Security Accreditation Scheme for UICC Production - Methodology

Version 5.0

27 July 2016

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

Security Classification: Non-confidential

Copyright Notice

Disclaimer

Antitrust Notice

Table of Contents

1 Introduction

1.1 Overview

The GSMA Security Accreditation Scheme (SAS) for Universal Integrated Circuit Card (UICC) Production (SAS-UP) is a scheme through which UICC suppliers subject their production sites to a comprehensive security audit. The purpose of the audit is to ensure that UICC suppliers have implemented adequate security measures to protect the interests of mobile network operators (MNOs).

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-UP Standard [1] and its supporting documents ([3], [4]) by various methods such as document review, interviews and tests in specific areas. UICC suppliers that demonstrate compliance with the SAS-UP standard are certified by the GSMA.

NOTE: All references to UICCs and UICC suppliers in this document apply equally to Embedded UICCs and Embedded UICC suppliers unless specifically stated otherwise.

1.2 Scope

This scope of this document covers:

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

1.3 Intended Audience

- Security professionals and others within UICC supplier organisations seeking to obtain accreditation under SAS-UP.
- Security professionals and others within organisations seeking to procure UICCs
- SAS Certification Body members
- SAS-UP auditors

1.4 Definitions

Role	Description
Audit Management	A GSMA team, which administers SAS-UP under the governance of the Certification Body
Audit Team	Two auditors, one each from different auditing companies, jointly carrying out the audit on behalf of the GSMA.
Auditee	UICC supplier
Auditor	A person qualified to perform audits
Certification Body	A committee comprised of GSMA staff and mobile network operator representatives.

See section 4 for more detailed explanations of SAS-UP roles.

1.5 Abbreviations

Term	Description
CSR	Consolidated Security Requirements
CSG	Consolidated Security Guidelines
GSMA	GSM Association
MNO	Mobile Network Operator
SAS	Security Accreditation Scheme
SAS-UP	Security Accreditation Scheme for UICC Production
SGP.nn	Prefix identifier for official documents belonging to GSMA SIM Group
SP	Sensitive Process
UICC	Universal Integrated Circuit Card

1.6 References

Ref	Doc Number	Title
[1]	PRD FS.04	GSMA SAS-UP Standard, latest version available at www.gsma.com/sas
[2]	N/A	GSMA SAS-UP Standard Agreement, available from sas@gsma.com
[3]	PRD FS.17	GSMA SAS Consolidated Security Requirements, latest version available at www.gsma.com/sas
[4]	PRD FS.18	GSMA SAS Consolidated Security Guidelines, available to participating sites from sas@gsma.com

2 Audit Process

The audit process is described below.

2.1 Audit setup

2.1.1 Audit request

If a UICC supplier (*Auditee*) wants to be audited, the *Audit Management* (GSMA) should be informed of which site should be audited. On receipt of the request the *Audit Management* logs the details.

To ensure that the audit can be carried out in the requested timescales, the *Auditee* should give sufficient notice of the required audit dates. 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 always remains the responsibility of the *Auditee* to ensure that certification is in place to meet 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 [2] 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* travels to the site to be audited. The sample 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 process of auditing processes and systems for sites seeking certification of the data generation process, the *Audit Team* will make advance arrangements with the *Auditee* to:

- Exchange transport keys
- Submit test input files to the *Auditee*
- Perform data generation for the specified test input file(s)
- Return the corresponding output file(s) to the *Audit Team*

The *Auditee* will be expected to make appropriate arrangements within its systems to enable data generation to take place.

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 half 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, which should take half a day, the *Audit Team* identifies the key individuals to be interviewed during the audit. It is the responsibility of the *Auditee* to ensure the availability of these key 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 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 to the audit report, as outlined in Annex A.

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 the 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 result includes the *Auditors*' recommendations which are passed to the *Certification Body* for consideration.

2.4 Certification

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, updates the audit log.

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

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

2.5 Notification and Publication of Certification

GSMA will list certified and provisionally certified production sites on the SAS website, 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 GSMA is willing to support and respond to such requests.

2.6 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 throughout the audit.

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 likely to be difficult to conduct audit discussions with 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 appropriate evidence of improvement within agreed periods).

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.

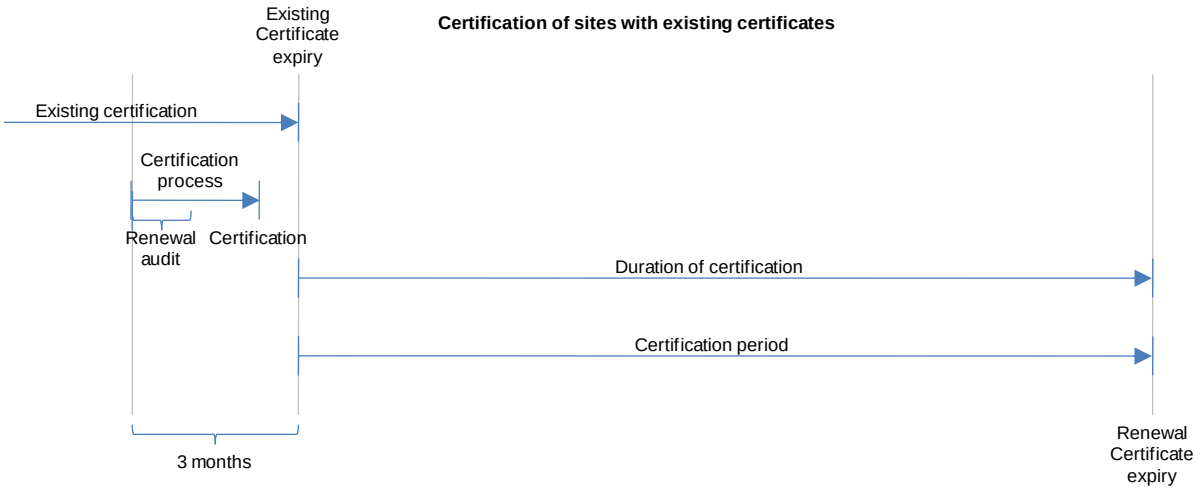

Figure 1 - Certification of sites with existing certificates

- 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

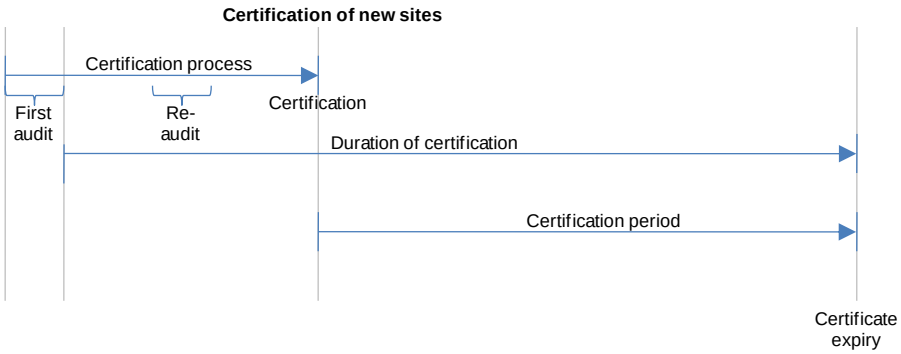

Figure 2 - Certification of new sites

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 1 year. The standard duration of certification of sites with an existing valid certificate is 2 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 changes planned at the site related to security-critical processes or facilities
- A significant reliance on very recently introduced processes or systems where there is little or no history of successful operation of similar or equivalent controls
- A repeated failure to maintain security controls at an appropriate level for the full certification period (as evidenced by significant failure to meet the requirements of the standard [1] at the initial 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.

Sites without an existing valid certificate shall be granted certification for a minimum of seven months from the month during which a fully compliant audit report and certification recommendation is received by the *Certification Body*. This allowance reduces the likelihood that the next renewal audit at the site resulting in 2 year certification is influenced by the most recent re-audit rather than being an assessment of steady-state controls in operation at the site.

4 Provisional Certification Process

SAS is open to both established and new UICC supplier sites.

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

- Undergo a full certification audit once sufficient production is in place at the site to provide evidence of controls in operation.

    - The full certification process requires that reasonable evidence exists of continued operation of controls (the Guidelines **Error! Reference source not found.** suggest 4-6 weeks of continuous operation).

- Undergo a two-stage certification process specifically designed for new sites that do not have sufficient production volumes to submit to a full certification audit. This certification process will initially lead to provisional certification.

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

4.1 Provisional Certification Process

The provisional certification process requires the conduct of two audits at the production site.

The first, which is referred to as a 'dry audit', takes place before live production commences at the site. In order 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-UP Standard. The site should be in a position to begin production for a customer immediately when an order is received, although it is not necessary to have processed live customer orders before or during the audit. The auditors will expect to see that at least one test or live production batch of a reasonable size has been processed prior to the audit, exercising all aspects of the production data flow and asset control mechanism. The auditee should be able to process at least one further batch of a reasonable size during the audit if requested. A batch of a "reasonable size" will normally be expected to demonstrate controls consistent with those for the typical size of a customer order (as a guide, in a mass production environment batches of 1's, 10's or 100's of devices would be unlikely to be considered representative, but 1000's of devices would).

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 nine months. A non-compliant result at a 'dry audit' requires the UICC supplier to remedy identified non-compliances within three months. Successful 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 nine months of the successful 'dry audit'.

Successful completion of a 'wet audit' leads to full certification. The period of this 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 conduct of the initial 'dry audit'
- The 'wet audit' result is non-compliant, and a successful repeat audit is not completed within three months
- Live production for a continuous period of six weeks cannot be demonstrated within nine months of the initial 'dry audit'

- The UICC supplier chooses to withdraw from the certification process

4.2 Provisional Certification Period

The nine 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 completion of a 'dry audit' whether that audit is an initial or repeat 'dry audit'. This differs from the normal certification process, which backdates certification to the initial audit. An exception has been made in the case of provisional certification because the three month period required to make improvements that may be necessary after an initial 'dry audit' would significantly reduce the window of opportunity within the nine month provisional certification period to ramp-up production.

The provisional certification period ends at the date specified on the site's 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 nine months and it is the responsibility of the participating UICC supplier to ensure the necessary 'wet audit' to achieve full certification is undertaken within the nine month provisional certification period.

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

Full certification will run for one year, in accordance with the provisions set out at 3.3 above for sites not holding an existing valid certificate, and this will be back dated to the date on which the first 'wet audit' was concluded.

4.4 Duration of Provisional Certification Audits

The initial 'dry audit' is conducted over a four day period and all controls will be audited. Production processes will also be examined but in the absence of live production it will not be possible to sample test controls. The duration of a repeat 'dry audit' will depend on the areas to be re-audited and will be agreed with the supplier in accordance with section 7.4 below.

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

5 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 key 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 the scheme. 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 UICC supplier that is 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 for disclosing to the *Audit Team* all areas of the site where assets related to UICC production for MNOs 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 UICC supplier sites. These decisions must be notified to the *Audit Management*.

5.3.2 Maintenance of SAS-UP Documentation

The SAS-UP documentation is comprised of the following;

- The Standard [1] which contains the security objectives for SAS-UP.
- The Consolidated Security Requirements (CSR) [3] 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 UICC production. The requirements that apply to UICC production indicated in that document. These are the requirements that the UICC supplier must satisfy in order to be certified.
- The Consolidated Security Guidelines (CSG) [4] to guide interpretation and operational application of the CSR 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 UICC supplier representatives. Where acute issues are identified ad hoc meetings may be convened to discuss updates to the SAS-UP 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 that administers SAS-UP under the governance of the *Certification Body*. *Audit Management* performs 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-UP documentation (this document, the Standard [1], the Consolidated Security Requirements [3], and the Consolidated Security Guidelines [4]) to *Auditees* and *Auditors*.
- Handling general queries for example, via sas@gsma.com.

5.5 Participant Relationships

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

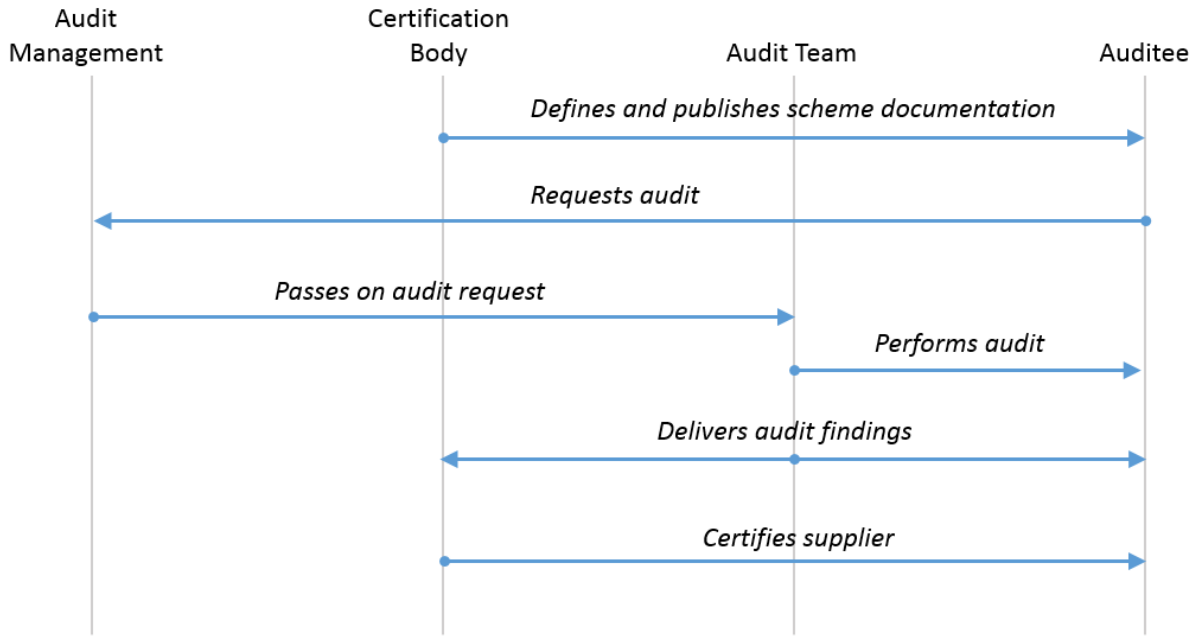

Figure 3: SAS-UP Participant Relationships

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.

<table>
<tr><td rowspan="3">Compliant (C)</td><td colspan="2">indicates that the Auditors' assessment of the site has found that a satisfactory level of compliance with the requirements of 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:</td></tr>
<tr><td>Compliant (C):</td><td>in the Auditors' assessment the Auditee has met the standard to an acceptable level. Comments for further improvement may be offered by Auditors.</td></tr>
<tr><td>Substantially compliant (C-):</td><td>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-.</td></tr>
<tr><td>Non-compliant (NC)</td><td colspan="2">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.</td></tr>
</table>

Table 2 - Assessments possible under SAS-UP

Non compliances and required actions will normally 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 comments made based on the audit findings. 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 report 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 re-audit within 3 months of the non-compliant audit
- Off-site through presentation of evidence of improvement within 3 months of the non-compliant audit

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 recommended 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 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 i.e. 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 each audit.

7.1 First audit or Renewal audit

The audit duration will depend on the logistics involved but will normally take 8 person days. Detailed costs will be quoted in the GSMA SAS standard agreement [2] which is sent to each *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 **Error! Reference source not found.** 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 proportionately between multiple *Auditees*.

7.2 Audit of small and large sites, and sites with limited scope

The size and scope of sites audited will vary. For very small sites or where the scope and scale of production is limited, it may be possible to cover all of the audit areas adequately in a shorter period of time. For very large or complex sites it may be necessary to increase the audit duration to ensure that all of the audit areas can be covered in sufficient detail.

Auditees' perceptions of the size of their site will vary:

- First audits for sites with full scope of certification will be carried out over four days. Where it is the *Auditors*' opinion that the duration of future renewal audits could be

reduced for small sites, or should be increased for large sites, the proposed duration will be documented in the audit report. Future audits may be carried out with the revised duration until such time as the size or scope of production changes and the *Auditors* update their recommendation for the length of renewal audits at the site.

- First audits for sites with very limited scope of certification (e.g. sites only conducting data processing) may be scheduled at less than 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.

7.3 Audit of central / corporate functions

Suppliers may be group companies that have a number of GSM UICC manufacturing sites. In some cases some functions, knowledge or expertise may be centralized, with common solutions deployed on multiple sites.

Suppliers may request that common solutions are audited in detail centrally against the requirements of SAS. Successful audits will result in approval of such solutions for deployment across SAS certified sites. 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 not normally be issued.

Subsequent audits at individual 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 centralized solutions. Renewal will be required every two years.

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

7.4 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 initial audit. The re-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 re-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.

7.5 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:

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.

7.6 Cancellation Policy

A cancellation fee shall be payable by the *Auditee* 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. More details are contained in the SAS-UP standard agreement [2].

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 report structure

A.1 First Page:

- Headline: GSM Association SAS for UICC Production (SAS-UP) Qualification Report
- 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 Following Pages:

- Audit Result and Summary
- Actions required
- *Auditors*' comments
- Appendix A – Scope of Certification
  - Scope, outsourcing and exclusions
- Appendix B – Detailed Results

Section	Result of sub-section	Auditor remarks
Policy, Strategy and Documentation Result		
Policy	C	+ comment
Strategy	C	
Business continuity planning	NC	- comment
Internal audit and control	C	
Organisation and Responsibility Result		
Organisation	C	
Responsibility	NC	Comment
Contracts and liabilities	NC	
Information Result		
Classification	NC	- comment - comment
Data and media handling	C-	
Personnel Security Result		
Security in job description	C	comment

Section		Result of sub-section	Auditor remarks
	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	NC	
	Access control	NC	- comment
	Security staff	NC	
	Internal audit and control	C	+ comment
Certificate and Key Management Result			
	Classification	C	
	Roles and Responsibilities	C	
	Cryptographic key specification	C	- comment
	Cryptographic key management	NC	
	Audit and accountability	NC	- comment
	Incident response and reporting		
Production Data Management Result			
	Data transfer	C	
	Access to sensitive data	C	
	Data generation	C	
	Auditability and accountability	C	+ comment - comment
	Data integrity	C	+ comment
	Duplicate production	C	
	Internal audit and control	C	
Logistics and Production Management Result			
	Personnel	C	comment
	Order management	NC	
	Raw materials	C	+ comment - comment
	Control, audit and monitoring	C	
	Destruction	C-	
	Storage	C	+ comment - comment
	Packaging and delivery	C	
	Internal audit and control	C	

Section	Result of sub-section	Auditor remarks
Computer and Network Management Result		
Policy	C	
Segregation of roles and responsibilities	NC	
Access control	C	
Network security	C	
Systems security	NC	- comment
Audit and monitoring	C	
External facilities management	C	- comment
Internal audit and control	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 standard audits (first and renewal audits) as a guide for *Auditees*. Non-standard audits (principally re-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 key 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	Preparation of introductory presentations to include: • Company/corporate background and overview • Site introduction/overview • Production and audit scope • Security management organisation, responsibility and system • Employee security training • IT and information security overview
2	• IT infrastructure	Preparation of copies of appropriate documents for review by the auditors during the audit, including: • IT security policy • Overall network layout • Production network layout • Firewall configuration policy and rules • Penetration test and vulnerability scan results • User authorisation / account creation process
3	• IT infrastructure (continued)	

	• Production data management
	  ○ Customer data exchange
	  ○ Certificate and key management
	  ○ Data generation profile development and verification
	  ○ Data generation process and control
	  ○ Data exchange for subscription management (where applicable)
	  ○ Personalisation system process and control
	  ○ User access management
	  ○ Audit trails
		Preparation of detailed data flow diagram showing end-to-end lifecycle of production data, to include:
		• Setup of new customers/products
		  ○ Preparation of customer production profiles
		• Certificate and key management
		• Receipt, processing and storage of customer input files
		• Secure generation of data for:
		  ○ Electrical personalisation
		  ○ Graphical personalisation
		  ○ Customer response/output
		  ○ Subscription management
		• Management of personalisation data and UICC status during the production process
		• Completion of the personalisation process
		• Delivery of output files to customers
		• Exchange of data for subscription management
		• Data retention and purging
		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 data generation mechanism used for sensitive personalisation data (e.g. individual subscriber keys)
		The *Auditors* will arrange for exchange of test data files with the site as part of the audit preparation (as described in the SAS Methodology).

4	• Logistics and production ○ Process and asset control	

5	• Detailed review of security management system documentation, including (but not limited to):
	  ○ Asset classification
	  ○ Risk assessment
	  ○ Business Continuity Plan
	• Human resources
		Preparation of printed copies of documents 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.

6	• Physical security concept • Physical security ○ External inspection	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.

7	• Physical security
	  ○ Internal inspection
	  ○ Control room	

8	• 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 the language of the audit, translation facilities must be provided by the *Auditee* within a reasonable timescales. The *Auditors* will seek to minimise such requests, whilst still fulfilling the requirements of the audit.

C.1 Document list

- Overall security policy
- IT security policy
- Security handbook
- Security management system description
- Security management system documentation as provided to employees
- Business continuity plan
- UICC production reconciliation process
- UICC production tracking / reconciliation documentation
- 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 Data processing audit

As part of the audit of the site's data processing system and supporting processes it is preferred that *Auditees* prepare some SAS-specific test data files in advance of the audit date. This document provides a suggested approach; the *Auditee* and *Audit Team* will agree the precise approach for each audit.

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

- Data transfer with MNO customers
- Data protection
- Log files

Using test data files created specifically for the SAS audit avoids any issues with the confidentiality or integrity of live production or customer data.

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

The tests will focus exclusively on data processing and will not involve any physical production.

D.1 Before the audit

D.1.1 Preparation

The *Auditee* should make arrangements to create a customer (or use an existing customer profile) and corresponding orders for the SAS-UP audit within its systems. The customer and orders may be set up for testing only, or for production (although no physical production will take place), as judged appropriate by the site.

It is recognised that different configurations will be used for different customers. One should be selected that is representative of the current production of the site. The audit will focus on those security processes that are typical and/or recommended by the *Auditee* to MNO customers. It is the *Auditee*'*s* responsibility to select appropriate, representative processes.

If more than one production data 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 tests.

Product or customer-related profiles and file formats already in use may be chosen by the *Auditee* for their convenience – e.g. by using/replicating existing customer profiles.

D.1.2 Key exchange

The *Auditee* should initiate its recommended process for secure key exchange, to include:

- Exchange of transport keys for encryption of sensitive data in test output files
- Exchange of encryption keys for test input and output files

D.1.3 Input file exchange

Two input files will normally be submitted to the *Auditee* in advance of the 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 format of the input files will be agreed between the *Auditee* and *Audit Team*, but in most cases could utilise an existing file format used by the *Auditee*.

D.1.4 Processing of input file 1

Auditees should carry out data generation for the first input file in advance of the audit.

NOTE: Input file 2 should not be processed before the audit

D.1.5 Output file exchange

Auditees should return the corresponding output file. The output file should be returned electronically by the *Auditee*'s nominated mechanism or an alternative mechanism if set up cost is implied.

The format of the output file will be agreed between the *Auditee* and *Audit Team*, but in most cases could utilise an existing file format used by the *Auditee*.

D.1.6 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 data processing exercise
Week –2	*Auditee* to communicate requirements for key exchange, file formats and input/output file exchange *Audit Team* to undertake key exchange
Week –1	*Audit Team* to deliver input files *Auditee* to process first input file *Auditee* to return output file for first input file.

D.2 During the audit

D.2.1 Review of key exchange

The *Audit Team* will discuss and review the key exchange process with the *Auditee*, including reference to relevant logs and records.

D.2.2 Review of input file 1 processing

The *Audit Team* will discuss and review the processing of input file 1 with the *Auditee*, including reference to relevant logs and records.

D.2.3 Demonstration of input file 2 processing

The *Audit Team* may request that *Auditees* use input file 2 to provide a live demonstration of the data processing flow (receipt, data generation, output file creation etc.).

D.3 After the audit

Following the audit the *Audit Team* will confirm that data files and records are no longer required and can be removed/archived as appropriate by the *Auditee* and deleted by the *Audit Team* (output file).

Annex E Document Management

E.1 Document History

Version	Date	Brief Description of Change	Editor / Company
3.2.0	24 Jul 2003	Stable version in use.	James Moran, GSMA
3.3.0	5 Sep 2006	Updates to reflect role of GSMC & qualified pass classification, new coversheet	David Maxwell, GSMA
3.3.1	16 Nov 2006	Updated evaluation matrix and audit report content to match security requirements in SAS Standard v.3.2.2	David Maxwell, GSMA
3.3.2	17 Jul 2007	Minor changes to reflect GSMC as GSMA subsidiary that undertakes auditee contracts.	David Maxwell, GSMA
3.4.0	13 Sep 2007	Updated with proposed changes to small site and corporate function audits and QP charging. Approved at SAS annual review 13 Sep 2007	James Messham, FML
3.5.0	11 Sep 2008	Added explicit requirement for openness in SAS Methodology, as agreed at SAS annual review 2008.	David Maxwell, GSMA
3.6.0	14 Sep 2009	Added section for certification process and comments relating to audit scheduling.	James Messham, FML
3.7.0	01 Mar 2010	Document updated to cater for the certification of new manufacturing facilities where production may not already be established	James Moran, GSMA
3.8.0	01 Oct 2010	Updated report scoring and assessment scheme (replace pass/fail terminology with compliant/non-compliant)	David Maxwell, GSMA
3.9	16 Oct 2012	Added details of data process audit, including additional appendix. Minor editorial modifications to update other sections, and application of latest GSMA document template.	James Messham, FML & David Maxwell, GSMA
3.10	5 Mar 2013	Default certification period for new sites reduced to one year.	David Maxwell, GSMA
3.11	10 Apr 2013	Replaced term “smart card” with “UICC” to clarify that non-card form factor (e.g. M2M) products are included in SAS scope.	David Maxwell, GSMA
3.12	30 Oct 2013	Clarified that sites with limited in-scope activities may qualify for audits shorter than the standard duration.	James Messham, FML
3.13	11 Apr 2014	Correction to maximum timeframe allowed for hosting repeat audits.	David Maxwell, GSMA
4.0	23 Apr 2015	Extend certification period following transition from provisional certification. General editorial review & update to reflect creation of SAS for Subscription Management (SAS-SM).	David Maxwell, GSMA
4.1	10 May 2016	Clarify dry audit prerequisites. Update to provisional certification duration to 9 months. Specify minimum	David Maxwell, GSMA

		certification duration for new sites.	
5.0	27 Jul 2016	Update to reflect new Consolidated Security Requirements (CSR) and Consolidated Security Guidelines (CSG) PRDs.	David Maxwell, GSMA

E.2 Other Information

Type	Description
Document Owner	SAS Certification Body
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. Your comments or suggestions & questions are always welcome.