SRIDA IT PROFESSIONAL REFERENCE PUBLICATION

GSMA SAS

Security Accreditation Scheme · SAS-UP & SAS-SM

FS.18 Consolidated Security Requirements: Requirements, Implementation Guidance & Audit Testing Procedures

DOCUMENT ID
SRIDA-GSMA-SAS-RTP-001

VERSION
1.0

STATUS
Final — Approved for Publication

Rajendra Bodda
Chief Information Security Officer (CISO)
Srida IT · 2026

Independent professional guidance.
Not a GSMA publication.

Free sample pages · The complete manual is available at sridait.com/manuals/rtp-gsma-sas · © 2026 Srida IT



GSMA Security Accreditation Scheme (SAS-UP & SAS-SM)

FS.18 Consolidated Security Requirements: Requirements, Implementation Guidance & Audit Testing Procedures

Prepared by

Rajendra Bodda

Chief Information Security Officer (CISO)

SAMPLE

Published by Srida IT

SRIDA-GSMA-SAS-RTP-001 · Version 1.0 · October 2026

This publication is an independently developed professional guidance document prepared by Srida IT. It is not a GSMA publication, is not endorsed by the GSM Association, does not replace GSMA PRD FS.18, FS.04, FS.05, FS.08 or FS.09, and does not confer SAS certification. Only the GSMA certifies sites, on the recommendation of a GSMA-appointed Audit Team.

Free sample pages · The complete manual is available at sridait.com/manuals/rtp-gsma-sas · © 2026 Srida IT

Document Information and Control

Field	Value
Document title	GSMA Security Accreditation Scheme (SAS-UP & SAS-SM)
Subtitle	FS.18 Consolidated Security Requirements: Requirements, Implementation Guidance & Audit Testing Procedures
Document identifier	SRIDA-GSMA-SAS-RTP-001
Version	1.0
Status	Final — Approved for Publication
Classification	Srida IT Professional Reference Publication
Author	Rajendra Bodda, Chief Information Security Officer (CISO)
Publisher	Srida IT
Publication year	2026
Issue date	October 2026
Reference documents	GSMA PRD FS.18 SAS Consolidated Security Requirements and Guidelines v11.1 (18 September 2024); GSMA PRD FS.04 SAS Standard for UICC Production v9.3 (19 July 2024)
Related documents	GSMA PRD FS.05 (SAS-UP Methodology), FS.08 (SAS-SM Standard), FS.09 (SAS-SM Methodology)
Companion publications	SRIDA-ISMS-27001-RTP-001; SRIDA-AIMS-42001-RTP-001; SRIDA-AIS-27090-RTP-001; SRIDA-DPDP-RTP-001
Next review	On publication of a new version of FS.18, FS.04, FS.05, FS.08 or FS.09, and at least annually

Version history

Version	Date	Author	Description of change
1.0	October 2026	Rajendra Bodda	First published edition, approved for publication.

Approval

Role	Name	Date
Approved for publication	Rajendra Bodda, Chief Information Security Officer (CISO)	27 October 2026

Distribution

Released for publication by Srida IT. Distribution and use are subject to the permitted-use terms in the Copyright, Legal and Usage Notices.

SAMPLE

Free sample pages · The complete manual is available at sridait.com/manuals/rtp-gsma-sas · © 2026 Srida IT

Table of Contents

Part I Foundations 15

Chapter 1 Introduction to the GSMA Security Accreditation Scheme 16
Chapter 2 The SAS Document Set and Certification Process 20
Chapter 3 Sensitive Processes, Assets, Threats and Security Principles 23
Chapter 4 SAS and Related Standards 27
Chapter 5 Terminology, Definitions and Abbreviations 30
Chapter 6 How to Use This Manual 34
Chapter 7 Audit Methodology, Evidence, Sampling and SAS Verdicts 38

Part II FS.18 Security Requirements 42

Chapter 8 Section 1 — Policy, Strategy and Documentation 43
1.1 Policy 44
1.2 Strategy 49
1.3 Business Continuity Planning 53
1.4 Internal audit and control 57
Chapter 9 Section 2 — Organisation and Responsibility 61
2.1 Organisation 62
2.2 Responsibility 66
2.3 Incident response and reporting 70
2.4 Contracts and liabilities 74
Chapter 10 Section 3 — Information 79
3.1 Classification 80
3.2 Data and media handling 84
Chapter 11 Section 4 — Personnel Security 88
4.1 Security in job description 89
4.2 Recruitment screening 94
4.3 Acceptance of security rules 98
4.4 Incident response and reporting 102
4.5 Contract termination 106
Chapter 12 Section 5 — Physical Security 110
5.1 Security plan 111
5.2 Physical protection 115
5.3 Access control 120
5.4 Security staff 125
5.5 Internal audit and control 129
Chapter 13 Section 6 — Certificate and Key Management 133
6.1 Classification 134
6.2 Roles and responsibilities 139
6.3 Cryptographic Key specification 144
6.4 Cryptographic Key management 148
6.5 Auditability and accountability 154
6.6 GSMA Public Key Infrastructure (PKI) Certificates 158
6.7 HSM as a managed service 163
Chapter 14 Section 7 — Sensitive Process Data Management 168
7.1 Data transfer 169
7.2 Sensitive Process Data access, storage and retention 174
7.3 Data generation 179
7.4 Auditability and accountability 183
7.5 Duplicate production 188

SAMPLE

Free sample pages · The complete manual is available at sridait.com/manuals/rtp-gsma-sas · © 2026 Srida IT

7.6 Data integrity 192
7.7 Internal audit and control 196
Chapter 15 Section 8 — SM-DP, SM-SR, SM-DP+, SM-DS and eIM Service Management 200
8.1 SM-DP, SM-SR, SM-DP+, SM-DS and eIM Service 201
8.2 Remote Entity Authentication 205
8.3 Audit trails 209
Chapter 16 Section 9 — Logistics and Production Management 213
9.1 Order management 214
9.2 Raw materials 219
9.3 Control, audit and monitoring 223
9.4 Destruction 229
9.5 Storage 233
9.6 Packaging and delivery 237
9.7 Internal audit and control 241
Chapter 17 Section 10 — Computer and Network Management 245
10.1 Policy 246
10.2 Segregation of roles and responsibilities 250
10.3 Access control 254
10.4 Remote Access 259
10.5 Network security 265
10.6 Systems security 270
10.7 Audit and monitoring 275
10.8 External facilities management 279
10.9 Software Development 283
10.10 Multi-tenancy Environments 287
10.11 Internal audit and control 291
Chapter 18 Section 11 — Two-Step Personalisation Process 295
11.1 Control of Duplicate production 296
11.2 Generation of hardware security credentials 300
11.3 Personalisation of security credentials 304
11.4 Generation of UICC OS credentials 308
11.5 Personalisation of UICC OS credentials 312
Chapter 19 Annex A (Normative): Limited interactive remote access from non-certified locations 316
Annex A Limited interactive remote access from non-certified locations 317

Part III Implementation Framework 321
Chapter 20 Programme Roadmap to First Certification 322
Chapter 21 Defining the Site, Sensitive Processes and Scope 327
Chapter 22 The Security Management System, Risk Assessment and Documentation 332
Chapter 23 Key Management Operations and HSM Governance 336
Chapter 24 Production, Logistics, Reconciliation and Destruction Controls 340
Chapter 25 IT and Network Security Architecture for SAS Sites 344

Part IV Audit and Certification Readiness 353
Chapter 26 Internal Audit Programme for SAS 354
Chapter 27 Audit Techniques and Evidence at SAS Sites 359
Chapter 28 Findings, Corrective Action and Evidence of Change 363
Chapter 29 The Certification Lifecycle 367

Part V Appendices and Templates 371
Appendix A Requirement Applicability Matrix 372
Appendix B Sub-section Summary Matrix 375

SAMPLE

Free sample pages · The complete manual is available at sridait.com/manuals/rtp-gsma-sas · © 2026 Srida IT

CHAPTER 1

Introduction to the GSMA Security Accreditation Scheme

A mobile network operator places a great deal of trust in the companies that produce its SIM cards and eSIMs and in the platforms that download operator profiles to devices. Each of those suppliers handles the secret values that authenticate a subscriber to the network. If those values leak, are duplicated or are altered, the operator bears the fraud, the service disruption and the reputational damage. The GSMA Security Accreditation Scheme (SAS) exists to give operators a common, independent basis for trusting those suppliers.

This chapter introduces the scheme, its two branches, the parties involved and the way FS.18 is organised. It also sets out what this manual is, and what it is not.

1.1 Why the scheme exists

A UICC or eUICC is only useful to a network operator once it has been made unique. During production, each device receives its own subscriber identity, its own authentication key and, for eUICCs, its own certificates and security domains. The supplier that generates and loads those values therefore holds, for a period, material that could be used to clone subscriptions, intercept traffic, redirect remote provisioning or impersonate the operator's own management systems. The same is true, in a different form, for the platforms that prepare, route and discover operator profiles for remote SIM provisioning.

Operators cannot realistically audit every supplier site themselves, and suppliers cannot sustain a separate audit for every customer. SAS resolves this by defining one set of security requirements, one audit approach and one certification decision taken by the GSMA, which operators and other customers can then rely on in their own procurement and supplier assurance. FS.04 describes the scheme as voluntary for suppliers; in practice, many operators expect or require certification as a condition of doing business, and certain GSMA eSIM ecosystem roles depend on it.

The scheme is site-based. It certifies that a defined physical facility, with its people, processes and systems, operates the controls needed to protect specified Sensitive Processes. It does not certify a product, a company as a whole or a software platform in the abstract.

SAMPLE

1.2 The two schemes: SAS-UP and SAS-SM

SAS currently has two branches that share one requirement document.

Table 1-1. The two SAS branches at a glance

Aspect	SAS for UICC Production (SAS-UP)	SAS for Subscription Management Roles (SAS-SM)
Typical Auditee	SIM and eUICC manufacturers, personalisation bureaux, data-generation centres, eUICC Manufacturers (EUMs) managing GSMA PKI certificates, and post-personalisation packaging sites	Operators of SM-DP, SM-SR, SM-DP+, SM-DS and eIM services, whether in their own data centres or on hosted or cloud infrastructure
What is protected	Personalisation data, MNO keys, PKI private keys, physical devices at every stage from blank stock to finished, packaged product, and rejects until destruction	Operator profiles, profile-protection keys, PKI private keys of the SM role, platform and profile management transactions, and the audit trails of those transactions
Scheme documents	FS.04 Standard and FS.05 Methodology	FS.08 Standard and FS.09 Methodology
Requirement source	FS.18 requirements marked **All** and **UP**	FS.18 requirements marked **All** and **SM**
Dominant risks	Duplicate or mismatched devices, theft of stock or rejects, disclosure of keys and personalisation files	Compromise of profile-protection keys, unauthorised profile operations, cross-tenant exposure and weaknesses in remote administration

A single organisation may hold both certifications for different sites, or for the same site where it performs both production and subscription management activities. FS.18 anticipates this; for example, its guidance on Section 6 discusses the conditions under which an EUM and an SM function may share HSM infrastructure.

Free sample pages · The complete manual is available at sridait.com/manuals/rtp-gsma-sas · © 2026 Srida IT

1.3 The parties involved

Several parties have defined roles in the scheme. The definitions below are summarised from FS.18 Section 1.7 and FS.04; the full terminology is in Chapter 5.

- **The GSMA** owns the scheme, publishes its documents, administers applications and takes the certification decision. Certification is based on the assessment and recommendation of the Audit Team; the Audit Team does not itself issue certificates.
- **The SAS Group** is the body of GSMA members and staff, working with the SAS Auditors, that maintains and develops the Standards, Methodologies and FS.18. It reviews the scheme and its documentation periodically with operators, suppliers and auditors.
- **The Audit Team** consists of two Auditors drawn from two different GSMA-selected auditing companies, who jointly carry out the Audit at the Auditee's Site on the GSMA's behalf.
- **The Auditee** is the supplier seeking certification of one or more of its Sites.
- **Customers**, chiefly mobile network operators, but also device makers and other eSIM ecosystem participants, rely on certification when selecting and overseeing suppliers.

> **Srida IT's position**
>
> Srida IT is not a GSMA-selected auditing company, does not form part of any Audit Team and cannot certify a Site or predict a certification outcome. This manual is an independent practitioner publication. It is not a GSMA document and has not been reviewed or endorsed by the GSMA. Only the GSMA certifies, on the recommendation of the Audit Team.

1.4 Sensitive Processes: the unit of protection

Everything in SAS is organised around the Sensitive Process (SP): the activity being evaluated together with the assets that pass through it. FS.18 notes that SPs can relate to UICC production, subscription management and certificate management. The scheme Standard defines which SPs exist for that scheme, and the Auditee is responsible for working out which of them, and therefore which FS.18 requirements, apply to its Site. Chapter 3 describes the SAS-UP SPs and scope options in detail, and Chapter 21 explains how to define the Site and its scope in practice.

The focus on SPs has a practical consequence that new Auditees often underestimate. Controls are assessed in relation to the SP, not in the abstract. A well-run corporate IT environment does not by itself satisfy SAS if the systems that generate personalisation data, the rooms in which devices are personalised or the routes by which files reach the Site are not themselves controlled to the required level.

SAMPLE

1.5 FS.18 and how it is organised

FS.18, the *Consolidated Security Requirements and Guidelines* (CSRG), is the single source of security requirements for both schemes. Version 11.1, dated 18 September 2024, is the version on which this manual is based. Earlier, SAS-UP requirements had also been carried in a separate document; FS.18 version 8.0 consolidated them so that FS.18 became the only requirement source.

FS.18 presents each topic in two columns. The left column contains numbered **requirement statements**, expressed with "shall" or "must", which are what the Audit Team assesses. The right column contains **guidelines**, expressed with "should" or "may", which illustrate one acceptable way of meeting the requirement. FS.18 makes clear that its requirements are generally non-prescriptive: an Auditee may meet them with controls of its own design, provided the same security objective is achieved to an acceptable level. Each statement carries a scope marker showing whether it applies to all participants or only to UICC production or subscription management activities.

Table 1-2. Structure of FS.18 v11.1 and where each section is treated in this manual

FS.18 section	Title	Sub-sections	Requirements	Chapter
1	Policy, Strategy and Documentation	4	5	8
2	Organisation and Responsibility	4	10	9
3	Information	2	3	10
4	Personnel Security	5	8	11
5	Physical Security	5	7	12
6	Certificate and Key Management	7	17	13
7	Sensitive Process Data Management	7	12	14
8	SM-DP, SM-SR, SM-DP+, SM-DS and eIM Service Management	3	7	15
9	Logistics and Production Management	7	16	16

Free sample pages · The complete manual is available at sridait.com/manuals/rtp-gsma-sas · © 2026 Srida IT

FS.18 SUB-SECTION 9.3

Control, audit and monitoring

GSMA SAS requirement · applies: UP | WP-SAS-9.3

A Requirement Reference

GSMA PRD FS.18 v11.1, 9.3 — Control, audit and monitoring

Section: 9 Logistics and Production Management

Summaries are in Srida IT's own words and do not reproduce GSMA text. Refer to the GSMA document for the authoritative requirement statements and guidelines.

Requirement	Applies	What it asks (Srida IT summary)
9.3.1	UP	Production must be governed by an audit trail that (i) fully accounts for the numbers of Class 1 assets created, processed, rejected and destroyed, (ii) makes the people responsible at each point identifiable and accountable, and (iii) forces escalation whenever a discrepancy or other security incident is found.
9.3.2	UP	Class 1 asset stock must be reconciled end to end so that every individual element can be accounted for.
9.3.3	UP	Sensitive production steps must be performed under auditable dual control and the four-eyes principle, at least: (i) counting assets into Personalisation, (ii) authorising Re-personalisation of rejected UICCs, (iii) counting assets packed for dispatch, and (iv) destroying rejected assets.
9.3.4	UP	It must be possible to prove, from production records together with CCTV, that the four-eyes principle was actually applied.
9.3.5	UP	The Site must carry out regular audits that confirm production controls and the audit trail remain intact and are being followed.
9.3.6	UP	The supplier must be able to show that unauthorised duplication cannot occur in production during Personalisation or Re-personalisation.
9.3.7	UP	The supplier must be able to show that batches keep their integrity inside the production Environment, preventing (i) assets from one batch contaminating another and (ii) uncontrolled assets weakening the asset-control mechanism.

B Objective

Sub-section 9.3 is the operational heart of SAS-UP physical production security. Its purpose is that, for every batch, the Site can prove how many Class 1 assets existed at each stage, who held them, what happened to every unit that did not reach the customer, and that no unit was personalised twice or left the process unaccounted for. It addresses the FS.04 threats of duplicate creation through technical error, rework or reuse of data, loss or theft, and cross-contamination, and it supports the SP security objectives of controlling the production process and guaranteeing a secure product flow. Unlike most sub-sections, its effectiveness is demonstrated less by documents than by numbers that add up and by CCTV that shows what the records claim.

C Interpretation

Audit trail (9.3.1). FS.18 requires a trail that accounts for quantities, identifies responsible individuals and triggers escalation. FS.18 guidance suggests recording quantities by asset type and status at each processing stage, a formal counted handover wherever responsibility changes, and a tracked register of discrepancies, with a risk assessment where a discrepancy cannot be resolved. Auditors test whether the trail is complete enough to re-perform a reconciliation from it alone: opening quantity, quantities in and out of every stage, good, rejected, surplus and destroyed, with names, dates and times. Module reels are recognised in the guidance as harder to control than card bodies; auditors still expect tracking of reel usage and set-up waste treated as rejects.

End-to-end reconciliation (9.3.2). The requirement is that every Class 1 element can be accounted for, from issue into the process to dispatch or destruction. FS.18 guidance suggests an independent end-of-production reconciliation, interim reconciliations, secure holding between stages, recounting before sensitive stages such as Personalisation, and treating missing removable elements (for example plug-ins) as incidents. Auditors will almost always re-perform at least one reconciliation from raw records rather than reading the reconciliation summary. A reconciliation that is signed by the same person who produced the batch, or that closes by an unexplained balancing adjustment, will not satisfy the requirement.

Dual control and four-eyes (9.3.3 and 9.3.4). The four listed steps are a minimum. Auditors expect the Site to identify all its sensitive steps in a risk-based way, typically also including issue of embedded bodies to personalisation, handling of rejects at the machine and transfers between buildings. The four-eyes principle must be auditable: records show who, when and what, and the time recorded allows the corresponding CCTV to be retrieved and shown. FS.18 guidance describes acceptable counting approaches for packaging (card counters, machine counts, weight checks) provided the Auditee can show the counting method is accurate, continuous CCTV

© 2026 Srida IT · Version 1.0 · Independent guidance, not a GSMA publication

Free sample pages · The complete manual is available at sridait.com/manuals/rtp-gsma-sas · © 2026 Srida IT

between count and seal, and a check that every envelope or box actually contains a UICC before the final count. Re-personalisation needs auditable four-eyes authorisation, and guidance expects the reject to be electrically disabled and physically marked under four-eyes first.

Duplication and batch integrity (9.3.5–9.3.7). 9.3.5 requires regular audits of production controls and the audit trail (distinct from the broader 9.7 programme, but usually delivered through it). 9.3.6 requires demonstrable prevention of duplication during Personalisation and Re-personalisation; FS.18 guidance links this to control over Personalisation Data availability under section 7.2 and to control of embedded bodies at the point of issue. 9.3.7 targets the practical reality that several batches run simultaneously and other activities, such as payment card personalisation or embedding, may share the physical Environment. Guidance mentions locked trolleys or cabinets and sealed boxes, and checking quantities before new assets enter the production Environment. Auditors walk the floor to see whether a stray card could join a stack unnoticed.

Common misreadings: treating MES or machine counters as self-evidently correct (accuracy must be demonstrated); assuming CCTV coverage exists because a camera points at the room (it must allow the count and sealing to be seen); treating Re-personalisation as an operator decision; and believing reconciliation is satisfied by an ERP report without independent review.

D Applicability and Scope

All seven requirements are marked UP (section 9 marker). They apply to SAS-UP Sites that personalise UICCs or eUICCs in card, embedded or wafer form and to post-personalisation packaging where personalised product is handled. For wafer-level personalisation the counting unit becomes die or wafer maps, and counting and four-eyes controls must be adapted; the Audit Team decides how the requirements are assessed. A data-generation-only Site with no physical product would not normally be assessed against 9.3 physical controls, but 9.3.6 links to its Personalisation Data controls under section 7. Section 9 is outside SAS-SM-only scope. FS.04 assets: PFP_UICC, FIN_UICC, PRJ_UICC, ISC_DEV, SEN_MAD (SEN_MAT traceability and SEN_MAU audit information); threats T_DOUB_TEC, T_DOUB_REW, T_DOUB_REU, T_LOSS, T_CONT.

E Implementation Guidance

1. Map the production flow for each product type (card, embedded, eUICC, wafer) from issue of Class 2 bodies to dispatch, marking each counting point, each change of custody and each sensitive step. Approve the map as the basis of the audit trail and of the four-eyes register.
2. Design the audit trail (paper travellers, MES or both) so that every stage records opening quantity, good, rejected, surplus and closing quantity by asset type, the identity of each responsible person, date and time. Make handovers explicit with a counted, signed transfer by both parties.
3. Define counting methods per stage and validate their accuracy: calibrate card counters and scales on a defined schedule, test them against known quantities, and record results. Reject a counting method whose error rate cannot be demonstrated.
4. Operate dual-control counts at entry to Personalisation and at final packaging (two independent counts or one count under four-eyes), with packing and sealing of boxes immediately after the count, under an overhead camera covering the workstation. Where UICCs are enclosed in envelopes or carriers, add a presence check (for example weight check or detection) before the final count.
5. Control Re-personalisation: require a documented, four-eyes authorisation per rejected unit or group; electrically disable and physically mark the reject under four-eyes before Re-personalisation; restrict the data operation so that the Personalisation Data for that unit can be re-issued only once and only against the recorded reject.
6. Hold work-in-progress in locked trolleys, cages or cabinets with controlled Physical Keys and sealed boxes; label every container with batch, stage and quantity; recount before Personalisation.
7. Control everything that enters the personalisation Environment: count assets in, prohibit unrelated Class 2 material, segregate other products (for example payment cards) by time, space or physical barrier, and perform a clear-line check at batch change-over.
8. Reconcile each batch end to end, independently of the production team, closing created = dispatched + rejected/destroyed + returned/held, with no balancing figures. Run interim reconciliations at shift ends and stage boundaries.
9. Operate a discrepancy and incident register: every variance is recorded, escalated to the security manager within a defined time, investigated (including CCTV review), and, where unresolved, risk-assessed with a documented decision on the batch.
0. Schedule regular audits (Srida IT recommends at least monthly sampling by a person independent of production) of the audit trail, the four-eyes evidence via CCTV, reconciliation accuracy and batch integrity; record findings and follow-up.

F Roles and Responsibilities

Role	Responsibility
Production operators	Perform counts and handovers, record quantities and rejects accurately, sign for custody.
Second-person controller (four-eyes)	Witnesses or independently performs counts, Re-personalisation authorisations and reject disabling; must not depend on the first person.
Production supervisor / shift leader	Ensures traveller or MES completeness, performs interim reconciliation, raises discrepancies.

SAMPLE

Free sample pages · The complete manual is available at sridait.com/manuals/rtp-gsma-sas · © 2026 Srida IT

Role	Responsibility
Reconciliation officer (independent)	Performs end-to-end batch reconciliation independent of the production team and signs the closure.
Security manager	Owns the 9.3 control design, the discrepancy register and escalation, reviews CCTV during investigations, owns regular audits.
CCTV / security operator	Retrieves footage for investigations and audits; maintains camera coverage of counting and sealing stations.
Data / personalisation engineering	Configures personalisation systems so Personalisation Data cannot be used twice, and Re-personalisation requires authorisation.
Internal auditor	Performs the regular audits under 9.3.5 and reports to management.

G Documentation and Records

- Production flow maps per product type with counting points and sensitive steps
- Audit trail design: traveller templates or MES configuration documentation
- Four-eyes/dual-control procedure listing all sensitive steps
- Re-personalisation procedure with authorisation, disabling and marking records
- Counting device calibration and accuracy test records
- Batch reconciliation procedure and completed reconciliation records
- Discrepancy and incident register, investigation reports and risk assessments for unresolved items
- CCTV camera coverage plan for counting, packing and sealing stations
- Work-in-progress storage and Physical Key control records
- Regular audit schedule, checklists, reports and corrective action records

H Audit Testing Procedures

Recommended Srida IT audit methodology; not prescribed by GSMA FS.18 or the SAS Methodology. Result columns follow the SAS verdict scale (C, C-, NC) as an internal-audit convention.

Table 16-4. Audit testing procedures, Sub-section 9.3

Test ID	Method	Testing procedure	Result
TP-SAS-9.3-01	EXAMINE	Examine the production flow maps, audit trail design and four-eyes procedure. Confirm that every change of custody, every counting point and every sensitive step (at minimum the four listed in 9.3.3) is identified and that the trail records quantities by type and status, responsible persons, date and time.	☐ C ☐ C- ☐ NC ☐ N/A
TP-SAS-9.3-02	RE-PERFORM	Select completed batches (see sampling) and re-perform the end-to-end reconciliation from raw records only (traveller or MES stage records, reject logs, destruction logs, packing lists, dispatch notes). Confirm that opening quantity equals dispatched plus destroyed plus held, without balancing adjustments, and compare with the Site's own reconciliation.	☐ C ☐ C- ☐ NC ☐ N/A
TP-SAS-9.3-03	OBSERVE	Observe a live dual-control count at entry to Personalisation and a final packaging count, pack and seal. Confirm two people participate, the counting device is used as validated, boxes are sealed immediately and the action is fully visible on the overhead CCTV view. Record seal numbers and verify they appear in the packing record.	☐ C ☐ C- ☐ NC ☐ N/A
TP-SAS-9.3-04	SAMPLE	From production records, select four-eyes events (entry counts, packaging counts, Re-personalisation authorisations, reject disabling) and, using the recorded dates and times, retrieve the CCTV footage. Confirm two named persons are present and that the footage matches the record (quantity handled, sealing, no interruption).	☐ C ☐ C- ☐ NC ☐ N/A
TP-SAS-9.3-05	SAMPLE	Select Re-personalisation events and verify for each: written four-eyes authorisation before the event, evidence that the reject was electrically disabled and physically marked, that the replacement used the same Personalisation Data exactly once, and that the disabled reject appears in the destruction log.	☐ C ☐ C- ☐ NC ☐ N/A
TP-SAS-9.3-06	RE-PERFORM	Test the accuracy of the counting devices used at packaging: with the operator, count a known quantity (for example a sealed reference stack) with the card counter or weigh scale and compare. Examine calibration and accuracy-test records for the period.	☐ C ☐ C- ☐ NC ☐ N/A

SAMPLE

Free sample pages · The complete manual is available at sridait.com/manuals/rtp-gsma-sas · © 2026 Srida IT

Test ID	Method	Testing procedure	Result
TP-SAS-9.3-07	**INSPECT**	Walk the personalisation and packaging Environment during production. Inspect work-in-progress storage (locked trolleys, cages, Physical Key control), container labelling and seals, the presence of any uncontrolled Class 2 or other-product material, and segregation between concurrent batches and other product lines.	☐ C ☐ C- ☐ NC ☐ N/A
TP-SAS-9.3-08	**EXAMINE**	Examine the discrepancy and incident register for the period. Select entries and confirm each was escalated within the defined time, investigated with CCTV where relevant, closed with a root cause or risk-assessed with a documented decision. Cross-check that discrepancies visible in sampled reconciliations appear in the register.	☐ C ☐ C- ☐ NC ☐ N/A
TP-SAS-9.3-09	**INSPECT**	Inspect the personalisation system and MES configuration for duplication controls: confirm that each Personalisation Data record can be consumed once, that a second use requires a logged Re-personalisation authorisation, and that data availability at the machine is limited to the current batch. Review a system log extract showing a refused duplicate attempt, if available.	☐ C ☐ C- ☐ NC ☐ N/A
TP-SAS-9.3-10	**EXAMINE**	Examine the schedule and reports of the regular production-control audits required by 9.3.5 for the period: confirm audits were performed as scheduled by independent persons, covered audit trail integrity, CCTV-based four-eyes checks and reconciliation, and that findings were tracked to closure.	☐ C ☐ C- ☐ NC ☐ N/A

I Sampling Guidance

Srida IT recommends: batch reconciliation re-performance on 3–5 batches across product types and shifts, including at least one batch with Re-personalisation and one with a recorded discrepancy; four-eyes CCTV correlation on 10–15 events spread across the evidence period and within CCTV retention (CCTV retention limits the look-back window, so sample the most recent weeks for footage and the full period for records); all Re-personalisation events if fewer than 25, otherwise 25; all discrepancy register entries if fewer than 25, otherwise 25 including every unresolved item; counting device accuracy test on every device type used at packaging. The evidence period is normally the period since the last audit.

J Interview Questions

Interviewee	Question
Production operator	Show me what you record when you hand a box of cards to the next stage, and what happens if your count differs from the label.
Four-eyes controller	When you are the second person at a packaging count, what exactly do you watch, and what would make you refuse to sign?
Shift leader	How do you authorise Re-personalisation, and how do you know the rejected card has been disabled before the new one is produced?
Reconciliation officer	Walk me through your last reconciliation that did not balance. What did you do and who did you tell?
Security manager	Which discrepancies remain unresolved, what risk assessment did you make, and what happened to the affected batch?
Personalisation engineer	What stops the system from writing the same Personalisation Data to two cards?

K On-Site and Technical Verification

- Re-performed reconciliation agrees with the Site's reconciliation and closes without adjustment
- CCTV footage for sampled four-eyes events shows two people and the full count-to-seal sequence
- Counting device test on a known quantity produces the correct result
- No uncontrolled Class 1 or Class 2 material found on the production floor or in unlocked containers
- Seal numbers observed at packaging match packing records
- Personalisation system rejects a second use of a Personalisation Data record without authorisation

L Expected Audit Evidence

- Production travellers or MES stage records for sampled batches
- Batch reconciliation records signed by an independent reconciler
- Four-eyes logs and CCTV footage references (date, time, camera)
- Re-personalisation authorisations, disabling and marking records
- Counting device calibration and accuracy test records
- Discrepancy and incident register with investigation reports

SAMPLE

Free sample pages · The complete manual is available at sridait.com/manuals/rtp-gsma-sas · © 2026 Srida IT

- WIP storage and Physical Key logs
- Regular production-control audit schedule and reports
- Personalisation system configuration and logs showing single-use control

M Evaluation Criteria

Indicators of C (Compliant)

- Re-performed reconciliations close exactly from raw records and are independently reviewed
- Four-eyes is applied at all listed sensitive steps and is consistently verifiable through records and CCTV
- Re-personalisation is authorised, rejects are disabled and destroyed, and duplicate use of data is technically prevented
- Discrepancies are escalated, investigated and registered; regular audits are performed and followed up

Indicators of C-

- Isolated recording omissions (missing time or second signature) where CCTV confirms the control was applied
- Regular audits performed but less often than scheduled or without full CCTV correlation
- Counting device accuracy not formally tested although results are consistent

Indicators of NC (Non-compliant)

- Reconciliation cannot be re-performed or closes only through unexplained adjustments
- Packaging counts or Re-personalisation performed by one person, or CCTV does not cover the count and seal
- Personalisation Data can be reused without authorisation, or unresolved discrepancies are not escalated

N Common Gaps and Findings

- FS.18 9.3.2 – re-performance of batch reconciliation for an eUICC batch showed 12 units unaccounted for; the Site's reconciliation recorded them as 'machine waste' without reject records – Class 1 assets not fully accounted for.
- FS.18 9.3.4 – for four of 12 sampled packaging counts, the recorded time did not correspond to any CCTV footage of the packing table; the overhead camera had been repositioned – four-eyes not auditable through CCTV.
- FS.18 9.3.3(ii) – Re-personalisation is authorised by the machine operator alone through the personalisation software – no four-eyes authorisation.
- FS.18 9.3.7(ii) – a tray of payment cards from another line was found beside the UICC personalisation machine during production – uncontrolled assets could compromise counts.
- FS.18 9.3.1(iii) – three reconciliation discrepancies in the last quarter were corrected by recount but not recorded in the discrepancy register or escalated – escalation not operating.
- FS.18 9.3.5 – no audit of the production audit trail has been performed in the last six months – regular audits not evidenced.

SAMPLE

O Remediation Guidance

- Redesign travellers or MES to capture stage quantities, statuses, names and timestamps without free-text balancing fields
- Fix camera positions with a documented coverage plan and include a monthly CCTV coverage check in security patrols
- Configure the personalisation system so Re-personalisation requires a second authorised user and links to a disabled-reject record
- Introduce an independent reconciliation role and prohibit balancing adjustments without security manager approval
- Train all staff on discrepancy escalation and make the register the single source for variance tracking
- Establish a monthly production-control audit with CCTV correlation and report results to management

P Monitoring Metrics

- Percentage of batches reconciled to zero at first closure (and number requiring investigation)
- Number of four-eyes events sampled per month and percentage verified on CCTV
- Average time from discrepancy detection to escalation and to closure
- Number of Re-personalisations per 10,000 units, trended by line

Q Control Maturity Indicators

Initial	Defined	Managed	Optimised
Counts recorded inconsistently; reconciliation performed by production and adjusted to balance; CCTV used only after incidents.	Documented audit trail, four-eyes procedure and reconciliation; CCTV covers counting and sealing; discrepancies recorded.	Independent reconciliation, routine CCTV correlation of four-eyes events, validated counting devices, system-enforced Re-personalisation authorisation, discrepancy metrics reviewed monthly.	MES-integrated serial-level tracking, automated reconciliation and duplicate detection, CCTV bookmarks generated from MES events, trend analysis feeding risk assessment.

R Related Requirements and Standards

- FS.18 7.2 Sensitive Process Data access, storage and retention; 7.4 Auditability and accountability; 7.5 Duplicate production; 5.2 Physical protection (CCTV); 2.3 Incident response and reporting; 9.2 Raw materials; 9.4 Destruction; 9.7 Internal audit and control; 11.1 Control of Duplicate production

© 2026 Srida IT · Version 1.0 · Independent guidance, not a GSMA publication

Free sample pages · The complete manual is available at sridait.com/manuals/rtp-gsma-sas · © 2026 Srida IT