditees* and the GSMA and auditing companies
- Distribution of SMS-SM documentation (this document, the standard [1], and the guidelines [2]) to *Auditees* and *Auditors*.
- Handling general queries for example, via sas@gsma.com.

5.5 Participant Relationships

The relationships between SAS-SM participants are indicated in Figure 3.

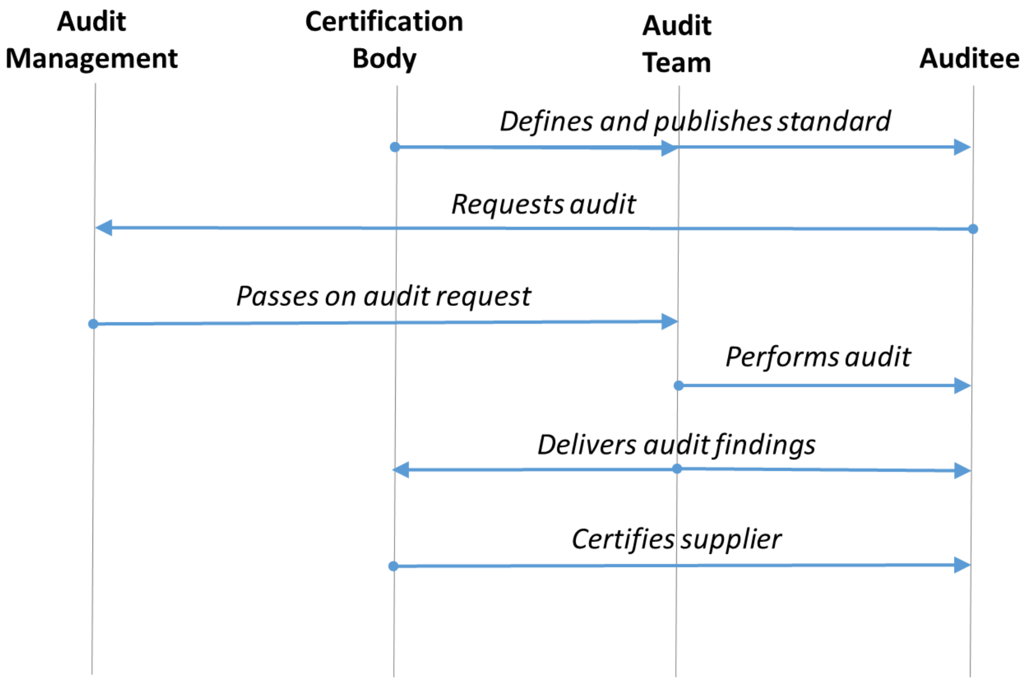

Figure 3: SAS-SM Participant Relationships

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.

Compliant (C)	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:	
	Compliant (C):	In the auditors' assessment the auditee has met the standard to an acceptable level. Comments for further improvement may be offered by auditors.
	Substantially compliant (C-):	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-.
Non-compliant (NC)	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 normally recommend certification 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.

The audit result will typically not recommend certification where one or more area of non-compliance is identified.

After the *Auditee* has submitted to successful re-assessment in the non-compliant areas, an updated audit result will be issued recommending certification.

7 Costs

The costs of an audit differ depending on whether it is a first audit, a renewal audit, or a repeat audit following a non-compliant result at a previous 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 that prescribed in the example outlined in Table 3 below. Quotations for each audit will be sent by the *Audit Management* to the *Auditee* in advance of the audit.

7.1 First Audit or Renewal Audit

The audit duration will depend on the logistics involved but will normally take eight person days for an SM-SR or SM-DP 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 [3] which is sent to the *Auditee* in advance of each audit.

Variable costs such as accommodation and travel will be agreed between the *Auditors* and the *Auditee* on an individual basis with a view to minimising costs while maintaining reasonable standards (see the agreement [3] 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.

7.2 Audit of Central / Corporate Functions

SM-SR and SM-DP entities may be group companies that have a number of SM-SR and/or SM-DP sites. In some cases some functions, knowledge or expertise may be centralised, with common solutions deployed at multiple sites.

SM-SRs and SM-DPs 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 SM-SR SAS and/or SM-DP SAS certified sites within the corporate group. Audits will be undertaken by the *Audit Team* to a scope agreed between the *Auditee*, *Audit Management* and *Audit Team*. Approval will be recommended in an audit report prepared by the *Audit Team*, formally agreed by the *Certification Body*, and notified in writing to the *Auditee*. A formal certificate will be issued to the SM-SR and/or SM-DP entity, but will not be issued to the supporting sites that may be managing centralised solutions on behalf of those entities.

Subsequent audits at SM-SR and/or SM-DP sites will ensure that 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.

7.3 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.

7.4 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:

Administration	1 unit	Applies to all off-site reassessment. Covers updates to report, general communication with Auditee and GSMA
Minor items	1 unit per item	Applies to each audit report sub-section assessed as NC where the scope of improvement is limited to: • Minor changes to individual documents • Changes to individual controls, where changes can be illustrated by simple photographs, plans or updated documents
Major items	4 units per item	Applies to each audit report sub-section assessed as NC where the scope of improvement is:

🟥		• Significant changes to processes (new or existing) with multiple documents or elements to be reviewed • Changes to individual controls, where changes require detailed review or analysis of multiple documents, photographs, plans or video • Changes to multiple linked controls

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.

7.5 Cancellation Policy

A 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 unavoidable expenses incurred by the *Auditors* as evidenced by receipts, as a result of the audit cancellation.

8 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.

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-SR and SM-DP
- Kind of Audit:
  - “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
- 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
- Actions required
- Auditors’ comments
- Appendix A – Scope of Certification
  - Scope, outsourcing and exclusions
- Appendix B – Detailed Results (to be updated to reflect SM-SR and SM-DP standard)

Section	Result of Sub-Section	Auditor Remarks
Policy, Strategy and Documentation Result		
Strategy	C	**+** comment
Documentation	C	
Business continuity planning	NC	**-** comment
Internal Audit	C	
Organisation and Responsibility Result		
Organisation	C	
Responsibility	NC	Comment
Contracts and Liabilities	NC	

Section	Result of Sub-Section	Auditor Remarks
Information Result		
Classification	NC	**-** comment **-** comment
Data and media handling	C-	
Personnel Security Result		
Security in job description	C	Comment
Recruitment screening	C	**+** comment
Acceptance of security rules	C	
Incident response and reporting	C	
Contract termination	C-	
Physical Security Result		
Security plan	C	
Physical protection (for example, windows, doors, glazing, access, lighting, alarms)	NC	
Access control	NC	**-** comment
Security staff	NC	
Internal audit	C	**+** comment
SM-DP and SM-SR Data Management Result		
Data transfer	C	
Access to sensitive data	C	
Cryptographic keys	C-	**-** comment
Auditability and accountability	C	**+** comment **-** comment
Data integrity	C	**+** comment
Internal audit	C	
SM-DP and SM-SR Service Management Result		
Personnel	C	Comment
SM-SR / SM-DP service	NC	
Remote entity authentication	C	
Control, audit and monitoring	C	
Internal audit	C	
Computer and Network Management Result		
Policy	C	
Segregation of roles and responsibilities	NC	
Access control	C	
Network security	C	

Section	Result of Sub-Section	Auditor Remarks
Database security	C	
Virus controls	NC	**-** comment
System back-up	C	
Audit and monitoring	C	
Insecure terminal access	C-	
External facilities management	C	**-** comment
Systems development and maintenance	C	**+** comment
Internal audit	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	• Company / site introduction and overview • Overview of changes to site and security management system • Description of security management system • Review of security policy and organisation • IT infrastructure • Subscription management architecture and infrastructure	Preparation of introductory presentations to include: • Company/corporate background and overview • Site introduction/overview • Production and audit scope • Security management organisation, responsibility and system • IT and information security overview Preparation of copies of appropriate documents for review by the *Auditors* during the audit. 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
2a	• **For SM-SR** • SM-SR system ○ eUICC registration ○ Platform management ○ SM-SR change ○ Control ○ Audit trails	Preparation of detailed data flow diagram showing end-to-end lifecycle of remote management, to include: • Certificate enrolment • eUICC Registration • Management of requests and eUICC status during the SM-SR process Diagrams should include detailed description of controls in place to preserve the confidentiality, integrity and availability of data throughout the process and its auditability. • Preparation of detailed description of SM-SR mechanism used for sensitive data (for example, individual eUICC keys)

2b	• **For SM-DP** • SM-DP system o Platform management o Data Preparation o Profile management o Control o Audit trails	Preparation of detailed data flow diagram showing end-to-end lifecycle of remote management, to include: • Certificate enrolment • Data Preparation and Profile Management o Profile Description management and generation of Un-personalised Profile o Generation of Personalisation Data for the targeted eUICC (for example, Network Access Credentials and other data) based upon input data from the MNO o Generation of Personalised Profiles for the targeted eUICC • Management of requests during the SM-DP process (for example, Platform Management) • Preparation of detailed description of SM-DP mechanism used for sensitive data (for example, individual MNO keys) • Diagrams should include detailed description of controls in place to preserve the confidentiality, integrity and availability of data throughout the process and its auditability.
3	• Key management and data protection o Asset control	Description of how asset is protected during its full lifecycle
4	• IT infrastructure and security • Systems development and maintenance	Preparation of detailed description of system maintenance procedures, to include: • Patch management • System Configuration • Security vulnerabilities management
5	• Physical security concept • Physical security o External and internal inspection o Control room	Preparation of printed copies of site plans and layouts of security systems for use by the *Auditors*. Plans will be used as working documents for annotation by the *Auditors* during the physical security review. Plans will only be used during the audit and will not be removed from the site at any time.
6	• Detailed review of security management system	Preparation of printed copies of documents for review by the *Auditors* (see also document list).

	documentation, including (but not limited to): o Asset classification o Risk assessment o Business continuity plan o Human resources	Documents will only be used during the audit and will not be removed from the site at any time.
7	• Internal audit system • Finalise report, present findings	

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 of the roles, SM-SR, SM-DP or both 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 (SM-SR and/or SM-DP) environment and other networks/zones
  - Critical components within the subscription management (SM-SR and/or SM-DP) environment, including systems, databases, firewalls, HSM and web servers, as applicable
  - Clear and separate identification of respective components for SM-SR and SM-DP systems. Description of associated SM-SR and SM-DP processes and responsibilities, in case a single site is operating both processes.

- 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 and/or SM-DP 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
- 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
- Profile creation, download and installation with SM-SR
- Profile management operations
- 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 other roles, EUM, MNO, SM-DP and/or SM-SR and eUICC is created and available to the SM-SR and/or SM-DP (for a dry audit) (or use existing connected roles for wet or full audit) for the SM-SR and/or SM-DP SAS audit within its systems. The roles may be set up for simulation only (for dry audits), or for production (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 and/or SM-DP 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.

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	Auditee to maintain profile ordering information available for review by the Audit Team Auditee to process the IF-1, Profile creation and Profile Download and Installation. Auditee to maintain output responses for first IF-1 for review by the Audit Team.

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.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 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

E.2 Other Information

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

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