



Security Accreditation Scheme for UICC Production - Methodology Version 10.1 12 April 2023

Security Classification: Non-confidential

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

Copyright Notice

Copyright © 2023 GSM Association

Disclaimer

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

Compliance Notice

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

This Permanent Reference Document is classified by GSMA as an Industry Specification, as such it has been developed and is maintained by GSMA in accordance with the provisions set out in GSMA AA.35 - Procedures for Industry Specifications.

Table of Contents

1	Introduction	5
1.1	Overview	5
1.2	Scope	5
1.3	Intended Audience	5
1.4	Language	5
1.5	Definitions	6
1.6	Abbreviations	8
1.7	References	8
2	Participants	9
2.1	Auditee	9
2.2	Audit Team	9
2.2.1	Observing Auditor	9
2.3	SAS Group	10
2.4	Audit Management	11
2.5	Participant Relationships	11
3	Audit Process	13
3.1	Audit Setup	13
3.1.1	Audit Request	13
3.1.2	Confirmation of Audit Date	13
3.1.3	Contract	13
3.2	Audit Preparation (off-site)	13
3.2.1	Audit Agenda	13
3.2.2	Audit Pre-requisites	14
3.3	Audit Process (on-site)	14
3.3.1	Presentation and Documentation for the Audit Team	14
3.3.2	Information collection	14
3.3.3	Assessment of compliance	14
3.3.4	Preparation of the Audit Report	15
3.3.5	Presentation of the Audit Results	15
3.4	Distribution of the Audit Report	15
3.5	Certification	16
3.6	Appeal	16
3.7	Notification and Publication of Certification	16
4	Certification Process	17
4.1	Certification Process	17
4.2	Certification Period	17
4.3	Duration of Certification	18
4.3.1	Standard durations	18
4.3.2	Exceptions	19
4.3.3	Minimum period of certification	19
4.3.4	Extension of the period of certification	19
5	Scope of certification	20

5.1	Provisional Certification	20
5.1.1	Provisional Certification Process	20
5.1.2	Provisional Certification Period	21
5.1.3	Duration of Provisional Certification	21
5.1.4	Duration of Provisional Certification Audits	22
5.2	Auditing and Certification of Supporting Sites	22
5.2.1	Definition	22
5.2.2	Auditing and Certification Approach	23
	Centralised or Outsourced IT Services	23
5.3	Management of PKI Certificates	24
6	Audit Report Scoring and Assessment	26
6.1	Audit Result	26
7	Maintaining SAS Compliance	28
7.1	Notifiable Events for PKI certificate management	28
7.2	Examples of other Notifiable Events	28
7.2.1	What should be Notified	29
7.2.2	What Would not Normally Require Notification:	29
8	Costs	30
8.1	First Audit or Renewal Audit	30
8.2	Audit of Small and Large Sites, and Sites with Limited Scope	31
8.3	Audit of Central / Corporate Functions	31
8.4	Repeat Audit	31
8.5	Off-Site Review of Improvements	32
8.6	Cancellation Policy	33
8.7	Appeals	33
Annex A	Sample audit agenda	34
Annex B	Audit modules	35
B.1	Audit modules	35
Annex C	Sample required documents list	47
C.1	Document List	47
C.1.1	Security Management System (modules B, C)	47
C.1.2	Key Management (modules J, K)	47
C.1.3	Production (modules O, P)	47
C.1.4	Human Resources (module D)	47
C.1.5	Security Internal Audit System (module U)	48
Annex D	Collection of information	49
Information		49
Annex E	Assessment of compliance	52
E.1	Audit assessment and compliance	52
Annex F	Final Audit Report Structure	56
F.1	First Page:	56
F.2	Following Pages:	56
Annex G	Data Processing Audit	59
G.1	Before the Audit	59

G.1.1	Preparation	59
G.1.2	Key Exchange	59
G.1.3	Input File Exchange	60
G.1.4	Processing of Input File 1	60
G.1.5	Output File Exchange	60
G.1.6	Timescales	60
G.2	During the Audit	60
G.2.1	Review of Key Exchange	60
G.2.2	Review of Input File 1 Processing	60
G.2.3	Demonstration of Input File 2 Processing	61
G.3	After the Audit	61
Annex H	Document Management	62
H.1	Document History	62
H.2	Other Information	63

1 Introduction

1.1 Overview

The GSMA Security Accreditation Scheme (SAS) for UICC Production (SAS-UP) is a scheme through which UICC suppliers subject their production Sites to an 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 the requirements specified in [3] by various methods such as document review, interviews and tests in specific areas. Sites 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 eUICCs and eUICC 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 an SAS-UP Audit
- Audit scoring and Audit 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 for Sites under SAS-UP.
- Security professionals and others within organisations seeking to procure UICCs
- SAS Group members
- Auditors

1.4 Language

The language of the scheme is English.

The language of the scheme will be used for the management and administration of the scheme itself, and for the Audit Process.

The Audit will, in all cases, be conducted in the language of the scheme. The Auditee is responsible to ensure that documents are available in the language of the scheme, as described in Annex C. 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 with knowledge of the business and subject matter to be available to the Audit Team.

1.5 Definitions

Term	Description
Appeals Board	Two Auditors, one each from different GSMA selected Auditing Companies who consider and rule on appealed Audit Results. Auditors for the SAS-UP Appeals Board will be drawn from the SAS-SM Auditing Companies and vice versa.
Audit	The SAS audit carried out by the Audit Team at the Auditee's Site.
Audit Management	A GSMA team, as described in 2.4, which: <ul style="list-style-type: none"> • Manages the scheme documentation. • Appoints the Auditing Companies • Administers SAS-UP • Monitors and assures the quality and consistency of the Audit Process and Audit Team • Issues Certificates to those Sites that the Audit Team assesses as compliant with the requirements.
Audit Process	The overall process followed by the Audit Management and Audit Team to deliver the Audit, as defined in section 3.
Audit Report, Audit Result, Audit Summary and Auditors' Comments	As defined in Annex A.
Audit Team	Two Auditors, one each from different GSMA selected Auditing Companies, jointly carrying out the Audit on behalf of the GSMA, as described in 2.1.
Auditee	An entity involved in the production of UICCs that is seeking SAS-UP certification of its Sites, as described in 2.1.
Auditing Companies	Companies appointed by the GSMA to provide Auditors.
Auditor	A person qualified to perform SAS-UP audits.
Certificate	Certificate issued by the GSMA to the Auditee following demonstration of compliance by the Site with the SAS requirements specified in [3].
Certification Process, Certification Period and Duration of Certification	As defined in section 4.
Dry Audit, and Wet Audit	As defined in section 5.
eUICC	A removable or non-removable UICC which enables the remote and/or local management of Profiles in a secure way. Note: The term originates from "embedded UICC".
Full Certification	SAS certification of Site controls in live operation.
PKI Certificate Management	The process of: <ul style="list-style-type: none"> • Securely generating a key pair and certificate signing request and submitting this to a recognised certificate authority / issuer • Securely storing the key pair and certificate and making them available under appropriate control for the generation of eUICC certificates.

Term	Description
	The definition refers only to the management of the key pair and certificate. The process of generating individual eUICC device certificates is included within the definition of "Generation of Data for Personalisation" for eUICCs.
Primary Site	See "Site".
Profile	A combination of data and applications to be provisioned on an eUICC for the purpose of providing services.
Provisional Certification, Provisional Certification Process, Provisional Certification Period and Duration of Provisional Certification	As defined in section 5.
Renewal Audit	Audit performed towards the end of a period of SAS certification to check continued compliance by the Site with the SAS requirements and provide the basis for a decision to award further SAS certification.
Re-audit	Audit performed to confirm that updated controls implemented by the Auditee following non-compliances found at an earlier Audit are sufficient to satisfy the SAS requirements.
SAS Group	A group of GSMA members and staff (including the Audit Management) that, together with the SAS Auditors, is responsible for maintenance and development of the SAS Standards, Methodologies, Consolidated Security Requirements and Guidelines. See also 2.3.
Scope Extension	Extension of the scope of certification of a Site that already holds some SAS-UP certification.
Secondary Site	See "Site".
Site	Auditee's physical facility and its relevant controls that are subject to the Audit. May be a: <ul style="list-style-type: none"> <li data-bbox="544 1413 1385 1480">Primary Site The main audit site for which the SAS-UP certificate will be issued. <li data-bbox="544 1491 1385 1697">Supporting Site Any independent locations that are subject to separate certification audits. Audit findings will be documented separately in another SAS-UP audit report. Dependence of the Primary Site on the Supporting Site(s) will be noted as part of the certification of the primary site. <li data-bbox="544 1709 1385 1915">Secondary Site Any location directly supporting the activities of a Primary Site and included as part of the same audit process and audit report. Secondary Sites will not be issued with SAS-UP certificates, but will be noted as part of the certification of the Primary Site.
Supporting Site	See "Site".
UICC	The platform, specified by ETSI, which can be used to run multiple

Term	Description
	security applications. These applications include the SIM for 2G networks, USIM for 3G, 4G and 5G networks, CSIM for CDMA, and ISIM (not to be confused with integrated SIM) for IP multimedia services. UICC is neither an abbreviation nor an acronym.

See section 2 for more detailed explanations of SAS-UP roles.

1.6 Abbreviations

Term	Description
CSRG	Consolidated Security Requirements and Guidelines
eUICC	Embedded UICC
GSMA	GSM Association
MNO	Mobile Network Operator
SAS	Security Accreditation Scheme
SAS-UP	Security Accreditation Scheme for UICC Production
SAS-SM	Security Accreditation Scheme for Subscription Management
SGP.nn	Prefix identifier for official documents belonging to the GSMA SIM Group
SP	Sensitive Process

1.7 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.18	GSMA SAS Consolidated Security Requirements and Guidelines, available at www.gsma.com/sas

2 Participants

The following section describes the roles of the participants during the standard Audit Process. The role of the Appeals Board is not considered here (see section 3.6 for details instead).

2.1 Auditee

The Auditee is the participant in the UICC supply chain that is to be subject to Audit.

The Auditee is responsible for:

- Providing all necessary information during the Audit to enable the Audit Team to perform its assessment of compliance with SAS-UP requirements for activities within the scope of certification.
- Ensuring that all key individuals are present when required.
- Delivering a short presentation at the beginning of the Audit describing how it believes that it is compliant with the Standard [1], and the relevant documentation that will be made available to the Audit Team during the Audit.
- Disclosing to the Audit Team all areas of the Site where assets related to UICC production 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.

2.2 Audit Team

The Audit Team consists of two independent Auditors, one from each of the Auditing Companies selected by the GSMA following a competitive tender for the supply of SAS auditing services and in accordance with selection criteria defined by the GSMA.

The Audit Team conducts the Audit by reviewing documentation, conducting interviews with key individuals and carrying out tests in key areas. After the Audit is conducted, the Audit Team writes a report (see 3.3.4).

The independence of the Audit Team is of paramount importance to the integrity of the scheme. It is recognised that the chosen Auditing Companies are professional in the conduct of their business. Where the Auditing Companies previously supplied consultancy services to an Auditee, the GSMA should be informed of this fact prior to commencement of the Audit, and the Auditors performing the Audit should be different individuals to those who have provided the consultancy services.

2.2.1 Observing Auditor

On some audits, an additional observing SAS Auditor may accompany the Audit Team, in order to:

- Support the development of a common understanding of SAS-UP between the Auditing Companies
- Ensure consistency in standards and the Audit Process

- Facilitate sharing of best practice in the Audit approach

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

- A maximum of one observer will be present on any one Audit, except by the prior agreement with the Auditee. Auditees will be under no obligation to agree to any requests for participation of more than one observer.
- The observer will comply with all requirements of the Auditee:
 - Prior to the Audit (e.g. signing NDAs, providing personal information for visitor authorisation).
 - On-site (e.g. behaviour and supervision).
- The role of the observer is to observe. The observation process should not interfere with the conduct of the Audit. Specifically, the observing Auditor should:
 - Not normally engage directly with the Auditee during the Audit Process to ask Audit questions.
 - Only engage in discussion with the Auditee about the observer's own SAS scheme when such discussion will not interfere with the Audit Process.
 - Not present or participate in any discussions during the closing meeting.
 - Not contribute to the preparation of the Audit Report.

To maximise the benefits of the observation process the observer and Audit Team are expected to discuss elements of the Audit Process and approach. Such discussions:

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

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

2.3 SAS Group

The SAS Group is a committee comprised of GSMA staff (including the Audit Management) and members, and representatives of the Auditing Companies. It is responsible for maintenance of the following SAS-UP documentation:

- The Standard [1] which contains the security objectives for SAS-UP.
- The Consolidated Security Requirements and Guidelines (CSRG) [3] which:
 - Provides 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.

- Provides guidelines to guide interpretation and operational application of the requirements
- The Methodology (this document)

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

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

2.4 Audit Management

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

- Selecting suitably qualified Auditing Companies to carry out the audits, in conjunction with the SAS Group as indicated in section 2.3, and ensuring that they provide a high-quality service.
- Ensuring that audits are conducted in accordance with the SAS-UP Methodology and that Audit Reports meet GSMA quality requirements.
- Managing Audit lifecycle tasks, pre and post Audit, for example maintenance of the Audit logs and list of certified and provisionally certified Sites
- Contract and financial management between the GSMA and Auditees and the GSMA and Auditing Companies
- Distribution of SAS-UP documentation (this document, the Standard [1], the Consolidated Security Requirements and Guidelines [3], and other supporting documents to Auditees and Auditors.
- Handling general queries for example, via sas@gsma.com.

2.5 Participant Relationships

The relationships between SAS-UP participants are indicated in Figure 1.

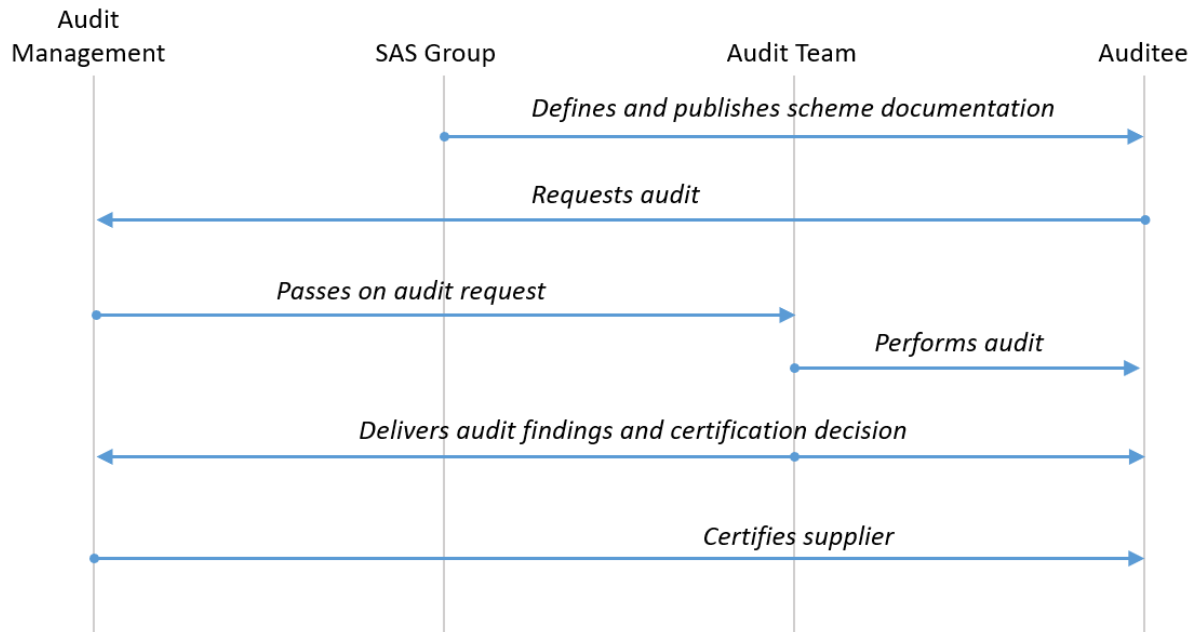


Figure 1: SAS-UP Participant Relationships

3 Audit Process

The Audit Process is described below.

3.1 Audit Setup

3.1.1 Audit Request

If an entity involved in the UICC production chain wishes to be SAS-UP certified, the entity should present itself to the Audit Management as a potential participant in the scheme.

Prior to contacting the Audit Management, the potential participant should have familiarised itself with the current published scheme documentation.

The potential participant should contact the Audit Management to obtain a copy of the Audit Application Form and supporting guidance notes. The completed Audit Application Form should be formally submitted to the Audit Management to request a certification audit. On receipt of the request the Audit Management will log the details of the request.

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

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

Table 1 - Audit Scheduling Guidance

It 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.

3.1.2 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.

3.1.3 Contract

The Auditee enters into a standard agreement [2] with the GSMA and pays the GSMA in advance for the Audit.

3.2 Audit Preparation (off-site)

After Audit dates have been agreed, the Audit Team and Auditee will liaise to agree arrangements for the Audit.

3.2.1 Audit Agenda

A provisional agenda will normally be agreed at least one week before the Audit Team travels to the Site to be audited.

A sample agenda is included in Annex A. The sample agenda includes guidance for Auditees on information that should be prepared for each element of the Audit.

Changes to the agenda may need to be made during the Audit itself, as agreed between the Audit Team and Auditee.

3.2.2 Audit Pre-requisites

To assist in the process of auditing the data generation process (for Sites where this is part of the audit or certification scope), the Audit Team may request that a test/demonstration of the Site's data processing operations is carried out. The process may include 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 a test/demonstration of the data processing 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 G.

3.3 Audit Process (on-site)

The process of conducting the audit follows a number of defined phases.

3.3.1 Presentation and Documentation for the Audit Team

During the first half day of the Audit the Auditee introduces the Site's activities and security management system, and 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.

Based on the Audit agenda, presentation and documentation, the Audit Team agrees the key individuals to be interviewed during the Audit. It is the responsibility of the Auditee to ensure the availability of these key individuals.

3.3.2 Information collection

The Audit Team collects information according to the agreed agenda to form the basis of the assessment of compliance.

The approach to collection of information is described in more detail in Annex D.

3.3.3 Assessment of compliance

Based on the information collected during the Audit, the Audit Team assesses the compliance of the Auditee's controls with the SAS requirements.

The assessment of compliance with the SAS requirements is described in more detail in Annex E.

3.3.4 Preparation of the Audit Report

The Audit Team summarises the findings of the Audit in a report that follows a fixed structure, as described in Annex F, that comprises:

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

Detailed results are provided in an annex to the Audit Report, following the structure of the SAS requirements.

3.3.5 Presentation of the Audit Results

The Audit Report is normally completed during the Audit and delivered to the Auditee on completion of the closing meeting.

During the final half day of the Audit, the Audit Team will normally 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.

The Audit Result includes the Audit Team's decision on certification of the Site, which is passed to the Audit Management.

It is not deemed necessary to have a slide presentation, or to undertake a detailed review of the Audit Report, as part of the presentation of the Audit Results.

3.4 Distribution of the Audit Report

On completion, the Audit Team will distribute the Audit Report to:

- The Auditee for the purpose of internal review and formulation of action plan(s).
- The Audit Management for the purpose of quality control and certification.

Neither the Auditee nor Audit Management will distribute the report to any other party as part of the Audit Process, except:

- In case of an appeal (see below), the Audit Report will also be provided to the Appeals Board.
- For the purpose of Auditor training and SAS quality management, the Audit Report may be provided by the Audit Management to other SAS-UP and SAS-SM Auditors.

The Auditee is free to distribute the report to its customers, but is responsible to ensure that neither the Audit Findings, Audit Result or status of Certification are misrepresented.

3.5 Certification

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

In the event of a successful Audit the Audit Management issues a Certificate to the Auditee within fifteen (15) business days of completion of the Audit.

3.6 Appeal

In the event that the certification decision and/or duration of certification are in dispute the Auditee may lodge a submission with the Audit Management within twenty (20) business days of completion of the Audit. The Audit Management will refer the appeal to the Appeals Board.

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

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

- Review of the Audit Report, focussing on the appealed assessment(s)
- Discussion with the Audit Team and the Auditee

The Appeals Board should not need to visit the Site.

The Auditee may request the members of the Appeals Board to sign an NDA prior to receiving a copy of the Audit Report and other information about the Site.

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

The Auditee and the Audit Team agree to accept the decision of the Appeals Board as final.

A description of the costs associated with the appeals process is included in section 0.

3.7 Notification and Publication of Certification

The GSMA will list certified Sites on the [SAS website](#). The listing will include:

- The Auditee name and the address of the certified Site.
- The scope of certification, including whether the certification is full or provisional.
- The expiry date of the certification.
- Details of any exceptions or specific comments that apply to the Site's certificates.

4 Certification Process

The Certification Process is described below.

4.1 Certification Process

The Certification Process begins with the first full Audit, first Dry Audit (provisional certification) or Renewal Audit at a Site.

The Certification Process ends when:

- A Certificate is issued based on the decision of the Audit Team.

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 Audit Team's requirements for continuing with the Certification Process following a non-compliant Audit Result (Typically, the Audit Team 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.

4.2 Certification Period

The Certification Period begins when a Certificate is issued based on the decision of the Audit Team.

The Certification Period ends at the date specified on the Site's SAS Certificate.

The Certification Period will be determined by the Audit Team 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 awarded before the expiry of the existing Certificate

then

 - the Certification Period will begin at the expiry of the existing Certificate

In all other cases the Certification Period will begin at the time that the Certificate is issued.

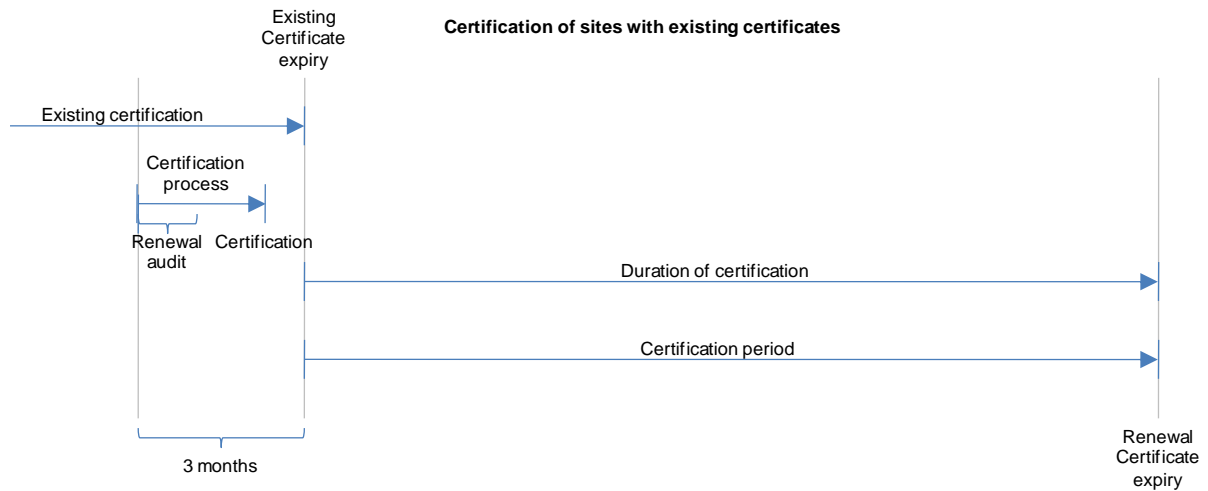


Figure 2 - Certification of Sites with existing Certificates

- For Sites without an existing valid Certificate (new Sites, Sites where certification has lapsed):
 - the Certification Period will begin at the time that the Certificate is issued.

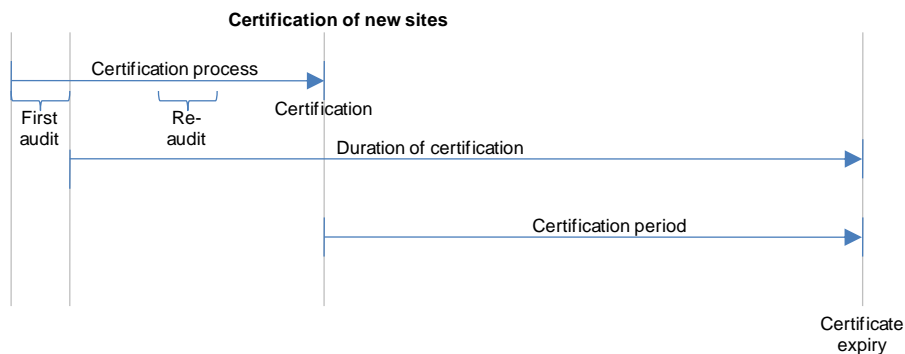


Figure 3 - Certification of new Sites

Under the terms of their contract with the GSMA, all Sites must be aware of their obligations relating to notification of significant changes at certified Sites within the Certification Period, as specified in section 7.

4.3 Duration of Certification

4.3.1 Standard durations

The duration of certification is determined by the Audit Team based on a standard framework:

Type of certificate	Standard duration of certification
First full certification	1 year
Renewal full certification	2 years
First provisional certification	9 months

Table 2 – Standard Durations of Certification

These durations will be applied in most cases.

4.3.2 Exceptions

The Audit Team may, at its discretion, decide that certification should be 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 entire Certification Period (as evidenced by significant failure to meet the requirements of the standard [1] at the initial Renewal Audit).

The Audit Team may also, at its discretion, decide that certification should be for two years for Sites without an existing valid Certificate that perform exceptionally well at the first Audit.

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

4.3.3 Minimum period of certification

Sites without an existing valid Certificate shall, in all cases, be granted certification for a minimum of seven months from the month during which a Certificate is issued. This allowance reduces the likelihood that the next Renewal Audit at the Site resulting in 2-year certification is influenced by the most recent Repeat Audit rather than being an assessment of steady-state controls in operation at the Site.

4.3.4 Extension of the period of certification

The SAS-UP Methodology does not normally allow the GSMA to extend a Site's duration of certification. Sites with an existing Certificate that are planning or making major changes in advance of a Renewal Audit, which could affect the ability to demonstrate the necessary period of evidence, may be eligible for a temporary extension of certification based on the TEA process described in the GSMA SAS remote auditing and certification policy.

Sites wishing to be considered for a temporary extension are encouraged to contact the GSMA as early as possible.

5 Scope of certification

As part of the application process, the Auditee will be required to specify the scope of activities for which it is applying for certification.

The possible scope items for certification are defined as part of the Audit Application Form.

In most cases, Audits take place of Primary Sites leading to Full Certification, however SAS-UP also offers the ability for Audits to take place:

- For Sites that are not yet operating; under the provisional certification scheme.
- Of Supporting Sites that perform specific functions or activities in support of activities at one or more Primary Sites.

SAS-UP certification is also a pre-requisite for Sites wishing to apply for an EUM PKI certificate from one of the GSMA's root CIs. Sites wishing to obtain such PKI certificates will be required to demonstrate compliance with the specific requirements for:

- PKI certification management.

These certification scopes are described in more detail below.

5.1 Provisional Certification

SAS-UP 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 [3] suggest 4-6 weeks of continuous operation).
- Undergo a two-stage Provisional Certification Process specifically designed for new Sites that do not have sufficient production volumes to submit to a Full Certification Audit. This Provisional Certification Process will initially lead to Provisional Certification.

The Auditee will be responsible for choosing its preferred approach.

5.1.1 Provisional Certification Process

The Provisional Certification Process requires 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. 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 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

5.1.2 Provisional Certification Period

The nine-month Provisional Certification Period begins when the Site is first certified.

NOTE: The Provisional Certification Period extends from the date of the successful 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.

5.1.3 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 normally run for one year, in accordance with the provisions set out at 4.3 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. If the Wet Audit extends the scope of existing Full Certification for a Site, and there is significant overlap in controls between the existing and new scope elements, the Audit Team may extend the Full Certification expiry date for the new scope element to match the expiry date of the existing certification (if later).

5.1.4 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 8.4 below.

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

5.2 Auditing and Certification of Supporting Sites

SAS provides auditing and certification on a Site-by-Site basis. However, Sites that participate in the scheme may use additional physical Sites owned and operated by themselves or by third party subcontractors to provide some supporting infrastructure or services within the scope of certification. This section specifies how Supporting Sites are formally handled within the scheme.

5.2.1 Definition

A Supporting Site is one that meets all of the following criteria:

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

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

A Secondary Site is a Supporting Site that is included as part of the same Audit Process and Audit Report as the Primary Site.

5.2.2 Auditing and Certification Approach

The auditing and Certification Process to be followed is slightly different depending on the type of Supporting Site. To date, a single type of Supporting Site has been encountered within SAS-UP, as follows:

Centralised or Outsourced IT Services

Item	Description
Examples	Centralised IT administration, network operations centre, server farm, firewall management
Application form	The application form provides space to provide Supporting Site details and to outline the Site activities.
Audit scheduling and duration	<p>Supporting Sites providing centralised or outsourced IT services may host initial audits scheduled back-to-back or closely scheduled with Primary Site audits. Audits of additional Primary Sites that depend on the Supporting Site's certification are scheduled independently.</p> <p>The Audit duration depends on the Supporting Site activities, and should be agreed on a case-by-case basis with the Audit Team. For back-to-back audits, transfer time between Sites should also be agreed.</p>
SAS agreement and invoicing	<p>The Supporting Site (whether owned by the Primary Site applicant or a third-party subcontractor) must be subject to the terms of the SAS participation agreement. The Site should be specified in the Primary Site's agreement. If the Supporting Site Audit request is received after the Primary Site's agreement has already been executed, then another instance of the agreement specifying the Supporting Site will need to be signed.</p> <p>The Primary Site applicant or its parent company is invoiced for the Audit.</p>
Audit Report	<p>Only the sections of the Audit Report relevant to the activities performed by the Site need to be completed by the Audit Team. Relevant contextual information about the Supporting Site Audit should be provided within all Audit Reports. The information provided should include Site location(s), dates and duration, Audit type and approach, summary of activities performed at each Site, any relevant Audit history, and explanatory notes in relation to how the report has been prepared and any deviations from standard Audit practice if necessary.</p>
SAS Certificate and website listing	<p>The Supporting Site name and address are mentioned on the SAS Certificate of the Primary Site(s) to which they provide support.</p> <p>If the certification expiry dates of a Primary Site and a supporting backup Site are different, the GSMA will include both expiry dates on the Certificate. This approach will trigger reissue of Certificates to Primary Site(s) by the GSMA each time a Supporting Site with a different certification expiry date renews certification.</p> <p>If the certification of a Supporting Site lapses, the GSMA may withdraw the SAS certification of the associated Primary Site(s).</p>

5.3 Management of PKI Certificates

Certification for management of PKI certificates is slightly different to other elements of SAS-UP Audit scope.

SAS-UP certified Sites may make use of eUICC Manufacturer (EUM) PKI test or live certificates that are issued as part of the GSMA ecosystem, or other, non-GSMA PKIs (e.g. national, supplier or product-specific PKIs). Controls are likely to be the same, or very similar, in all cases; however, SAS-UP certification for PKI certificate management focusses specifically on a Site's compliance with the requirements for use of live PKI certificates as part of the GSMA PKI ecosystem.

SAS-UP certification with this scope is one pre-requisite for a Site to apply for a GSMA EUM PKI certificate from a GSMA-appointed Certificate Issuer.

Any Site that demonstrates an appropriate level of compliance with the relevant requirements during an SAS-UP audit may be certified with PKI certificate management within scope, however certification will distinguish between those Sites that have:

- Demonstrated SAS-UP compliance without GSMA PKI live certificates in use (i.e. either via test/self-signed PKI certificates or via non-GSMA PKI certificates).
- Demonstrated SAS-UP compliance with GSMA PKI certificates in use.

SAS-UP certification will be indicated as shown in Table 3.



Value	Symbol	Criteria
GSMA PKI Ready		Site has demonstrated compliant controls for PKI certificate management, either via <ol style="list-style-type: none"> test/self-signed PKI certificates (controls audited 'dry', i.e. no live operations) or certificates used in live operations issued by non-GSMA CAs.
GSMA PKI Live		Site has demonstrated compliant controls with GSMA PKI live certificate(s) in use.

Table 3 – Possible values for “Management of PKI Certificates”

In all cases, a Site must first be certified as “GSMA PKI Ready” before being issued with a GSMA PKI live certificate to act as an eUICC manufacturer. Once the first GSMA PKI EUM live certificate has been issued, the Site's SAS-UP certification can be updated to “GSMA PKI Live” following a further successful audit of activities.

SAS-UP certification with “GSMA PKI Ready” or “GSMA PKI Live” certification will be awarded as shown in Table 4.









		PKI Certificate(s) held at time of audit			SAS-UP status on successful completion of audit	
Audit type		Test/self-signed only (no live operations)	GSMA PKI live certificate	Non-GSMA PKI used in live operations	Certification Status	Certification duration
1	Initial ⁽ⁱ⁾	X	Not available			(ii)
2		N/A		X		(iii)
3	Wet	N/A		X		(iii)
4			X			
5			X	X		
6	Renewal	N/A		X		(iii)
7			X			
8			X	X		
(i)	Initial audit of PKI certificate management, carried out as part of a first audit for a new Site or as a renewal or scope extension audit for an existing SAS-UP certified Site. The duration of certification will be dictated by whether this is a new activity (equivalent to a dry audit under the provisional certification scheme) or an existing activity (equivalent to full certification).					
(ii)	Certification is valid until provisional certification expiry date of other scope elements audited during dry audit (typically 9 months)					
(iii)	Certification is valid until certification expiry date of other full certified scope elements (1 year following first full or wet audit, 2 years following renewal audit)					

Table 4 - SAS-UP PKI certification lifecycle

6 Audit Report Scoring and Assessment

The Audit Report (see section 3.3.4) 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 5.

Compliant (C)	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:
	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 5 - 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 specify that certification will be awarded by the GSMA without further improvement.

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

- On-site during a Repeat Audit 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 awarded where one or more areas of non-compliance are identified.

Once the Auditee has submitted to successful re-assessment of the issues identified an updated Audit Report will be issued specifying that certification will be awarded.

7 Maintaining SAS Compliance

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

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

7.1 Notifiable Events for PKI certificate management

Sites that are SAS-UP certified for PKI certificate management must notify the GSMA of some specific events that are directly related to that activity:

- Revocation of EUM certificate(s)

If any live EUM PKI certificate (whether issued as part of the GSMA or other PKI) is revoked by the relevant certificate issuer, by the Site itself or by another party this must be notified to the GSMA. Certificates used solely for test purposes that are revoked at end-of-life are excluded from this requirement.

- Security incidents

Any security incident involving personnel, processes, physical locations, systems or sensitive materials related to management of EUM PKI certificates or key pairs must be notified to the GSMA, even if the security incident itself does not relate to certificates or key pairs within the scope of SAS-UP certification.

- Transfer of GSMA PKI EUM certificate private keys.

Any activity involving the transfer of GSMA PKI EUM certificate private keys to a new physical location (e.g. transfer between sites or relocation of key management systems or HSMs) or logical transfer or replication to a new key management system or HSM must be notified to the GSMA.

Transfer of GSMA PKI EUM certificate private keys must always be carried out in accordance with the requirements of section 6.6 of [3].

7.2 Examples of other Notifiable Events

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

7.2.1 What should be Notified

- Revisions to policy or procedure that change controls audited within the scope of the SAS Audit, e.g.:
 - A change from dual control to single control
 - Removal of a procedural count or control of sensitive assets
 - Removal of a security screening step for new employees.
 - Reduction in the frequency of a risk assessment process, security awareness training programme or IT vulnerability scan.
- Changes to the responsibility for security management at the Site.
- Changes to the physical environment where sensitive processes are located or housed, e.g.:
 - Relocation of sensitive processes to new premises or alternative locations within the existing certified Site.
 - Enlargement or other physical change to a room or workshop containing a sensitive process
 - Changes to the physical construction of areas of the Site where sensitive processes are carried out.
- Changes to the architecture of the networks used for sensitive processes, or to the security level of networks where sensitive processes take place.

7.2.2 What Would not Normally Require Notification:

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

8 Costs

The costs of an Audit differ depending on whether it is a first Audit, a Renewal Audit, or a Re-Audit following a non-compliant result at a previous Audit. Costs may also depend on the exact scope of activities and 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 7 below. Quotations for each Audit will be sent by the Audit Management to the Auditee in advance of each Audit.

8.1 First Audit or Renewal Audit

The Audit duration will depend on the logistics involved and the scope of certification but will normally be based on the following.

		UICC	eUICC ⁽²⁾
Scope of activity	Production ⁽¹⁾ only (no data generation)	8 person-days ⁽³⁾	
	Production ⁽¹⁾ and data generation	8 person-days ⁽³⁾	10 person-days ⁽³⁾
	Data generation only	5 person-days ⁽³⁾	7 person-days ⁽³⁾

Table 6 – Influence of Scope on Audit Duration

- Note 1: “Production” includes personalisation of the UICC and any value-added fulfilment activities carried out at the Site.
- Note 2: Sites requiring certification as an eUICC manufacturer (EUM), where personalisation and/or data generation for eUICC personalisation takes place, will require a longer Audit to consider the processing of data for subscription management.
- Note 3: Each Audit is conducted by two Auditors on-site simultaneously; therefore the duration of the Audit will be half the time in person-days (i.e. 8 person-days = 4 Audit-days with 2 Auditors).

It is the Auditee’s responsibility to notify the Audit Management of the Audit scope at the time of application for each Audit. A proposed Audit duration will be agreed in advance and detailed costs will be quoted in the GSMA SAS standard agreement [2] which is sent to each Auditee.

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 [2] 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.

8.2 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:

- In all cases, Auditees should notify the Audit Management of the Audit scope at the time of application for first Audit. A proposed Audit duration will be agreed in advance of the first Audit.
- First audits for Sites will be carried out based on the standard structure as described in section 8.1. 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.
- The proposed duration for subsequent Renewal Audits will be documented by the Auditors in the Audit Report.

8.3 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-UP certified Sites. Audits will be undertaken by the Audit Team to a scope agreed in advance between the Auditee, Audit Management and Audit Team. Approval will be granted via an Audit Report prepared by the Audit Team, issued to the Audit Management, and notified in writing to the Auditee. 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.

8.4 Repeat Audit

The costs for a Re-Audit will depend on the required duration of the Re-Audit, which in turn depends on the number of areas assessed as non-compliant during the initial 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 the GSMA

and the Auditee, multiplied by the number of Auditor days required to conduct the Repeat-Audit.

Re-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 Re-Audits.

8.5 Off-Site Review of Improvements

Where the Auditors' recommendation at an 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:

$$\text{Total units} = \text{Administration} + \text{Minor items} + \text{Major items}$$

where:

Administration	1 unit	Applies to all off-site reassessment. Covers updates to report, general communication with Auditee and the 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: <ul style="list-style-type: none"> • 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: <ul style="list-style-type: none"> • 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 7 - Estimating Auditor Time for Off-Site Review of Improvements

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

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

8.6 Cancellation Policy

An Audit 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 certain unavoidable and non-recoverable expenses (e.g. visa application fees) incurred by the Auditors where less than 60 days' notice of cancellation, from the date that an Audit is due to commence, is given by the Auditee, or where the GSMA cancels the Audit as a result of non-compliance by the Auditee with the terms of the SAS-UP standard agreement. Such expenses shall be evidenced by receipts. More details are contained in the SAS-UP standard agreement [2].

8.7 Appeals

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

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

Annex A Sample audit agenda

The following agenda proposes a mapping of audit modules (as described in Annex B) onto audit sessions for standard audits (First and Renewal Audits) as a guide for Auditees. Non-standard audits (re-audits; audits with extended or reduced scope) may have different duration and a specific agenda will be agreed.

The agenda is split into sessions which will normally be carried out in the sequence set out below. Auditees should ensure that appropriate information has been prepared to facilitate the Audit Process (see module details in B.1).

For each part of the Audit the Auditors will normally expect to:

- Discuss the controls in place (documentation, processes, systems) with responsible personnel to understand the security management system. Discussions will typically take place within a meeting room environment.
- Review and validate controls on-site where the sensitive processes are carried out.

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.

Audit day	Morning session		Afternoon session	
	Modules			
1	A	Introduction	Q, R	IT policy and networks
	B	Documents		
	E	Awareness training		
2	S, T	IT systems	L, M, N	Data processing
	J, K	Key management		
3	O, P	Production security	F, G	Physical security
	D	HR		
4	H, I	Physical security	U	Internal audit
	C	Risk assessment BCP	V	Closing meeting

Annex B Audit modules

The audit agenda will typically comprise a number of audit sessions that will be agreed with each auditee based on the scope of the audit. During each session, one or more audit modules will be planned. The modules will typically be conducted across the audit sessions to allow the auditor team to build their understanding of controls, then test/validate them. The table below is intended to help auditees understand the contents of each module, how they relate to the requirements, how the auditee should prepare to simplify the audit process (see also the sample document list in Annex C). A sample mapping of modules onto a typical agenda for a 4-day audit is included in Annex A.

B.1 Audit modules

Module	FS.18	Outline agenda	Assessment source (ref. Annex E)	Suggested Auditee preparation	Auditee personnel
A		<ul style="list-style-type: none"> Company / Site introduction and overview. Overview of changes to Site and security management system. Description of security management system. 	Auditee presentation [D, S]	Preparation of introductory presentations to include: <ul style="list-style-type: none"> Company/corporate background and overview. Site introduction/overview. Confirmation of Audit scope and sensitive processes carried out at the Site. Security management organisation, responsibility and system. IT and information security overview. 	Key members of security organisation
B	1.1 2.x 3.x	<ul style="list-style-type: none"> Review of security policy and organisation. Detailed review of security management system documentation. 	Auditee presentation Off-line review by Audit Team Question and answer [D, S, P, L]	Preparation of printed copies of security management system documents, as described in Annex C.	Key members of security organisation

Module	FS.18	Outline agenda	Assessment source (ref. Annex E)	Suggested Auditee preparation	Auditee personnel
C	1.2 1.3	<ul style="list-style-type: none"> Risk assessment Business Continuity Plan 	Q+A [D, S, L]	Preparation of copies of documents for review by the Auditors (see also document list). Evidence of the most recent security risk assessment completed. Business continuity training and testing records.	Risk assessment responsible representative BCP responsible representative
D	4.x	<ul style="list-style-type: none"> Human resources 	Q+A Presentation of requested samples [D, S, L]	Description of processes for: <ul style="list-style-type: none"> Security screening as part of on-boarding process. Regular re-screening of personnel. Defining security responsibilities within job description. Security and confidentiality within legal documentation (e.g. employment contracts). Security incident reporting and whistleblowing. Disciplinary action. Off-boarding at end of employment. Sample employee files to provide evidence of controls being applied (Audit Team will specify the requested files for the HR team to present). 	HR representative Security manager
E	4.3	<ul style="list-style-type: none"> Security awareness training 	Q+A	<ul style="list-style-type: none"> Copies of employee security 	Security manager / HR

Module	FS.18	Outline agenda	Assessment source (ref. Annex E)	Suggested Auditee preparation	Auditee personnel
			[D, S, P, L]	awareness training materials. Employee security awareness training records for the past 2 years.	/ training as appropriate
F	5.x	<ul style="list-style-type: none"> Physical security 	<p>For physical security, the scope of the audit will be primarily based around the activities at the site within the scope of SAS-UP certification (UICC/eUICC data generation, personalisation and post-personalisation packaging, and any key and certificate management related to those activities)</p> <p>The audit will consider all areas involved in:</p> <ul style="list-style-type: none"> The storage and processing of relevant assets: <ul style="list-style-type: none"> Information (including production data) IT Production Cryptographic keys Operational management of systems and components related to: <ul style="list-style-type: none"> Activities within the scope of SAS-UP certification The management of logical and physical security controls for activities within the scope if SAS-UP certification. <p>Specifically, this will include the:</p> <ul style="list-style-type: none"> Overall site perimeter. Building perimeter for each building housing activities or assets within the scope of SAS-UP certification. Floors or areas within each building housing activities or assets within the scope of SAS-UP certification. The areas of normal or potential access between the site perimeter and building perimeter. The points of normal or potential access between the building perimeter and relevant floors or areas. 		

Module	FS.18	Outline agenda	Assessment source (ref. Annex E)	Suggested Auditee preparation	Auditee personnel
			<ul style="list-style-type: none"> Activities within areas where site security is managed, monitored or administered, including: <ul style="list-style-type: none"> Security control rooms. Access / badge administration offices. Security reception desks. 		
	5.x	<ul style="list-style-type: none"> Physical security concept 	Q+A [D, S, P, C, T, L, R]	Detailed plans showing: <ul style="list-style-type: none"> The mapping of security levels onto the site's physical layout. The location of all physical security hardware within the environments including: <ul style="list-style-type: none"> CCTV cameras. Alarm system sensors. Points of entry / exit (personnel access, vehicle access, materials transfer, emergency exits). Access control hardware (access card readers, biometric sensors etc). Documentation of the physical security concept: <ul style="list-style-type: none"> Security levels: <ul style="list-style-type: none"> Level definitions. Baseline security controls (for access control, CCTV, alarm systems) applied at each security level. 	Security manager Physical security supervisor and/or technical systems representative

Module	FS.18	Outline agenda	Assessment source (ref. Annex E)	Suggested Auditee preparation	Auditee personnel
				<p>Presentation of the implementation of the concept for areas within the scope of the SAS-UP audit (as described below).</p> <p>Presentation of management controls for physical security elements:</p> <ul style="list-style-type: none"> • CCTV: <ul style="list-style-type: none"> • CCTV layout concept. • Recording and retention policies. • Operational system checks. • Preventative and reactive maintenance. • Alarm system: <ul style="list-style-type: none"> • Alarm system concept. • Arming and disarming policies. • Alarm review and response process. • Operational system checks. • Preventative and reactive maintenance. • Access control: <ul style="list-style-type: none"> • Operational system checks • Preventative and reactive maintenance. • Lifecycle management of access for permanent and temporary employees, 	

Module	FS.18	Outline agenda	Assessment source (ref. Annex E)	Suggested Auditee preparation	Auditee personnel
				contractors, visitors etc, to include: <ul style="list-style-type: none"> • Policies for granting access. • Processes for application, approval, granting, modification, revocation and removal of access. • Management of physical access tokens (access cards / badges). <ul style="list-style-type: none"> • Control of unauthorised use. • Processes for periodic review and re-approval of access rights. • Monitoring and response for access control events. <ul style="list-style-type: none"> • Forced opening. • Denied access. • Door open too long. • Anti-passback. 	
G	5.x	<ul style="list-style-type: none"> • Physical security <ul style="list-style-type: none"> • External inspection <ul style="list-style-type: none"> • Physical protection at the site boundary. • Control of authorised and unauthorised access. • Deployment of physical 	Live audit [P,O,C,T,L,R]	Plans (as above). Preparation of appropriate test equipment to enable physical security system components (e.g. alarm sensors, emergency exits) to be tested during the live audit. The ability to simultaneously view	Security manager Physical security supervisor

Module	FS.18	Outline agenda	Assessment source (ref. Annex E)	Suggested Auditee preparation	Auditee personnel
		security systems (CCTV, alarms, access control).		video from the live audit location with streams from the alarm console(s) may allow significant time to be saved if this can be achieved reliably.	
H		<ul style="list-style-type: none"> Internal inspection <ul style="list-style-type: none"> Physical protection within the areas of the site linked to the scope of SAS-UP certification. Control of authorised and unauthorised access. Deployment of physical security systems (CCTV, alarms, access control). 			Security manager Physical security supervisor
I		<ul style="list-style-type: none"> Security control room operations <ul style="list-style-type: none"> Validation of physical security system operation. Evaluation of control room operating procedures and discipline of personnel. 			Security manager Physical security supervisor
J	6.x	<ul style="list-style-type: none"> Key management. Overview of key storage mechanisms in use for UICC production activities. Processes for secure generation and exchange of keys with other entities in the production chain. Processes for secure generation and management of keys for internal protection of data. 	Q+A Presentation of samples [D, S, P, C, T, L, R]	Preparation of key management process documentation and supporting evidence, including: <ul style="list-style-type: none"> Process documentation. Roles and responsibilities. Training records. Key management activity records. Technical details of key storage mechanisms. 	Security manager Key manager Key administrator(s) Technical system architect / developer representative

Module	FS.18	Outline agenda	Assessment source (ref. Annex E)	Suggested Auditee preparation	Auditee personnel
		<ul style="list-style-type: none"> Examination of physical storage facilities for keys/key components (key safes or similar). Examination of key management system / HSM configuration. Review and reconciliation of sample keys. 		The Auditors may request completion of a demonstration key ceremony during the Audit using test/dummy keys.	
K	6.x	<ul style="list-style-type: none"> Key management. 	Live audit [P,O,C,T,L]	Sample systems and checks to be agreed during audit.	Security manager Key manager Key administrator(s) Key custodian(s)
L	7.x 11.x	<ul style="list-style-type: none"> Data generation <ul style="list-style-type: none"> Development and management of data generation profiles. Secure exchange of data (input files, output files, production data etc.). Generation of sensitive data. <ul style="list-style-type: none"> Authentication and other keys. Device certificates. Protection of sensitive data (encryption and access control). Prevention of duplicate production. Production audit trails. 	Q+A [D,S,P,C,T,L,R]	Preparation of detailed data flow diagrams and supporting information to show end-to-end lifecycle of production data, to include: <ul style="list-style-type: none"> Exchange of: <ul style="list-style-type: none"> Input files / data. Personalisation data. Response / output data. With other entities in the production chain. <ul style="list-style-type: none"> Generation / processing of data for: <ul style="list-style-type: none"> Electrical personalisation. Graphical personalisation. Customer response/output. 	Security manager Data processing team representative Technical system architect / developer representative
M	7.x	<ul style="list-style-type: none"> Production data management. 	Q+A	<ul style="list-style-type: none"> Management of personalisation data and UICC status during and 	Security manager

Module	FS.18	Outline agenda	Assessment source (ref. Annex E)	Suggested Auditee preparation	Auditee personnel
	11.x	<ul style="list-style-type: none"> • Receipt and transfer of personalisation data into the production network. • Protection of sensitive data (encryption and access control). • Control of personalisation. • Repersonalisation flow. • Prevention of duplicate production. • Production audit trails. 	[D, S, P, C, T, L, R]	<p>after the personalisation process.</p> <p>Diagrams should include detailed description of controls in place to preserve the confidentiality, integrity and availability of data throughout the process and its auditability.</p> <p>Preparation of detailed description of data generation mechanism used for sensitive personalisation data (e.g. individual subscriber keys).</p> <p>Overview of controls in place to prevent duplicate production occurring.</p> <p>The Auditors may arrange for exchange of test data files with the Site as part of the Audit preparation (as described in the SAS-UP Methodology).</p>	<p>Data processing team representative</p> <p>Production data management representative</p> <p>Technical system architect / developer representative</p>
N	7.x 11.x	<ul style="list-style-type: none"> • Production data processing. 	<p>Live audit</p> <p>[P, O, C, T, L]</p>	<p>Sample systems and checks to be agreed during audit.</p>	<p>Data processing team representative</p> <p>Production data management representative</p>
O	9.x	<ul style="list-style-type: none"> • Production process. • Storage of materials. • Asset control within the personalisation process. • Repersonalisation. 	<p>Q+A</p> <p>[D, S, T, L, R]</p>	<p>Presentation of the production process flow describing controls in place for the personalisation process, including:</p> <ul style="list-style-type: none"> • Incoming materials flow for devices prior to personalisation, including storage and stock 	<p>Logistics manager</p> <p>Logistics supervisor(s)</p> <p>Production manager</p> <p>Production supervisor(s)</p>

Module	FS.18	Outline agenda	Assessment source (ref. Annex E)	Suggested Auditee preparation	Auditee personnel
		<ul style="list-style-type: none"> • Post-personalisation packaging. • Finished goods storage. • Reject handling and destruction. 		<p>control.</p> <ul style="list-style-type: none"> • Control of quantity of devices entering environment where the personalisation process is carried out. • Embedded cards or embedded form-factor devices for dedicated personalisation workshops. • White or printed card bodies for combined card body / personalisation workshops. • Control of quantity of good, reject and unused devices at end of personalisation process. • Control of quantity of good, reject and unused devices at end of any post-personalisation packaging process. • Confirmation of point of final control and sealing of finished, personalised UICCs. • Materials flows for: <ul style="list-style-type: none"> • Finished, sealed personalised UICCs. • Surplus unused devices from the personalisation process. • Rejects from the personalisation and/or post- 	

Module	FS.18	Outline agenda	Assessment source (ref. Annex E)	Suggested Auditee preparation	Auditee personnel
				<p>personalisation packaging processes.</p> <ul style="list-style-type: none"> Remake processes for devices: <ul style="list-style-type: none"> Rejected during the personalisation process. <p>Rejected after the personalisation process.</p>	
P	9.x	<ul style="list-style-type: none"> Production process. 	<p>Live audit [P,O,T,L]</p>	<p>Sample systems and checks to be agreed during audit.</p>	<p>Logistics manager Logistics supervisor(s) Production manager Production supervisor(s)</p>
Q	10.1 10.2	<ul style="list-style-type: none"> IT security policy 	<p>Q+A [D,S,P]</p>	<p>Preparation of copies of appropriate documents for review by the Auditors during the Audit, including: IT security policy.</p>	<p>IT security business owner/representative</p>
R	10.5	<ul style="list-style-type: none"> IT network security 	<p>Q+A Presentation of requested samples [D,S,P,C,T,L,R]</p>	<ul style="list-style-type: none"> Overall network layout. Production network layout. Firewall configuration policy and rules. <ul style="list-style-type: none"> Samples of documentation for recent firewall rule change. Samples of documentation for recent firewall rule review. <p>Penetration test and vulnerability scan results.</p>	<p>Network security team representative System administrator(s)</p>
S	10.6 10.3	<ul style="list-style-type: none"> IT systems security 	<p>Q+A</p>	<ul style="list-style-type: none"> System hardening checklists. 	<p>Systems security team</p>

Module	FS.18	Outline agenda	Assessment source (ref. Annex E)	Suggested Auditee preparation	Auditee personnel
			Presentation of requested samples [D,S,P,C,T,L,R]	<ul style="list-style-type: none"> Patch and virus management records. User authorisation / account creation process and example records. System backup process and example records. Component destruction records. System event log review records.	representative System administrator(s)
T	10.x	<ul style="list-style-type: none"> IT security 	Live audit [P,O,C,T,L]	Sample systems and checks to be agreed during audit.	Network security team representative Systems security team representative System administrator(s)
U	1.4 5.5 7.7 9.7 10.11	<ul style="list-style-type: none"> Internal audit system 	Q+A Presentation of requested samples [D,S,P,L,I]	Overall plan for internal audits/operational controls covering physical security, production, data processing and IT security controls. Internal audit checklists used at operational, supervisory and independent audit levels for each area. Access to samples of completed checklists and tracking mechanisms for remediation actions as requested.	Internal audit lead Internal auditors
V		<ul style="list-style-type: none"> Closing meeting 	Audit Team summary presentation of findings.		Auditee representatives

Annex C Sample required documents 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 the language of the Audit (English) for each Auditor.

Sites should note that failure to provide these printed documents in the language of the Audit may result in:

- Significant delays in the Audit process
- Inability to fully evaluate their content and make an appropriate Audit assessment
- A recommendation to extend the Audit duration of future audits at the Site (at the Auditee's expense).

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 timescale. The Auditors will seek to minimise such requests, whilst still fulfilling the requirements of the Audit.

C.1 Document List

C.1.1 Security Management System (modules B, C)

- Overall security policy
- IT security policy
- Security handbook / manual
- Security management system documentation as provided to all employees
- Information and asset classification system documentation
- Risk assessment process
- Business continuity plan

C.1.2 Key Management (modules J, K)

- Key management processes and supporting documentation
- Records of appointment and training for key management personnel
- Lifecycle management records for HSMs (where used)
- Key management records

C.1.3 Production (modules O, P)

- UICC production reconciliation process
- UICC production tracking / reconciliation documentation

C.1.4 Human Resources (module D)

- Sample job descriptions for all employees with security responsibilities
- Confidentiality agreement for employees
- Standard employment contract
- Employee exit checklists

C.1.5 Security Internal Audit System (module U)

- Overall audit policy and plan
- Audit concept (operational checks, supervisory audits, independent audit)
- Audit checklists for each area (physical security, key management, data processing, production processes, IT) for each level of audit/control (operational checks, supervisory audit, independent audit etc.)

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 Collection of information

The table below provides a detailed mapping of how the Audit Team will normally expect to collect information to assess each applicable SAS requirement. The mapping identifies whether the information is being used to support:

CMP	Compliance	Review of the auditee’s defined and implemented policies, procedures and operational controls to confirm that they are compliant with the requirements of SAS-UP.
CSY	Consistency	Review of the understanding and operation of controls by personnel at all levels to confirm that they are consistent with those defined and documented.
CNF	Confidence	Review of evidence to confirm appropriate operation of controls over an extended period and the application of a system of internal audits to ensure the level of effectiveness is maintained.

CSRG section	Assessed through								
	Document review	Stakeholder interview	Operational personnel interview	Live observation	System configuration review	Sampling and testing	Logs, reports and records	Internal audit reports	CCTV recordings
Policy, Strategy and Documentation	D	S	P	O	C	T	L	I	R
1.1 Policy	CMP	CMP CSY							
1.2 Strategy	CMP	CMP CSY					CNF		
1.3 Business continuity planning	CMP	CMP CSY					CNF		
1.4 Internal audit and control	CMP	CMP CSY						CNF	
Organisation and responsibility									
2.1 Organisation	CMP	CMP CSY	CSY				CNF		
2.2 Responsibility	CMP	CMP CSY	CSY						
2.3 Incident response and reporting	CMP	CMP CSY	CSY				CNF		
2.4 Contracts and liabilities	CMP	CMP CSY							
Information									
3.1 Classification	CMP	CMP CSY					CNF		
3.2 Data and media handling	CMP	CMP CSY					CNF		

CSRG section	Assessed through								
	Document review	Stakeholder interview	Operational personnel interview	See explanations in Audit tools reference					
Personnel security	D	S	P	O	C	T	L	I	R
4.1 Security in job description	CMP	CMP CSY					CNF		
4.2 Recruitment screening	CMP	CMP CSY					CNF		
4.3 Acceptance of security rules	CMP	CMP CSY					CNF		
4.4 Incident response and reporting	CMP	CMP CSY					CNF		
4.5 Contract termination	CMP	CMP CSY					CNF		
Physical security									
5.1 Security plan	CMP	CMP CSY	CSY	CSY					
5.2 Physical protection	CMP	CMP CSY	CSY	CSY	CSY	CSY	CNF		CNF
5.3 Access control	CMP	CMP CSY	CSY	CSY	CSY	CSY	CNF		CNF
5.4 Security staff	CMP	CMP CSY	CSY				CNF		CNF
5.5 Internal audit and control	CMP	CMP CSY	CSY					CNF	
Certificate and key management									
6.1 Classification	CMP	CMP CSY					CNF		
6.2 Roles and Responsibilities	CMP	CMP CSY					CNF		
6.3 Cryptographic key specification	CMP	CMP CSY			CSY	CSY	CNF		
6.4 Cryptographic key management	CMP	CMP CSY	CSY	CSY	CSY	CSY	CNF		CNF
6.5 Audit and accountability	CMP	CMP CSY			CSY		CNF		CNF
6.6 GSMA PKI Certificates	CMP	CMP CSY		CSY	CSY		CNF		
Sensitive process data management									
7.1 Data transfer	CMP	CMP CSY	CSY		CSY	CSY	CNF		CNF
7.2 Sensitive data access, storage, retention	CMP	CMP CSY	CSY	CSY	CSY	CSY	CNF		
7.3 Data generation	CMP	CMP CSY	CSY	CSY	CSY	CSY	CNF		CNF
7.4 Auditability and accountability	CMP	CMP CSY	CSY	CSY	CSY	CSY	CNF		CNF
7.5 Duplicate production	CMP	CMP CSY	CSY	CSY	CSY	CSY	CNF		

CSRG section	Assessed through								
	Document review	Stakeholder interview	Operational personnel interview	See explanations in Audit tools reference					
	D	S	P	O	C	T	L	I	R
7.6 Data integrity	CMP	CMP CSY	CSY	CSY	CSY	CSY	CNF		
7.7 Internal audit and control	CMP	CMP CSY	CSY		CSY	CSY	CNF	CNF	
Logistics and production management									
9.1 Order management	CMP	CMP CSY	CSY	CSY					
9.2 Raw materials	CMP	CMP CSY	CSY	CSY		CSY	CNF		
9.3 Control, audit and monitoring	CMP	CMP CSY	CSY	CSY		CSY	CNF		CNF
9.4 Destruction	CMP	CMP CSY	CSY	CSY		CSY	CNF		CNF
9.5 Storage	CMP	CMP CSY	CSY	CSY		CSY			
9.6 Packaging and delivery	CMP	CMP CSY	CSY	CSY		CSY			
9.7 Internal audit and control	CMP	CMP CSY	CSY				CNF	CNF	
Computer and network management									
10.1 Policy	CMP	CMP CSY	CSY						
10.2 Segregation of roles and responsibilities	CMP	CMP CSY	CSY	CSY	CSY		CNF		
10.3 Access control	CMP	CMP CSY	CSY	CSY	CSY		CNF		CNF
10.4 Remote access	CMP	CMP CSY	CSY	CSY	CSY		CNF		
10.5 Network security	CMP	CMP CSY	CSY	CSY	CSY	CSY	CNF		CNF
10.6 Systems security	CMP	CMP CSY	CSY	CSY	CSY	CSY	CNF		CNF
10.7 Audit and monitoring	CMP	CMP CSY	CSY	CSY	CSY	CSY	CNF		
10.8 External facilities management	CMP	CMP CSY	CSY	CSY			CNF		
10.11 Internal audit and control	CMP	CMP CSY	CSY				CNF	CNF	
Two-step personalisation process									
11.1 Control of duplicate production	CMP	CMP CSY	CSY	CSY	CSY	CSY	CNF		CNF
11.2 Generation of hardware security credentials	CMP	CMP CSY	CSY	CSY	CSY	CSY	CNF		CNF
11.3 Personalisation of security credentials (Perso_SC)	CMP	CMP CSY	CSY	CSY	CSY	CSY	CNF		CNF
11.4 Generation of UICC OS security credentials (Perso_UICC)	CMP	CMP CSY	CSY	CSY	CSY	CSY	CNF		CNF

Annex E Assessment of compliance

E.1 Audit assessment and compliance

The audit seeks to utilise a number of different sources to allow the auditors to assess compliance, consistency and confidence of the controls in place. As described in section 6, the Auditee must receive a C or C- assessment in each section of the audit report for certification to be granted - reflecting an appropriate level of conformity across all applicable sections of the FS.18 SAS Consolidated Security Requirements and Guidelines [3].

Assessment source					
D	Documentation review	O	Live observation of activities/behaviour	L	Records, logs and reports
S	Stakeholder interview	C	System configuration review	I	Internal audit reports and findings
P	Operational personnel interview and activity review	T	Operational sampling and testing	R	CCTV recordings

For the Audit to demonstrate operation of SAS-UP compliant controls, the Auditee must provide appropriate access to relevant information to enable the Audit Team to assess compliance, consistency and confidence. Assessment will normally consider the information sources documented below. For reference, an indication of what might be considered poor conformity (resulting in an NC assessment) and good conformity (resulting in a C assessment) is also included. In general:

An assessment of C will be made for each section of the audit report where the auditee demonstrates a good level of conformity for compliance, consistency *and* confidence.

An assessment of NC will be made for each section of the audit report where the auditee demonstrates a poor level of conformity for one or more of compliance, consistency *or* confidence.

An assessment of C- will be made, at the Audit Team's discretion, for any section of the audit report where the auditee demonstrates a level of conformity that is substantially conformant for compliance, consistency *and* confidence, but where improvements should be considered by the site to achieve a sustainable level of compliance.

Assess	Target	Assessed through		Poor conformity (NC)	Good conformity (C)
Compliance	The Auditee has defined and implemented policy, procedures and operational controls that meet the requirements of SAS-UP.	[D] [S]	Documentation review. Stakeholder interview.	Controls appear to be new and/or untested. Documentation is missing or incomplete, or shows a very high level of inconsistency at the same level (e.g. policies are inconsistent) or across levels (e.g. work instructions are not consistent with procedures; processes do not comply with policies). Controls defined and documented are not consistent with SAS-UP requirements.	Controls are well-established and documented and have been in regular operation for an extended period. Controls documented fulfil SAS-UP requirements. There is a high level of stability, with major changes happening infrequently. Where changes do occur, their introduction is carefully managed through training and monitoring to ensure effectiveness.
Consistency	Controls are clearly understood by personnel at all levels and are operated consistent with those defined and documented.	[S] [P]	Stakeholder interview. Operational personnel interview and activity review.	Personnel do not appear to clearly understand the controls that should be in place through a lack of training and/or familiarity. General discipline appears poor.	Personnel understand the controls and their responsibilities clearly and are able to explain and demonstrate them when asked. The need for sustained compliance is understood, based on personnel having a clear recognition of the importance of the controls to the business and certification and their personal accountability for maintaining the appropriate level of control. Personnel are disciplined and demonstrate a clear culture of security and compliance as core to their actions. Personnel embrace their individual and collective accountability.

Assess	Target	Assessed through	Poor conformity (NC)	Good conformity (C)
		<p>[O] Live observation of activities and behaviour.</p> <p>[C] System configuration review.</p> <p>[T] Operational sampling and testing.</p>	<p>Appropriate records are not maintained or cannot be provided. Records that are available are incorrect or incomplete.</p> <p>There is little or no evidence available that live activities are being carried out following the defined processes. Quality, consistency and accuracy of record taking is consistently poor. Samples taken during the audit are often incorrect or unclear, showing a high level of deviations or discrepancies.</p>	<p>Complete, comprehensive and accurate records exist. Records are reliable and genuine. Different sources are consistent and can readily be validated through cross cross-correlation to validate them. Sampling checks of live operational activities, inventories, records and system configurations show no significant errors or discrepancies.</p>
Confidence	Reliable evidence exists of appropriate operation of controls over an extended period, with an effective system of internal audits acting to ensure the level of effectiveness is maintained.	<p>[L] Written records.</p> <p>[L] Notifications and reports.</p> <p>[L] System audit logs and trails.</p> <p>[I] Internal audit reports and findings.</p> <p>[R] CCTV recordings.</p>	<p>Records are not available to demonstrate that controls have been applied prior to the audit. Where records do exist, they are incomplete or inconsistent or do not show that controls have been applied consistent with those described or presented.</p> <p>The internal audit system is poorly</p>	<p>Sampling checks of operational activities carried out over an extended period prior to the audit show a sustained level of performance with very few errors or discrepancies. Where errors or deviations have occurred, these have been identified quickly and handled appropriately to resolve them and prevent recurrence.</p> <p>A comprehensive system of internal</p>

Assess	Target	Assessed through	Poor conformity (NC)	Good conformity (C)
			<p>defined, infrequent and carried out by personnel without a clear understanding of the requirements.</p>	<p>audits is in place at a number of levels. Clear evidence exists of audits being carried out based on well-defined checklists. Details of samples are recorded. Personnel conducting audits are trained and experienced. Where improvements and non-compliances are identified these are reported through a clear escalation process to ensure appropriate action is taken to address them quickly and effectively.</p>

Annex F Final Audit Report Structure

F.1 First Page:

- Headline: GSM Association SAS for UICC Production (SAS-UP) Qualification Report
- Type of Audit:
 - “First-Audit” for the first Audit at the Site
 - “Renewal Audit” in the following years after a first Audit
 - “Re-Audit” because the result of the “First Audit” or the “Renewal Audit” was unsatisfactory
 - “Dry Audit” / “Wet Audit”, if applicable
- Name of the Auditee and location of the audited Site
- Date of the Audit
- Audit number
- Audit team participants

F.2 Following Pages:

- Audit summary
- Summary of certification
- Auditors’ comments
- Actions required
- Annex A – 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
Incident response and reporting	C-	
Contracts and liabilities	NC	
Information Result		
Classification	NC	- comment - comment
Data and media handling	C-	

Section	Result of sub-section	Auditor remarks
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	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
GSMA PKI Certificates	C-	
Production Data Management Result		
Data transfer	C	
Sensitive data access, storage and retention	C	
Data generation	C	
Auditability and accountability	C	+ comment - comment
Duplicate production	C	+ comment
Data integrity	C	
Internal audit and control	C	
Logistics and Production Management Result		
Order management	NC	
Raw materials	C	+ comment - comment
Control, audit and monitoring	C	
Destruction	C-	
Storage	C	+ comment - comment
Packaging and delivery	C	

Section	Result of sub-section	Auditor remarks
Internal audit and control	C	
Computer and Network Management Result		
Policy	C	
Segregation of roles and responsibilities	NC	
Access control	C	
Remote access	C-	
Network security	C	
Systems security	NC	- comment
Audit and monitoring	C	
External facilities management	C	- comment
Internal audit and control	C	
Two-step personalisation process		
Control of duplicate production	C	
Generation of hardware security credentials	NC	
Personalisation of security credentials	C	
Generation of UICC OS credentials	C-	
Personalisation of UICC OS credentials	C	

- Annex B – SAS scoring mechanism (that is, a copy of Table 5 of this document)
- Annex C – Document management

Annex G 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 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.

G.1 Before the Audit

G.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.

G.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

G.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.

G.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

G.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.

G.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.

G.2 During the Audit

G.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.

G.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.

G.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.).

G.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 H Document Management

H.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 Re-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	David Maxwell, GSMA

		Management (SAS-SM).	
4.1	10 May 2016	Clarify Dry Audit prerequisites. Update to Provisional Certification duration to 9 months. Specify minimum certification duration for new Sites.	David Maxwell, GSMA
5.0	27 Jul 2016	Update to reflect new Consolidated Security Requirements (CSR) and Consolidated Security Guidelines (CSG) PRDs.	David Maxwell, GSMA
6.0	31 Mar 2017	Specify that auditing of processing of data for subscription management requires increased Audit duration. Specify that Certification Period may be extended in exceptional circumstances where Site due for Renewal Audit is completing major changes	David Maxwell, GSMA & James Messham, FML
7.0	16 Feb 2018	Remove Certification Body. Specify that Audit Team makes certification decision. Introduce Appeals Body. Revise cancellation policy. New section on maintaining SAS compliance.	David Maxwell, GSMA
7.1	19 Feb 2019	Clarify Provisional Certification and Wet Audit durations	David Maxwell, GSMA
8.0	25 Jul 2019	Add process for auditing and certification of Supporting Sites	David Maxwell, GSMA
9.0	3 Apr 2020	Updates to standard Audit agenda and document list to reflect current practice.	SAS-UP Auditors
9.1	1 Jul 2020	Editorial changes adding defined terms to support legal framework for SAS-UP.	David Maxwell, GSMA
9.2	21 Apr 2021	Updates to how certification for PKI certificate management is communicated. Added notifiable events for PKI certificate management	David Maxwell, GSMA & James Messham, FML
9.3	1 Apr 2022	Removed references to SAS Consolidated Security Requirements PRD FS.17, allowing withdrawal of that document (content merged into FS.18).	David Maxwell, GSMA
10.0	22 Feb 2023	Integrated information collection and assessment from Covid 19 Methodology Variation. Restructured and updated core document.	James Messham, FML
10.1	12 Apr 2023	Updated GSMA logo	David Maxwell, GSMA

H.2 Other Information

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

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