GSMA SAS Remote Auditing and Certification Policy
Version 4.0
31 August 2022

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

Disclaimer

Antitrust Notice

Table of Contents

1   Introduction

SAS audits are normally carried out on-site by an audit team, and this is the preferred approach for most audit types. However, circumstances may arise where an on-site audit would normally be required but is not possible or acceptable. Such scenarios normally arise based on government travel advice not to visit a country or region e.g. due to war, political instability, a pandemic or other safety concerns for visitors, and associated travel or workplace attendance restrictions.

It is often unclear how long such restrictions or circumstances will last. In these scenarios, alternative options are available in most cases for sites to gain or maintain SAS certification. These include the option of conducting Remote Audits in certain circumstances where this can provide a sufficient level of assurance to enable SAS certification of those Sites.

1.1   Applicability

This policy applies while disruption to normal on-site SAS Audits exists, as determined by the GSMA at its sole discretion. The following factors will influence a decision by the GSMA on whether an alternative to a physical Audit should take place

- Travel advice from the United Kingdom Foreign and Commonwealth Officer (FCO), and/or other relevant government travel advice.
- GSMA, Auditee and Auditing Company travel and employee protection policies.
- Travel and entry restrictions in the country of the Site to be audited that would apply to the SAS Auditors.
- Quarantine restrictions in the country of the Site to be audited and/or the Auditors (that would apply on return from the Audit).
- Onward international travel restrictions that may apply to Auditors following a visit to the country of a Site to be audited.
- Delays in performing a backlog of on-site SAS Audits after other restrictions are lifted.

The possibility of performing a normal on-site audit shall be evaluated separately for each audit request. An on-site audit shall remain as the preferred approach in SAS even while this policy exists, and shall be conducted if feasible, considering the factors above.

Circumstances may also arise where a certified Site wishes to extend its SAS certification beyond its current expiry date for a short period (< 6 months) only. For example, a certified Site may be planning to halt production, or move production to a new Site, within a few months after expiry of its SAS certificate. In such circumstances, an On-Site Renewal Audit may not be justified. The Site may normally apply for a (single) extension of its existing SAS certificate for a period of 6 months, subject to a Temporary Extension Assessment (TEA) process carried out remotely by the Audit Team, and based on a review of key documents and certified security control indicators.

1.2   Definitions

Definitions are as specified in [1], [2], [3], [4], and [5].

1.3   References

Ref	Doc Number	Title
[1]	PRD FS.05	GSMA SAS Methodology for UICC Production, latest version available at www.gsma.com/sas
[2]	PRD FS.05C19	SAS-UP Covid-19 Methodology Variations
[3]	PRD FS.09	GSMA SAS Methodology for Subscription Manager Roles, latest version available at www.gsma.com/sas
[4]	PRD FS.09C19	SAS-SM Covid-19 Methodology Variations
[5]	SAS-UP Scope Definitions	SAS for UICC Production (SAS-UP) Scope Definitions, latest version available at www.gsma.com/sas

2   Overview

Table 1 summarises the options available for different scenarios under SAS-UP and SAS-SM. The following sections provide more details on each option.

Site seeking	Policy & Approach	
	SAS for UICC Production (SAS-UP)	**SAS for Subscription Management (SAS-SM)**
First or Dry Audit, or Scope Extension	Certification based on a Remote Audit may be possible for some sites, depending on their activities, the Audit type, additional criteria and meeting certain pre-requisites, as indicated in section 3.1. Certification will be awarded on condition that an On-site Audit takes place once possible to ensure all controls have been validated. Certificate will have a note to this effect. Sites that are not eligible for a Remote Audit should register their interest with the GSMA, so that scheduling of an On-site Audit can take place once conditions allow.	Certification based on a Remote Audit is normally possible, as many of the controls relate to logical security and it is possible to assess them remotely. Certification will be awarded on condition that an On-site Audit takes place once possible to ensure all controls have been validated. Certificate will have a note to this effect.
Renewal Audit or Wet Audit	Options: • A Renewal Audit or Wet Audit performed remotely may be possible for some sites, depending on their activities, the Audit type, additional criteria and meeting certain pre-requisites, as indicated in section 3.1. Certification will be awarded on condition that an On-site Audit takes place once possible to ensure all controls have been validated. Certificate will have a note to this effect. The standard Duration of Certification following a Renewal Audit performed remotely is 1 year. This applies for all Remote Renewal Audits scheduled after the publication date of version 4.0 of this policy. The Duration of Certification will normally be extended if an On-site Audit takes place duration the Certification Period.	Options: • Certification based on a Remote Audit is possible, on condition that an On-site Audit takes place to validate controls once this is possible. Certificate will have a note to this effect. The standard Duration of Certification following a Renewal Audit performed remotely is 1 year. This applies for all Remote Renewal Audits scheduled after the publication date of version 4.0 of this policy. The Duration of Certification will normally be extended if an On-site Audit takes place duration the Certification Period. OR (Auditee choice), • One temporary (6 month) extension of certification per Certification Period is possible following a Temporary Extension Assessment (TEA).

Site seeking	Policy & Approach	
	SAS for UICC Production (SAS-UP)	SAS for Subscription Management (SAS-SM)
	OR (Auditee choice), • One temporary (6 month) extension of certification is possible per Certification Period following a Temporary Extension Assessment (TEA). OR (Auditee choice), • (Renewal audit only): Hybrid renewal approach involving 2-step Audit process (Off-site review, On-site assessment). This option is available when an On-site Audit is possible now or forecast as possible within 4 months of the completion of the Off-site review. Sites that are not eligible for a Remote Renewal Audit or Wet Audit should register their interest with the GSMA, so that scheduling of an On-site Audit can take place once conditions allow.	
Re-Audit	The previous Audit report will specify the means by which the Re-Audit should take place, already considering the factors that might influence physical attendance at the Site. The possible Re-Audit approaches are: a) Off-site evidence review without need for remote interactive session(s) between Audit Team and Auditee b) Off-site evidence review including remote interactive session(s) between Audit Team and Auditee c) On-site Where On-site Re-Audit (c) has been specified in the previous Audit report, it is an indication from the Audit Team that a Remote Re-Audit is not suitable. Scheduling of an On-site Audit may need to be postponed until conditions allow. For SAS-UP, a hybrid approach for the Re-Audit may be possible in some circumstances.	
Major change at certified site	SAS certified Sites planning major changes to the certified controls should notify the GSMA as described in section 7 of FS.05 (for SAS-UP) and FS.09 (for SAS-SM), so that an Auditor assessment can be made regarding the need for auditing the planned changes and the options available for this.	

Table 1 - Summary of Auditing and Certification Options

3   SAS-UP

For SAS-UP this document describes the types of Audit / audit interactions (the Audit Process in 3.1) and the applicable methodology(ies) (in 3.2).

3.1   Audit Process

3.1.1   First or Dry Audit, Scope Extension

A Site seeking initial certification via a first or Dry Audit, or a Scope Extension to existing certification, should submit an Audit application to the GSMA with details of:

- Its requested scope of certification.

- Any of the components (key management systems, data generation mechanisms, production asset control systems etc.) that form part of the activities for the Site for which certification is being sought that have previously been deployed and proven at other SAS-UP Sites.

- Its ability to comply with the requirements for an Off-site Audit as defined in FS.05C19 "SAS-UP Covid-19 Methodology Variations" [2]

The GSMA and the SAS-UP Auditors may request additional information, and will assess the Site's eligibility for a Remote Audit in accordance with 3.2.3.

If the Site is not eligible for a Remote Audit, GSMA will record the request and monitor the restrictions preventing an On-site Audit, so that scheduling of an On-site Audit can take place once conditions allow.

3.1.2   Renewal and Wet Audits

Sites seeking a Renewal or Wet Audit may apply for:

- A Temporary Extension.

Or

- A Remote Audit if this option is available to them (in accordance with 3.2.3 and following consultation with GSMA) and they are able to comply with the requirements defined in FS.05C19 [2].

Sites seeking a Renewal Audit may also request a Hybrid Renewal Audit.

The standard Duration of Certification following a Renewal Audit performed remotely is 1 year. This applies for all Remote Renewal Audits scheduled after the publication date of version 4.0 of this policy. The Duration of Certification will normally be extended if an On-site Audit takes place duration the Certification Period.

3.1.3   Temporary Extension

Temporary Extension (TE) of existing certification for 6 months, is available to Sites with existing SAS-UP Provisional or Full Certification. Sites may receive one TE per Certification

Period only. Each Temporary Extension is subject to a Temporary Extension Assessment (TEA). For details, see document FS.05C19 [2].

3.1.4   Re-audits

In many cases and according to the SAS-UP Methodology [1], Re-Audits are performed via Off-site review of improvement evidence, with no On-site visit needed. Such Re-Audits may or may not involve a remote interactive session between the Audit Team and Auditee. These approaches are unaffected by disruption to On-site Audits.

In some cases, the outcome of a previous Audit may have specified that an On-site Re-Audit should take place to assess the improvements made to Auditee controls judged as non-compliant, due to the nature and/or volume of the non-compliances. Such an outcome is an indication from the Audit Team that a Remote Re-Audit is not suitable. Scheduling of an On-site Audit may need to be postponed until conditions allow. In some circumstances, a Hybrid Audit approach may be available as an option to the Site, to reduce the On-site Re-Audit duration. For details, see document FS.05C19 [2].

3.1.5   Major changes

SAS certified Sites planning major changes to their certified controls, including Sites that want / need to transfer certified activities to a new physical location, should notify the GSMA in advance as described in section 7 of the applicable SAS Methodology (FS.05/FS.09), so that an Auditor assessment can be made regarding the need for auditing the planned changes and the options available for this. Sites should avoid making changes without notifying the GSMA in advance as this may limit their eligibility to receive a Temporary Extension of Certification.

3.2   Applicable Audit methodology

3.2.1   On-site Audit

Applies to: All audit types

On-site Audits remain the preferred option for certification. Where possible, Auditees will be offered the option for an On-site audit in-line with the SAS-UP Methodology document. The ability to conduct an Off-site Audit will, however, be affected by the issues described in 1.1 and may result in a delay to the certification process.

3.2.2   Hybrid audit

Applies to: Renewal audits
                 Re-audits

A hybrid approach allows Sites the opportunity to complete a review of documentation and evidence during an Off-site phase. An On-site validation of controls will still be required to complete certification renewal, however the duration of this period on-site will be reduced compared with the Conventional Audit Process. This Hybrid Audit option for Renewal Audits should be pursued when the interval between the Off-site and On-site stages is not expected to exceed 4 months. This approach has the following benefits:

- Minimises time spent on-site by Audit Team, reducing site effort and risk in complying with any workplace attendance / activity restrictions.
- Provides a period between Off-site and On-site phases during which the Site may resolve non-compliances highlighted during the Off-site phase.
- Allows audit teams to conduct any backlog of SAS Audits more quickly once travel restrictions are lifted.

For details, see document FS.05C19 [2].

3.2.3   Remote Audits

Applies to: Eligibility for remote audits will be determined based on Site type and activity as specified in Table 2, with reference to the colour coding in Table 3. Activity definitions are provided in [5].

Site type			Activity			Notes
			UICC data gen & perso only[1]	eUICC perso[2]	eUICC data gen + PKI[3]	
Site type	A (New Site)	(i) New activity	🟨	🟧	🟥	Brand new Sites with no track record / history of certification
		(ii) Activity certified elsewhere	🟨	🟧	🟥	
	B (Scope Extension)	(i) New activity	🟨	🟨	🟥	Existing certified Sites with track record / history of certification for some activities, but wish to extend the scope of certification to include new ones
		(ii) Activity certified elsewhere	🟨	🟨	🟧	
	C (Site Relocation)	N/A	🟨	🟨	🟧	Existing certified Sites that want / need to transfer certified activities to a new physical location
	D (Major change)		🟨	🟨	🟧	Existing certified Sites undergoing a major change to how existing activities are performed or controlled
	E (On-site Re-audit)		🟥	🟥	🟥	If a Site has been assessed at the previous Audit as needing an On-site Re-audit to demonstrate improved controls, then a Remote Re-audit is not possible.
	F (Renewal / wet)		🟨	🟨	🟧	Sites requiring a Renewal or Wet Audit (no changes to how activities are performed or controlled)

[1] Generation of data for UICC personalisation and/or UICC personalisation only

[2] eUICC personalisation

[3] Generation of data for eUICC personalisation; Management of PKI certificates

(i)   Activity completely new to Auditee and unproven within SAS-UP.

(ii)   Activity utilising existing components (equipment, procedures etc.) previously deployed and proven at other SAS-UP Sites.

Table 2 – SAS-UP Remote Audit Eligibility

Colour	Remote Audit Eligibility
(red)	Off-site audit process not considered acceptable. Certification only possible with On-site Audit.
(orange)	Off-site Audit process and certification (with caveats clarifying lack of On-site Audit) may be possible, subject to agreement of GSMA and SAS-UP Auditors, considering: - Level of certified component/activity re-use - Scope of activities, and - History of Audit performance at Auditee Site and/or at other certified Sites using components planned for re-use at Auditee Site. Prerequisites below must also be satisfied.
(yellow)	Off-site Audit process and certification (with caveats clarifying lack of On-site Audit) normally possible, subject to agreement of GSMA and SAS-UP Auditors. Site must satisfy Off-site audit prerequisites e.g.: - Additional application information (for new sites) & pre-audit planning call(s) as necessary to allow assessment of whether off-site audit is feasible - Provision of tools to facilitate off-site audit (video conference service, secure document sharing repository, live streaming for physical evidence review, translation if needed etc.). Full details in FS.05C19 [2].

Table 3 – Key to Remote Audit Eligibility Matrix

The Remote Audit considerations in section 4.1.1 are applicable to SAS-UP. More details are available in document FS.05C19 [2].

Sites requesting an Off-site Audit will be required to confirm their ability to satisfy the requirements defined in FS.05C19 for facilitation of the audit process. Sites unable or unwilling to meet these requirements will be ineligible for the Off-site Audit process and will need to revert to a conventional On-site audit.

4 SAS-SM

Core controls for SAS-SM Audits relate to the logical security of the environment and SM platforms. GSMA and SAS-SM Auditing Companies therefore consider it possible to carry out Remote Audits to achieve a minimum satisfactory level of SAS-SM assurance, subject to a case-by-case- assessment.

4.1 First or Dry Audit, Scope Extension

Sites seeking initial SAS-SM certification via a first or Dry Audit, or a Scope Extension to existing certification may request a Remote Audit, subject to their confirmation that they can satisfy the Remote Audit mandatory pre-requisites specified in document "FS.09C19 SAS-SM Covid-19 Methodology Variations".

4.1.1 Remote Audit Considerations

There are several differences in approach between a standard Audit and a Remote Audit:

- A Remote Audit may take longer than a standard Audit, and therefore have higher Audit fees compared to an on-site Audit. This chargeable duration and cost will be determined during the pre-audit planning and preparation.
- A Remote Audit will require Audit planning and preparation sessions between the Auditee and the Audit Team to exchange preliminary information about the Site to be Audited, the Audit scope, duration, schedule and costs, Audit Team expectations etc.
- A Remote Audit requires the advance sharing of documentation within Audit scope with the Audit Team for assessment.
- A Remote Audit will normally require a further chargeable on-site follow-up visit once this becomes possible to confirm compliance against certain requirements.
- Following a compliant Remote Audit outcome, the resulting Certificate will be marked to differentiate to interested parties that this Certificate was not awarded following a standard on-site Audit (until after the on-site follow-up visit).
- A number of other logistical challenges related with remote meetings will need to be agreed between the Auditee and Auditors.

More details are available in document "FS.09C19 SAS-SM Covid-19 Methodology Variations" [4].

4.2 Renewal and Wet Audits

Sites seeking a Renewal or Wet audit may avail of one or both of the options below.

4.2.1 Temporary Extension Assessment (TEA).

A single Temporary Extension of Certification for 6 months is available to Sites with existing SAS-SM Provisional or Full Certification that either:

- Would normally require a Renewal Audit to maintain existing certification
- Would normally require a Wet Audit to move from Provisional to Full Certification

The Temporary Extension is subject to a Temporary Extension Assessment (TEA). For details, see FS.09C19 [4]. Prior to the end of the Temporary Extension period, the site must undergo a successful Remote Audit in order to maintain certification.

4.2.2 Remote Audit

As per section 4.1.

The standard Duration of Certification following a Renewal Audit performed remotely is 1 year. This applies for all Remote Renewal Audits scheduled after the publication date of version 4.0 of this policy. The Duration of Certification will normally be extended if an On-site Audit takes place duration the Certification Period.

4.3 Re-Audit

In many cases and according to the SAS-SM Methodology [3], Re-Audits are performed via Off-site review of improvement evidence, with no On-site visit needed. Such Re-Audits may or may not involve a remote interactive session between the Audit Team and Auditee. These approaches are unaffected by disruption to On-site Audits.

In some cases, the outcome of a previous Audit may have specified that an On-site Re-Audit should take place to assess the improvements made to Auditee controls judged as non-compliant, due to the nature and/or volume of the non-compliances. Such an outcome is an indication from the Audit Team that a Remote Re-Audit is not suitable. Scheduling of an On-site Audit may need to be postponed until conditions allow.

4.4 Major Changes

As per section 3.1.5.

5 Next steps

Please contact sas@gsma.com with any questions or to discuss or apply for any of the auditing and/or certification options described above.

Annex A   Document Management

A.1   Document History

Version	Date	Brief Description of Change	Editor
1.0	27 May 2020	First released version as remote audit policy and process only.	GSMA, SRC & NCC Group
2.0	23 Jun 2020	Extended to cover all options available per audit type for SAS-UP and SAS-SM. Moved processes into separate documents.	David Maxwell, GSMA
2.1	1 Jul 2020	Updates following legal review	David Maxwell, GSMA
3.0	9 Oct 2020	Introduced SAS-UP remote audits. Updated SAS-UP references to point to a single SAS-UP methodology variation. Introduced limitation on SAS-UP temporary extension availability.	David Maxwell, GSMA
3.1	1 Feb 2022	Amended policy (section 3.2.3) to specify that SAS-UP remote audits of new eUICC personalisation activities at sites new to the scheme may be possible.	David Maxwell, GSMA
4.0	31 Aug 2022	Updated policy to apply to general scenarios where on-site audits are not appropriate. Standard duration of certification following a renewal audit performed remotely changed to 1 year.	David Maxwell, GSMA