GSMA SAS Standard for Subscription Manager Roles
Version 3.0
31 March 2017

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

Security Classification: Non-confidential

Copyright Notice

Disclaimer

Antitrust Notice

Table of Contents

1 Introduction

1.1 Overview

The GSMA Security Accreditation Scheme for Subscription Management Roles (SAS-SM) is a scheme through which Subscription Manager – Secure Routing (SM-SR), Subscription Manager – Data Preparation (SM-DP), Subscription Manager – Data Preparation+ (SM-DP+) and Subscription Manager – Discovery Server (SM-DS)suppliers subject their operational sites to a comprehensive security audit to ensure that adequate security measures to protect the interests of mobile network operators (MNO) have been implemented.

MNOs are dependent on suppliers to control risks; to ensure that adequate security is in place. Consistency and confidence is improved by the introduction of an auditable SAS standard, which is applied to all SM-DP, SM-SR, SM-DP+ or SM-DS suppliers. The purpose of the SAS-SM Standard is;

- to minimise risks to MNOs introduced by SM-DP, SM-SR, SM-DP+ or SM-DS functionality and,
- to provide a set of auditable requirements, together with the SAS Consolidated Security Requirements [2] and Guidelines [3] and the SAS-SM Methodology [1], to allow SM-DP, SM-SR, SM-DP+ or SM-DS suppliers provide assurance to their customers that risks are controlled.

Security objectives applicable to organisations in the role of SM-SR, SM-DP, SM-DP+ and/or SM-DS are herein outlined.

1.2 Background

This SAS-SM Standard and related documents have been created and developed within GSMA through collaboration between representatives from MNOs, suppliers and the GSMA-appointed auditing companies. The GSMA is responsible for maintaining the SAS-SM Standard. A review of the scheme and its documentation takes place with MNOs, suppliers and the appointed auditors annually.

1.3 Scope

Organisations and the operational sites eligible for auditing include only those where remote provisioning and management takes place.

The scope of the document is restricted to security issues relating to:

- Creation, remote provisioning and management of MNO Profiles via SM-DP specified by GSMA in SGP.01 [4] and SGP.02 [5].
- Remote provisioning and management of eUICCs via SM-SR specified by GSMA in SGP.01 [4] and SGP.02 [5].
- Creation of MNO Profiles, remote provisioning and management of MNO Profiles and eUICCs via SM-DP+ specified in SGP.21 [6] and SGP.22 [7].
- Discovery services via SM-DS specified by GSMA in SGP.21 [6] and SGP.22 [7].

The security objectives have been achieved by defining:

- eUICC life-cycle and processes in the scope of SM-SR.
- Profile life-cycle and processes in the scope of SM-DP and SM-DP+.
- SM-DS processes
- Assets to be protected.
- Risk and threats.
- Security requirements.

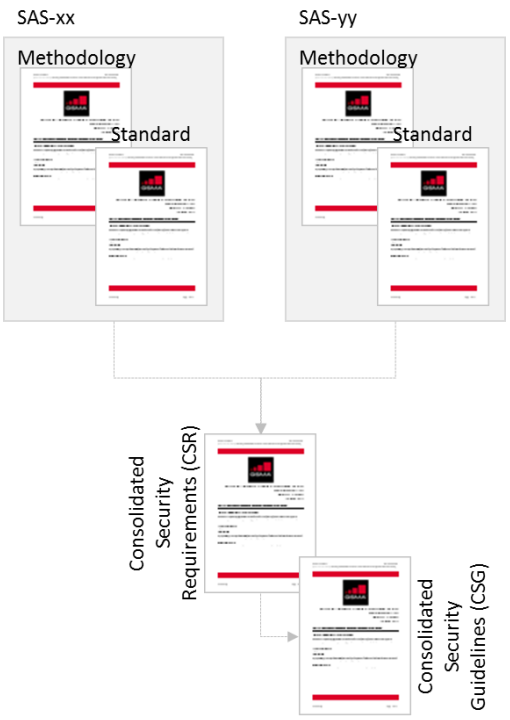
This document is not intended to be an SM-DP, SM-SR, SM-DP+ or SM-DS product protection profile.

1.4 Intended Audience

- Security professionals and others within organisations offering SM-DP, SM-SR, SM-DP+ or SM-DS functionality who are responsible for SM-DP, SM-SR, SM-DP+ or SM-DS SAS implementation and compliance.
- SAS-SM Auditors
- MNOs.

1.5 Related Documents

This document is part of the Security Accreditation Scheme documentation published by the GSMA. Documentation is structured as follows:



Each SAS scheme comprises a **Methodology** and **Standard** relevant to Sensitive Processes (SPs) that should be protected**.**

The **Methodology** describes the purpose of the scheme and how it is administered.

The **Standard** describes the security objectives related to the relevant SPs.

The **Consolidated Security Requirements (CSR)** describes all of the security requirements that may apply to SPs in the different SAS schemes.

The **Consolidated Security Guidelines (CSG)** provides examples of how the security requirements may be achieved.

Figure 1 - SAS Documentation Structure

The accreditation schemes and documents are designed such that multiple schemes may utilise the same Consolidated Requirements and Guidelines.

The security objectives described in this document are supported by FS.09 GSMA SAS Methodology for Subscription Manager Roles [1], the GSMA SAS Consolidated Security Requirements [2], and the GSMA SAS Consolidated Security Guidelines [3].

1.6 Definitions

Term	Description
Actor	Person who is involved in, or can affect, the Sensitive Process.
Business Continuity	Capability of the operator of a SP to continue to operate the SP at predefined levels (as determined by customer requirements) following a failure incident.
Data Preparation	A set of functions related to the Profile generation including Key handling, Personalisation data generation, encryption and transfer of a Profile in a dedicated eUICC.
Employee	An individual who works part-time or full-time under a contract of employment, whether oral or written, express or implied, and has recognized rights and duties. Also called worker.
Environment	Environment of use of the Sensitive Process limited to the security aspects
eUICC	A UICC which is not easily accessible or replaceable, is not intended to be removed or replaced in a device, and enables the secure changing of profiles. The term originates from "embedded UICC".
eUICC Management	A set of functions related to the registration of an eUICC to a SM-SR and the change of SM-SR for an eUICC.
Key	Refers to any logical key for example, a cryptographic key
Local Profile Assistant	A functional element in the Device or in the eUICC that provides the Local Profile Download (LPD), Local Discovery Services (LDS) and Local User Interface (LUI) features.
Platform Management	A set of functions related to the transport, enabling, disabling and deletion of a Profile on an eUICC.
Profile	Combination of a file structure, data and applications to be provisioned onto, or present on, an eUICC and which allows, when enabled, the access to a specific mobile network infrastructure.
Profile Management	A set of functions related to the downloading, installation and content update of a Profile in a dedicated eUICC.
Profile Metadata	Information about a profile for example, MSISDN, POL2, required by the SM-SR or the LPA to be able to manage the eUICC.
Sensitive Process	The security evaluation field, covering the processes and the assets within those processes
Universal Integrated Circuit Card	A smart card that conforms to the specification written and maintained by the ETSI Smart Card Platform.

1.7 Abbreviations

Term	Description
CI	Certificate Issuer
CSR	Consolidated Security Requirements

Term	Description
CSG	Consolidated Security Guidelines
EIS	eUICC Information Set
eUICC	Embedded UICC
EUM	Embedded UICC Manufacturer
FS.nn	Prefix identifier for official documents belonging to GSMA Fraud and Security Group
GSMA	GSM Association
ISI	Incoming Sensitive Information characterise the process sensitive inputs such as requests, files and keys.
IT	Information Technology
LDS	Local Discovery Service
LPA	Local Profile Assistant
LPD	Local Profile Download
LUI	Local User Interface
M2M	Machine-to-machine
MNO	Mobile Network Operator
OSI	Outgoing Sensitive Information characterise the process sensitive outputs such as responses, files and keys.
PRD	Permanent Reference Document
SAS-SM	Security Accreditation Scheme for Subscription Management Roles
SAS-UP	Security Accreditation Scheme for UICC Production
SGP.nn	Prefix identifier for official documents belonging to GSMA SIM Group
SM-DP	Subscription Manager – Data Preparation
SM-DP+	Subscription manager – Data Preparation (Enhanced compared to the SM-DP in SGP.02 [5])
SM-DS	Subscription Manager – Discovery Server
SM-SR	Subscription Manager – Secure Routing
SP	Sensitive Process
UICC	Universal Integrated Circuit Card

1.8 References

Ref	Doc Number	Title
[1]	PRD FS.09	GSMA SAS Methodology for Subscription Manager Roles
[2]	PRD FS.17	GSMA SAS Consolidated Security Requirements, latest version available at www.gsma.com/sas
[3]	PRD FS.18	GSMA SAS Consolidated Security Guidelines, available to participating sites from sas@gsma.com
[4]	PRD SGP.01	Embedded SIM Remote Provisioning Architecture
[5]	PRD SGP.02	Remote Provisioning Architecture for Embedded UICC Technical Specification
[6]	PRD SGP.21	Remote SIM Provisioning (RSP) Architecture V2.0

Ref	Doc Number	Title
[7]	PRD SGP 22	Remote SIM Provisioning (RSP) Technical Specification
[8]	RFC2119	“Key words for use in RFCs to Indicate Requirement Levels”, S. Bradner, March 1997. Available at http://www.ietf.org/rfc/rfc2119.txt

1.9 Conventions

The key words “must”, “must not”, “required”, “shall”, “shall not”, “should”, “should not”, recommended”, “may”, and “optional” in this document are to be interpreted as described in RFC2119 [8].

2 Process Definitions

The eUICC product life-cycle can be broken down into a number of phases:

#	Title	Description
1.	Software development	Basic software and operating system development; application software development, integration and validation
2.	IC design	IC development; hardware development, initialisation and test program development, integration and validation, initialisation of identification information and delivery keys
3.	Production	Manufacture, assembly and testing of the eUICC to be personalised.
4.	Personalisation of Initial Provisioning Profile	Receipt and processing of input data; production data generation and preparation; output data generation, preparation and transfer. Receipt and management of physical assets for personalisation, personalisation of assets, packaging and delivery. Re-work of defective or reject personalised assets
5.	Remote Provisioning and Management	Encompasses the functions for eUICC, Platform and Profile Management and Data Preparation as defined in SGP.01 [4] and SGP.21 [6]. For the machine-to-machine (M2M) use case, it commences when the SM-SR takes responsibility for the eUICC, including the registration of an eUICC to a SM-SR. It also includes MNO requests to create, personalise, download and install Profiles to the eUICC. These functions are provided by the SM-DP or the SM-DP+. Profile transport to eUICC and subsequent Platform Management of the Profiles, such as enabling, disabling, deletion (only M2M use case), and master deletion is provided by the SM-SR or the local profile assistant (LPA).
6.	End-of-life	When the eUICC reaches a stage where it can no longer perform the functions for which it was produced

Table 1 - eUICC Product Life-Cycle

This SAS-SM Standard is defined only for SM-DP, SM-SR, SM-DP+ and SM-DS activities within phase 5 – Remote Provisioning and Management that is, eUICC Management, Platform Management, Data Preparation and Profile Management.

3 Process Models

The life-cycle is used to depict the security target implementation. The representation of the steps within the process is based on data flows. All possible combinations are not described and chronological order is not necessarily represented.

3.1 Overall View

3.1.1 Remote SIM Provisioning for M2M

This schema is extracted from SGP.01 [4].

Three interfaces are defined for SM-DP:

- ES8 for Profile Management (between SM-DP and eUICC)
- ES3 for Profile and Platform Management (between SM-DP and SM-SR)
- ES2 for Profile and Platform Management (between SM-DP and MNO)

Five interfaces are defined for SM-SR:

- ES1 for eUICC provisioning ((between EUM and SM-SR)
- ES3 for Profile and Platform Management (between SM-DP and SM-SR)
- ES4 for Platform Management (between SM-SR and MNO)
- ES5 for Platform Management (between SM-SR and eUICC)
- ES7 for SM-SR change (between two SM-SR)

These interfaces are indicated in Figure 1. Proprietary interfaces not specified in SGP.02 [5] are those between the certificate issuer (CI) and the SM-DP and the SM-SR. These interfaces are used in certificate management. The certificate exchange operation is within scope of the audit.

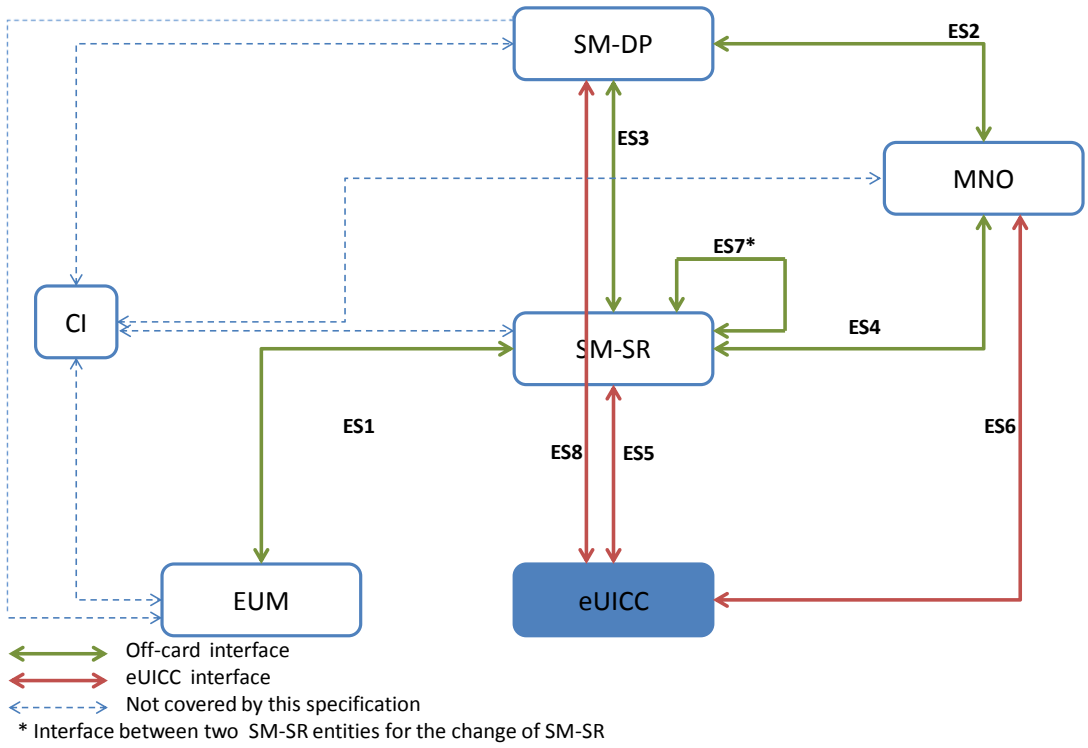


Figure 1 - eUICC Remote Provisioning System for M2M (SGP.02)

3.1.2 Remote SIM Provisioning for Consumer

This schema is extracted from SGP.21 [6].

Four interfaces are defined for SM-DP+:

- ES2+ for Profile and Platform Management (between SM-DP+ and MNO)

- ES8+ for Profile Management (between SM-DP+ and eUICC)
- ES9+ for Profile and Platform Management (between SM-DP+ and LPA)
- ES12 for Event Management (between SM-DP+ and SM-DS)

Three interfaces are defined for SM-DS:

- ES11 for Event Retrieval (between SM-DS and LDS)
- ES12 for Event Management (between SM-DS and SM-DP+)
- ES15 for Event Management (between two SM-DS)

These interfaces are indicated in Figure 2. Proprietary interfaces not specified in SGP.22 [7] are those between the CI and the SM-DP+ and the SM-DS. These interfaces are used in certificate management. The certificate exchange operation is within scope of the audit.

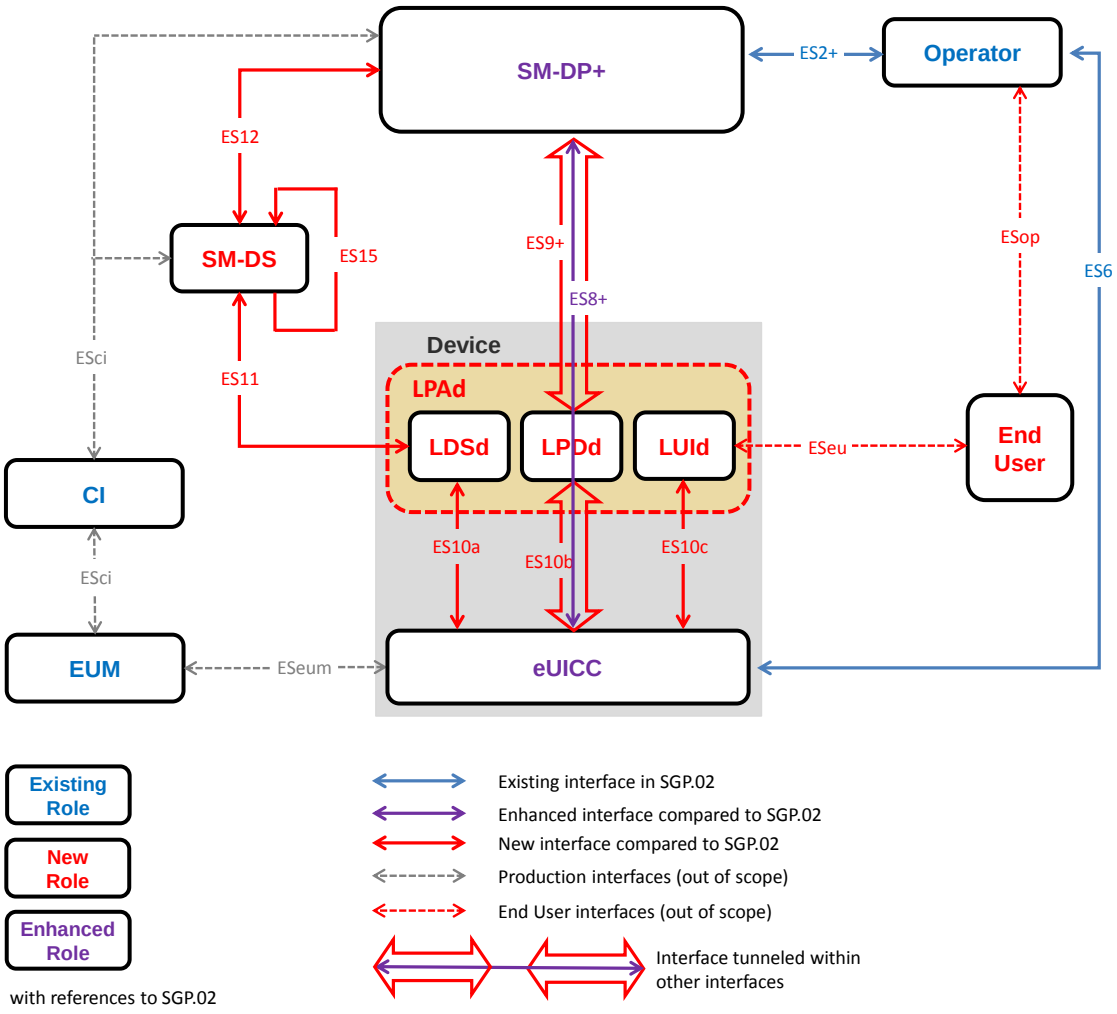


Figure 2 - eUICC Remote Provisioning System for RSP (SGP.22)

3.2 SM-SR

3.2.1 SM-SR Overview

The SM-SR enables, disables and deletes Profiles on the eUICC in accordance with the MNO's policy rules. The SM-SR is the only entity allowed to establish a transport channel to the eUICC to manage the eUICC platform.

Only one SM-SR can be associated with an eUICC at any point in time, but it can be changed during the lifetime of the eUICC.

The SM-SR obtains the Platform Management credentials of the eUICC from the eUICC Manufacturer or from the previous SM-SR.

3.2.2 SM-SR Processes

SM-SR processes include customer requests in various forms. A high level view of SM-SR processes are indicated in Figure 3.

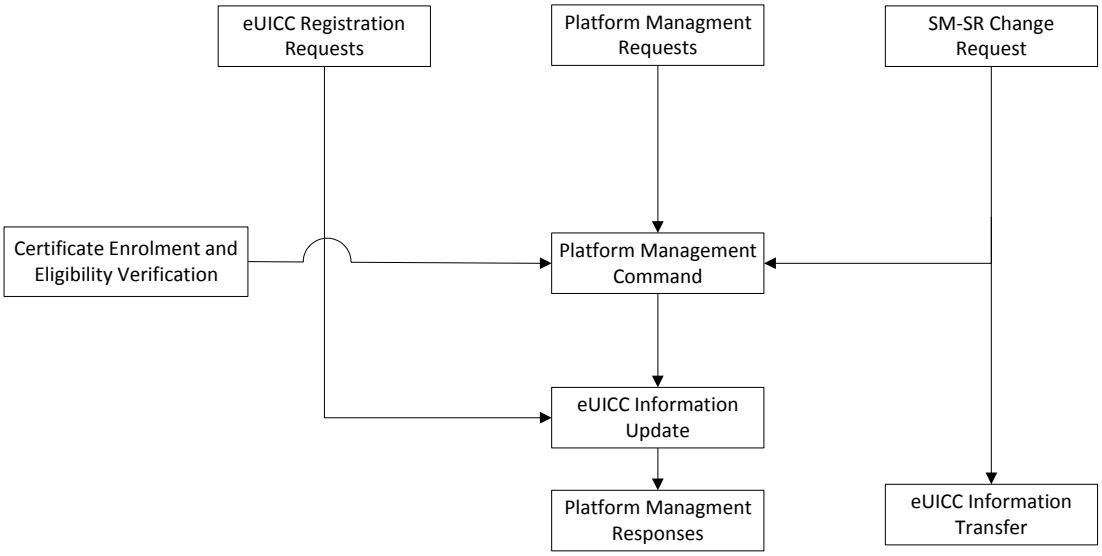


Figure 3 - SM-SR Processes

SM-SR processes consist of eUICC Registration, Platform Management and SM-SR Change. In addition to these, the SM-SR manages the authentication and authorisation of remote entities, indicated as 'Certificate Enrolment and Eligibility Verification' in Figure 3.

3.3 SM-DP

3.3.1 SM-DP Overview

The SM-DP acts on behalf of the MNO.

The SM-DP receives a Profile Description from the MNO and creates an un-personalised Profile.

The SM-DP generates Personalisation Data for the targeted eUICC (for example, network access credentials and other data) based upon data received from the MNO.

The SM-DP builds Personalised Profiles for the targeted eUICC. The SM-DP secures the Profile package with the Profile Installer Credentials of the targeted eUICC.

The SM-DP installs the Personalised Profile on the eUICC through the SM-SR.

On request of the MNO, the SM-DP also initiates Profile enabling, and Profile deletion requests to the eUICC via the SM-SR.

3.3.2 SM-DP Processes

SM-DP processes include customer requests in various forms. A high level view of SM-DP processes are indicated in Figure 4.

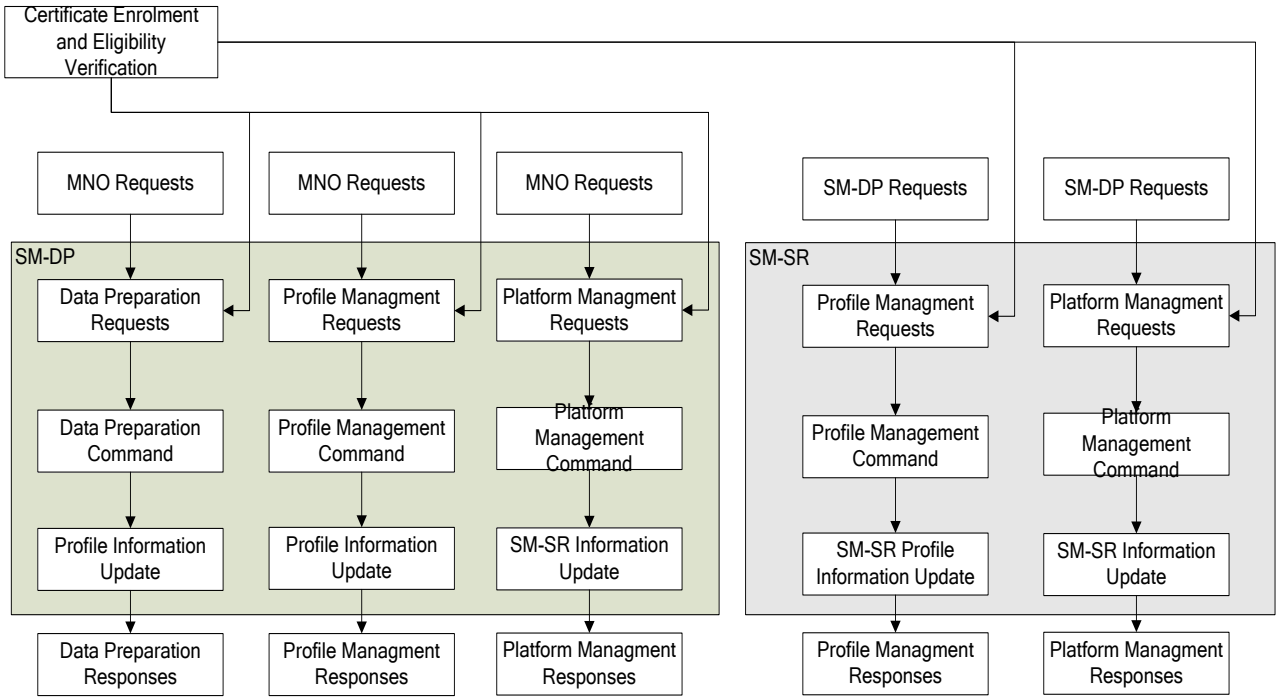


Figure 4 - SM-DP Processes

SM-DP processes consist of Data Preparation and Profile and Platform Management. In addition, the SM-DP manages the authentication and authorisation of remote entities, indicated as ‘Certificate Enrolment and Eligibility Verification’ in Figure 4.

NOTE If SM-SR and/or SM-DP components are distributed across multiple sites/systems and actively involved in SM-SR and/or SM-DP processes, the scope of the SAS certification process must include those sites/systems.

3.4 SM-DP+

3.4.1 SM-DP+ Overview

The SM-DP+ acts on behalf of the MNO.

The SM-DP+ receives a Profile Description from the MNO and creates an un-personalised Profile.

The SM-DP+ generates Personalisation Data for the targeted eUICC (for example, network access credentials and other data) based upon data received from the MNO.

The SM-DP+ builds Personalised Profiles for the targeted eUICC. The SM-DP secures the Profile package with the Profile Installer Credentials of the targeted eUICC.

The SM-DP+ installs the Personalised Profile on the eUICC through the LPA and the SM-DS.

3.4.2 SM-DP+ Processes

SM-DP+ processes include customer requests in various forms. A high level view of SM-DP processes are indicated in Figure 5.

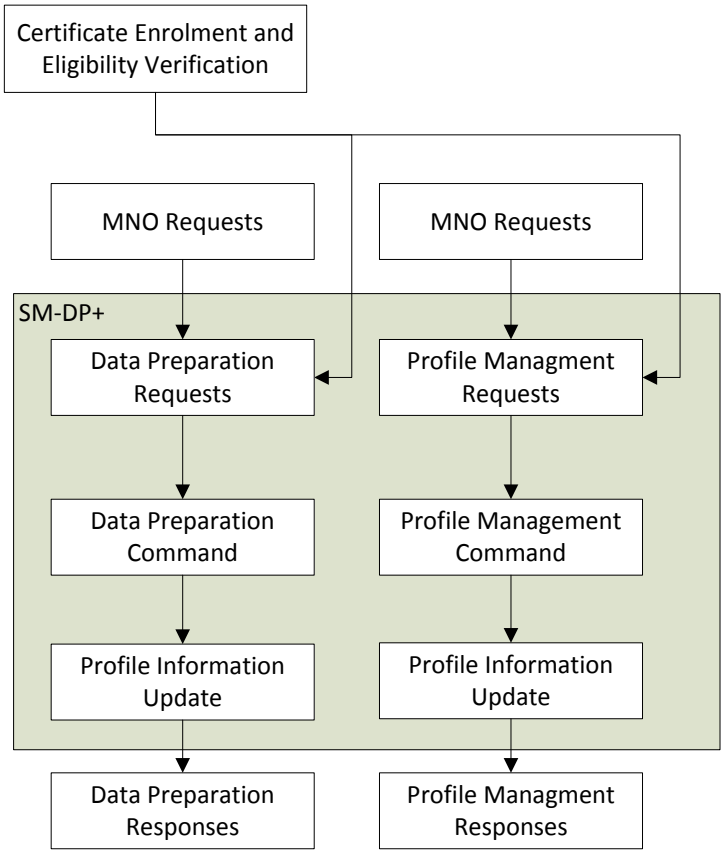


Figure 5 - SM-DP+ Processes

SM-DP+ processes consist of Data Preparation and Profile Management. In addition, the SM-DP+ manages the authentication and authorisation of remote entities, indicated as ‘Certificate Enrolment and Eligibility Verification’ in Figure 5.

3.5 SM-DS

3.5.1 SM-DS Overview

The role of the SM-DS is to provide mechanisms that allow an SM-DP+ to inform the LDS within any device that an SM-DP+ wishes to communicate with it. The purpose of the SM-DS to LDS communication SHALL be informing the LDS of a pending event.

3.5.2 SM-DS Processes

SM-DS processes include customer requests in various forms. A high level view of SM-SR processes are indicated in Figure 6.

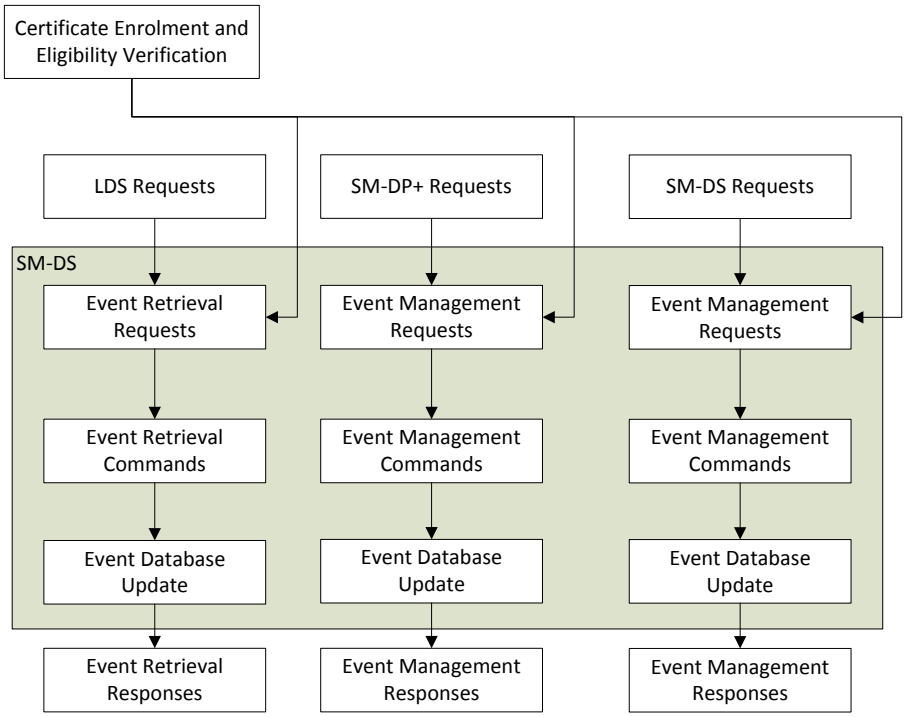


Figure 6 – SM-DS Processes

3.6 Actors

There are four classes of Actor:

- Internal Authorised – [**INT_AUTH**] – Employees authorised to access the Sensitive Process (SP) and supporting Environment (for example, System Administrator, Support & Maintenance user).
- Internal Unauthorised – [**INT_UNAU**] – Employees not authorised to access the SP. But can access the supporting Environment (for example, IT Administrator).
- External Authorised – [**EXT_AUTH**] – third party with authority to access the SP and supporting Environment (for example, an SM-SR, an SM-DP or MNO).
- External Unauthorised – [**EXT_UNAU**] – third party not authorised to access the SP or supporting Environment (for example, physical data centre, attacker and hacker).

4 Assets

4.1 Introduction

Assets may be of different types, such as information, processes and systems. Within SM-DP, SM-SR, SM-DP+ or SM-DS the processes, information assets and SM-DP, SM-SR, SM-DP+ or SM-DS system assets must be controlled and closely supervised so that they are secure.

System assets of different types, such as servers, firewall, load balancers and software included in the SP environment must also be protected and security requirements are set out in [CSR]

4.2 SM-DP Assets

SM-DP information assets are laid out in Table 2.

Incoming Sensitive Information (ISI)	Outgoing Sensitive Information (OSI)
POL2 (ISI_PRM_POL2)	POL2 (OSI_PRM_POL2)
eUICC Information (ISI_EIS_CLASS_2)	eUICC Information (OSI_EIS_CLASS_2)
eUICC Information (ISI_EIS_CLASS_1)	eUICC Information (OSI_EIS_CLASS_1)
Platform Management Requests (ISI_PMR)	Platform Management Request Responses (OSI_PMRR)
Profile Management Requests (ISI_PrMR)	Profile Management Request Responses (OSI_PrMRR)
Data Preparation Requests (ISI_DPR)	Data Preparation Request Responses (OSI_DPRR)
Remote Entities Authentication and Authorization Credentials (ISI_AACRE)	Remote Entities Authentication and Authorization Credentials (OSI_AACRE)
Profile Management Command Responses (ISI_PrMCR)	Profile Management Command (OSI_PrMC)
Platform Management Command Responses (ISI_PlMCR)	Platform Management Command (OSI_PLMC)
MNO's Profile Description (ISI_MPD)	Profile Metadata including POL1 (OSI_PRM)
Keys (MNO_KEY, ASI_KEY)	
POL1 (ISI_PRM_POL1)	

Additional Sensitive Information (ASI)	Cryptographic Keys (KEY)
Customer Information (ASI_CUI)	Secret Keys (KEY _SEC)
Other Management Data (ASI_MAD)	Public Keys (KEY_PUB)
	Private Keys (KEY_PRI)

Table 2 - SM-DP Information Assets

The SM-DP system assets are laid out in Table 3.

Software (SW)
SM-DP application software (SW_SM-DP)

Table 3 - SM-DP System Assets

4.3 SM-SR Assets

SM-SR information assets are laid out in Table 4.

Incoming Sensitive Information (ISI)
Platform Management Requests (ISI_PMR)
Platform Management Command Responses (ISI_PLMCR)
eUICC Information (ISI_EIS)
Profile Metadata (ISI_PRM)
Remote Entities Authentication and Authorization Credentials (ISI_AACRE)

Outgoing Sensitive Information (OSI)
Platform Management Commands (OSI_PLMC)
eUICC Management Commands (OSI_EMC)
Remote Entities Authentication and Authorization Credentials (OSI_AACRE)
Profile Metadata (OSI_PRM)
eUICC Information (OSI_EIS)
Request Responses (OSI_RES)

Additional Sensitive Information (ASI)
Customer Information (ASI_CUI)
Other Management Data (ASI_MAD)

Cryptographic Keys (KEY)
Secret Keys (ASI_KEY)
Public Keys (KEY_PUB)
Private Keys (KEY_PRI)

Table 4 - SM-SR Information Assets

The primary SM-SR system assets are laid out in Table 5.

Software (SW)
SM-SR application software (SW_SM-SR)

Table 5 - SM-SR System Assets

4.4 SM-DP+ Assets

SM-DP+ information assets are laid out in Table 2.

Incoming Sensitive Information (ISI)
eUICC Information (ISI_EIS)
Keys (MNO_KEY, ASI_KEY)
MNO's Profile Description (ISI_MPD)
Remote Entities Authentication and Authorization Credentials (ISI_AACRE)
Profile Management Requests

Outgoing Sensitive Information (OSI)
eUICC Information (OSI_EIS_CLASS_2)
Profile Metadata (OSI_PRM)
Profile Management Command (OSI_PrMC)
Profile Management Request Responses (OSI_PrMRR)
Platform Management Request

(ISI_PrMR)	Responses (OSI_PMRR)
Data Preparation Requests (ISI_DPR)	Data Preparation Request Responses (OSI_DPRR)
Profile Management Command Responses (ISI_PrMCR)	Remote Entities Authentication and Authorization Credentials (OSI_AACRE)
PPR Information (ISI_PRM_PPR)	Event Management Requests (Registration or Deletion) (OSI_EMR)
Device Information (ISI_DEV)	

Additional Sensitive Information (ASI)	Cryptographic Keys (KEY)
Customer Information (ASI_CUI)	Secret Keys (KEY _SEC)
Other Management Data (ASI_MAD)	Public Keys (KEY_PUB)
	Private Keys (KEY_PRI)

Table 6 - SM-DP+ Information Assets

The SM-DP+ system assets are laid out in Table 3.

Software (SW)
SM-DP+ application software (SW_SM-DP+)

Table 7 - SM-DP+ System Assets

4.5 SM-DS Assets

SM-DS information assets are laid out in Table 8.

Incoming Sensitive Information (ISI)	Outgoing Sensitive Information (OSI)
Event Record (ISI_ER)	Event Management (Registration or Deletion) Requests (OSI_EMR)
Discovery Server Requests (ISI_DSR)	Discovery Server Responses (OSI_DSR)
Event Management (Registration or Deletion) Requests (ISI_EMR)	Remote Entities Authentication and Authorization Credentials (OSI_AACRE)
Remote Entities Authentication and Authorization Credentials (ISI_AACRE)	Audit logs (OSI_LOG)

Additional Sensitive Information (ASI)	Cryptographic Keys (KEY)
Customer Information (ASI_CUI)	Secret Keys (ASI_KEY)
Other Management Data (ASI_MAD)	Public Keys (KEY_PUB)
	Private Keys (KEY_PRI)

Table 8 - SM-DS Information Assets

The SM-DS system assets are laid out in Table 9.

Software (SW)
SM-DS application software (SW_SM-DS)

Table 9 - SM-DS System Assets

4.6 Asset Classification

Assets that require protection are in various forms within SM-DP, SM-SR, SM-DP+ or SM-DS processes. The protection required can be complex unless arranged logically in classes. A classification table is contained in Annex A.

4.7 Asset Characteristics

Files and data are transmitted, stored and used in many media and transport forms.

4.8 SM-DP Incoming Sensitive Information

Incoming sensitive information (ISI) includes:

- eUICC Information [**ISI_EIS_CLASS1**] containing classified information which must be protected in terms of integrity, confidentiality, authenticity and availability commensurate with the highest class of information contained in the SM-DP [**ISI_EIS_CLASS1**].
- eUICC Information [**ISI_EIS_CLASS2**] containing classified information which must be protected in terms of integrity, authenticity and availability commensurate with the highest class of information contained in the SM-DP [**ISI_EIS_CLASS2**].
- Keys [**MNO_KEY, ASI_KEY**] containing classified information which must be protected in terms of integrity, confidentiality, authenticity and availability commensurate with the highest class of information contained in the SM-DP.
- MNO's Profile Description [**ISI_MPD**] whose integrity and availability must be protected.
- Remote Entities Authentication and Authorization Credentials [**ISI_AACRE**] which must be protected in terms of availability and integrity.
- Platform Management Requests [**ISI_PMR**] whose authenticity, integrity and availability must be protected.
- Profile Management Requests [**ISI_PrMR**] whose authenticity, integrity and availability must be protected.
- Data Preparation Requests [**ISI_DPR**] whose authenticity, integrity and availability must be protected.
- Profile Management Command Responses from the SM-SR [**ISI_PrMCR**] whose authenticity, integrity and availability must be protected.
- Platform Management Command Responses from the SM-SR [**ISI_PlMCR**] whose authenticity, integrity and availability must be protected.
- POL1 Information [**ISI_PRM_POL1**] containing classified information which must be protected in terms of integrity, confidentiality, authenticity and availability commensurate with the highest class of information contained in the SM-DP [**ISI_PRM_POL1**].
- POL2 Information [**ISI_PRM_POL2**] containing classified information which must be protected in terms of integrity, authenticity and availability [**ISI_PRM_POL2**].

4.9 SM-DP+ Incoming Sensitive Information

Incoming sensitive information (ISI) includes:

- eUICC Information [**ISI_EIS**] containing classified information which must be protected in terms of integrity, authenticity and availability commensurate with the highest class of information contained in the SM-DP+ .
- Keys [**MNO_KEY, ASI_KEY**] containing classified information which must be protected in terms of integrity, confidentiality, authenticity and availability commensurate with the highest class of information contained in the SM-DP+.
- MNO's Profile Description [**ISI_MPD**] whose integrity and availability must be protected.
- Remote Entities Authentication and Authorization Credentials [**ISI_AACRE**] which must be protected in terms of availability and integrity.
- Profile Management Requests [**ISI_PrMR**] whose authenticity, integrity and availability must be protected.
- Data Preparation Requests [**ISI_DPR**] whose authenticity, integrity and availability must be protected.
- Profile Management Notification from the eUICC [**ISI_PrMCR**] whose authenticity, integrity and availability must be protected.
- PPR Information [**ISI_PRM_PPR**] containing classified information which must be protected in terms of integrity, confidentiality, authenticity and availability commensurate with the highest class of information contained in the SM-DP+ [**ISI_PRM_PPR**].
- Device Information [**ISI_DEV**] containing classified information which must be protected in terms of integrity, authenticity and availability.

4.10 SM-SR Incoming Sensitive Information

Incoming sensitive information (ISI) includes:

- eUICC Information [**ISI_EIS**] containing classified information which must be protected in terms of integrity, confidentiality and availability commensurate with the highest class of information contained in the SM-SR [**ISI_EIS**].
- Profile Metadata [**ISI_PRM**] whose confidentiality, integrity and availability must be protected.
- Remote Entities Authentication and Authorization Credentials [**ISI_AACRE**] which must be protected in terms of availability and integrity.
- Platform Management Requests [**ISI_PMR**] whose authenticity, integrity and availability must be protected.
- Platform Management Command Responses from the eUICC [**ISI_PLMCR**] whose authenticity, integrity and availability must be protected.

4.11 SM-DS Incoming Sensitive Information

Incoming sensitive information (ISI) includes:

- Event Record [**ISI_ER**] containing classified information which must be protected in terms of integrity, confidentiality and availability [**ISI_EIS**].

- Remote Entities Authentication and Authorization Credentials [**ISI_AACRE**] which must be protected in terms of availability and integrity.
- Discovery Server Requests [**ISI_DSR**] whose authenticity, integrity and availability must be protected.
- Event Management (Registration or Deletion) Requests [**ISI_EMR**] whose authenticity, integrity and availability must be protected.

4.12 SM-DP Outgoing Sensitive Information

Outgoing sensitive information (OSI) includes:

- eUICC Information [**OSI_EIS_CLASS1**] containing classified information which must be protected in terms of integrity, authenticity, confidentiality, and availability commensurate with the highest class of information contained in the SM-DP.
- eUICC Information [**OSI_EIS_CLASS2**] containing classified information which must be protected in terms of integrity, authenticity, and availability commensurate with the highest class of information contained in the SM-DP.
- Profile Metadata [**OSI_PRM**] whose confidentiality, authenticity, integrity and availability must be protected.
- Profile Management Commands [**OSI_PrMC**] towards SM-SR whose authenticity and integrity must be protected.
- Platform Management Commands [**OSI_PlMC**] towards the SM-SR whose authenticity and integrity must be protected.
- Platform Management Requests Responses [**OSI_PMRR**] to the MNO whose authenticity and integrity must be protected.
- Profile Management Requests Responses [**OSI_PrMRR**] to the MNO whose authenticity and integrity must be protected.
- Data Preparation Requests Responses [**OSI_DPRR**] to the MNO whose authenticity and integrity must be protected.
- SM-DP Authentication and Authorization Credentials [**OSI_AACRE**] which must be protected in terms of availability and integrity.
- POL2 Information [**OSI_PRM_POL2**] containing classified information which must be protected in terms of integrity, authenticity and availability [**OSI_PRM_POL2**].

In all cases, if the information contains different classes of data the higher class shall prevail.

4.13 SM-DP+ Outgoing Sensitive Information

Outgoing sensitive information (OSI) includes:

- eUICC Information [**OSI_EISCLASS2**] (e.g. EID) toward MNO or SM-DS, containing classified information which must be protected in terms of integrity, authenticity, and availability commensurate with the highest class of information contained in the SM-DP+.
- Profile Metadata [**OSI_PRM**] toward LPA whose authenticity, integrity and availability must be protected.
- Profile Management Commands [**OSI_PrMC**] towards LPA whose confidentiality, authenticity and integrity must be protected.

- Profile Management Requests Responses [**OSI_PrMRR**] to the MNO whose authenticity and integrity must be protected.
- Data Preparation Requests Responses [**OSI_DPRR**] to the MNO whose authenticity and integrity must be protected.
- SM-DP+ Authentication and Authorization Credentials [**OSI_AACRE**] which must be protected in terms of availability and integrity.
- Event Management (Registration or Deletion) Requests towards SM-DS [**OSI_EMR**] whose authenticity, integrity and availability must be protected.

In all cases, if the information contains different classes of data the higher class shall prevail.

4.14 SM-SR Outgoing Sensitive Information

Outgoing sensitive information (OSI) includes:

- eUICC Information [**OSI_EIS**] containing classified information which must be protected in terms of integrity, confidentiality, and availability commensurate with the highest class of information contained in the SM-SR [**OSI_EIS**].
- Profile Metadata [**OSI_PRM**] whose confidentiality, integrity and availability must be protected.
- Platform Management Commands [**OSI_PLMC**] towards the eUICC whose confidentiality, availability and integrity must be protected.
- eUICC Management Commands [**OSI_EMC**] towards other SM-SR whose authenticity, availability and integrity must be protected.
- Other SM-SR Authentication and Authorization Credentials [**OSI_AACRE**] which must be protected in terms of availability and integrity.
- Request responses [**OSI_RES**] generated by the SM-SR whose authenticity, integrity and availability must be protected.

In all cases, if the information contains different classes of data the higher class shall prevail.

4.15 SM-DS Outgoing Sensitive Information

Outgoing sensitive information (OSI) includes:

- Remote Entities Authentication and Authorization Credentials [**OSI_AACRE**] which must be protected in terms of availability and integrity.
- Event Management (Registration or Deletion) Requests [**OSI_EMR**] whose authenticity, integrity and availability must be protected.
- Discovery Server Responses [**OSI_DSR**] whose authenticity, integrity and availability must be protected.
- Audit logs [**OSI_LOG**]

4.16 Additional Sensitive Information (ASI)

Additional sensitive information (ASI) is:

- Customer information [**ASI_CUI**] from SM-DP, SM-SR, SM-DP+ or SM-DS that is created or can be obtained inside or by a third party attack. Customer information can be recorded in the following systems:

  - Transmission and ciphering systems [**DE_TRA**]
  - Testing systems [**DE_TST**]
  - Production systems [**DE_PRD**]

- Management Data [**ASI_MAD**], information on the management of SM-DP, SM-SR, SM-DP+ or SM-DS systems. This can consist of:

  - [**SEN_MAT**] traceability information which should allow the supplier identify the user, or group of users, who worked on SM-DP or SM-SR systems.
  - [**SEN_MAU**] audit information which should be available in relation to the recorded Remote Provisioning and Management history of a eUICC subject to local laws.

- [**SEN _ISD-P_KEYS**], transport keys used by SM-DP to encrypt the Profile sent to the eUICC.

Sensitive information includes all data, particularly working, temporary or safeguarded data that contain the information outlined above.

4.17 Cryptographic Keys [KEY]

Cryptographic keys [KEY] include:

- Secret Keys [**KEY_SEC**] whose confidentiality, authenticity, integrity and availability must be protected.
- Private keys [**KEY_PRI**] whose confidentiality, authenticity, integrity and availability must be protected.
- Public keys [**KEY_PUB**] whose authenticity, integrity and availability must be protected.

5 Threats

5.1 Introduction

A threat analysis has been completed to identify the main threats to SM-DP, SM-SR, SM-DP+ and SM-DS. The list is not intended to be exhaustive.

The main threats to data are loss of availability, confidentiality and integrity.

The threats are listed in sections 5.2 and 5.3 independently of the process step concerned.

In the threat description, data means all type of data assets described in Section 4.

5.2 Direct Threats Description

Threats	Actors	Assets	Description
T_LOSS	INT_AUTH INT_UNAU EXT_AUTH EXT_UNAU	ALL SENSITIVE ASSETS	Loss or theft or unrequested or unauthorized removal of classified assets (1, 2)
T_CONT	INT_AUTH	OSI_PMRR	Accidental or deliberate cross-contamination of assets in the SM-

Threats	Actors	Assets	Description
	INT_UNAU EXT_AUTH EXT_UNAU	OSI_PrMC OSI_PLMC	DP, SM-SR, and SM-DP+.
T_DISC	INT_AUTH INT_UNAU EXT_AUTH EXT_UNAU	ALL ASSETS CONTAINING CLASSIFIED INFORMATION	Disclosure of classified information
T_MODIF	INT_AUTH INT_UNAU EXT_AUTH	ALL ASSETS CONTAINING CLASSIFIED INFORMATION	Unauthorised modification of classified information causing loss of integrity through error or malevolence
T_FAKE_ACT	EXT_AUTH EXT_UNAU	ALL SENSITIVE ASSETS	Fake Actor accepted as an authorized entity
T_FAKE_PlMC	INT_AUTH INT_UNAU	OSI_PMRR	Unauthorized Platform Management requests sent to remote entities for example, SM-SR.
T_FAKE_PrlMC	INT_AUTH INT_UNAU	OSI_PrMC OSI_PLMC	Unauthorized Profile Management commands sent to remote entities for example, SM-SR and eUICC.
T_LOSS_AVAIL	INT_AUTH INT_UNAU EXT_AUTH EXT_UNAU	ALL ASSETS	Accidental or deliberate loss of availability of SM-DP, SM-SR, SM-DP+ and SM-DS functionality.

Table 10 - Direct Threats Description

Additional threats can result from combinations of those threats listed above.

5.3 Indirect Threats Description

Threats	Actors	Assets	Description
T_SEF	ANY	ANY	Accidental or deliberate security failure.

Table 11 - Indirect Threats Description

6 Security Objectives

6.1 Introduction

Organisations providing SM-DP, SM-SR, SM-DP+ or SM-DS functions are responsible for protecting assets from security risks to which they are exposed defined by the security objectives. It is this protection that provides assurance to the MNOs. The security objectives relate to both the Sensitive Process and its Environment. All objectives must be addressed but higher levels of assurance are needed depending on the asset classification.

6.2 Security Objectives for the Sensitive Process

#	Objective	Threat	Description
1	The SP must control the SM-DP, SM-SR, SM-DP+ or SM-DS processes	T_LOSS T_MODIF T_CONT, T_FAKE_PMC	To prevent • clone, mismatch, anomalies • any non-conforming actions due to use of components not compliant with SGP.01 [4] and SGP.02 [5] for SM-DP and SM-SR • any non-conforming actions due to use of components not compliant with SGP.21 [4] and SGP.22 [5] for SM-DP+ and SM-DS
2	The SP must control, manage and protect data against loss of integrity and confidentiality	T_LOSS T_DISC T_MODIF	To prevent: • any disclosure of assets • any non-conforming action due to loss of integrity
3	The SP must guarantee a secure process flow	T_LOSS T_DISC T_SEF T_CONT	To prevent theft, loss, misappropriation of assets
4	The SP must manage the elements that are specified as auditable	T_MODIF	To look for possible or real security violations.
5	The SP must be designed in such a way that independence of different customer data (asset) is always achieved	T_DISC	To prevent one customer's data being disclosed to another customer.
6	The SP must guarantee that fake remote entity authentication is discovered	T_FAKE_ACT	To prevent illegitimate action from fake entities.
7	The SP must be designed in such way that its availability is within defined SLA	T_LOSS_AVAIL	To prevent loss of service availability and maintain business continuity.

Table 12 - Security Objectives for the Sensitive Process

6.3 Security Objectives for the Environment

#	Objective	Threat	Description
1	The SP Environment must manage the elements that are specifically auditable	T_SEF	To look for possible or real security violations
2	The SP Environment must guarantee secure SM-DP, SM-SR, SM-DP+ or SM-DS functionality	T_SEF	To prevent theft, loss or misappropriation of assets

Table 13 - Security Objectives for the Environment

7 Security Requirements

7.1 Introduction

Certain requirements must be met to consider the SM-DP processes as being secure. These requirements are specified in the SAS Consolidated Security Requirements (CSR) document [2] as relevant to subscription management, and supported by the Consolidated Security Guidelines (CSG) [3], specifically addressing the requirements for:

- Policy, strategy and documentation (including business continuity planning)
- Organisation and responsibility
- Information
- Personnel security
- Physical security
- Certificate and key management
- Sensitive process data management
- SM-DP, SM-SR, SM-DP+ and SM-DS service management
- Computer and network management

These requirements are considered as minimum-security requirements for the Environment in which the SP is used.

The requirements of the SAS-SM Standard should be met by established processes / controls for which evidence of correct operation exists.

Annex A Assets

A.1 Class Definition

	Availability	Integrity	Authenticity	Confidentiality
Class 1	**X**	**X**	**X**	**X**
Class 2	**X**	**X**	**X**	**-**
Class 3	**X**	**-**	**-**	**-**

A.2 SM-DP Assets Classification

Code	Asset	Class
ASI_EIS_ISD-P	Information related to the ISD-P for example, keys to manage the Profile Lifecycle	**1**
MNO_KEY	MNO Cryptographic keys (for example, Ki, OP, OPC, IMSI, ISD and SSD keys)	**1**
ASI_KEY	Clear cryptographic keys/key components protecting class 1 assets for confidentiality and integrity. An asset protected by these cryptographic keys is considered a class 2 asset.	**1**
KEY_PRI	The private component of the asymmetric key pair	**1**
KEY_PUB	The public component of the asymmetric key pair	**2**
OSI_PRM	Profile Metadata	**1**
ISI_EIS_CLASS1	Incoming eUICC information.	**1**
OSI_EIS_CLASS 1	Outgoing eUICC information.	**1**
ISI_PRM_POL1	POL1 for Profile	**1**
ISI_PRM_POL2	POL2 for Profile	**2**
OSI_PRM_POL2	POL2 for Profile	**2**
ASI_MAD	Other management data. Information on the remote provisioning of eUICCs. This may contain: • Traceability information, which should allow the supplier to identify the person(s) who worked on a request. Audit information related to the remote provisioning history of a eUICC or batch of eUICCs.	**2**
ISI_EIS_CLASS2	Incoming eUICC information.	**2**
OSI_EIS_CLASS 2	Outgoing eUICC information.	**2**
OSI_RES	Outgoing information - for example to inform an MNO of the result of a Platform Management operation.	**2**
ISI_PMR	Incoming Platform Management Request	**2**
ISI_PrMR	Incoming Profile Management Request	**2**
ISI_DPR	Incoming Data Preparation Request	**2**
OSI_PIMC	Outgoing Platform Management command.	**2**
OSI_PrMC	Outgoing Profile Management command.	**2**

Code	Asset	Class
OSI_PMRR	Platform Management Request Responses	**2**
OSI_PrMRR	Profile Management Request Responses	**2**
OSI_DPRR	Data Preparation Request Responses	**2**
ISI_MPD	Description of the MNO Profile structure to be used to create the personalised Profile in the eUICC (un-personalised Profile).	**2**

Table 14 - SM-DP Assets Classification

A.3 SM-SR Assets Classification

Code	Asset	Class
ASI_KEY	Clear cryptographic keys/key components protecting class 1 assets for confidentiality and integrity. An asset protected by these cryptographic keys is considered a class 2 asset. A cryptographic key that is used with a secret-key (symmetric) cryptographic algorithm that is uniquely associated with one or more entities and is not made public.	**1**
ISI_EIS	Incoming eUICC information.	**1**
KEY	Clear cryptographic keys/key components protecting class 1 assets for confidentiality and integrity. An asset protected by these cryptographic keys is considered a class 2 asset.	**1**
KEY_PRI	The private component of the asymmetric key pair	**1**
OSI_EIS	Outgoing eUICC information. If the information contains class 1 information (e.g. ISD-R key), this information has to be Class 1 protected	**1**
ASI_MAD	Other management data. Information on the remote provisioning of eUICCs. This may contain: • Traceability information, which should allow the supplier to identify the person(s) who worked on a request. • Audit information related to the remote provisioning history of a eUICC or batch of eUICCs.	**2**
ISI_AACRE	Remote Entities Authentication and Authorisation Credentials	**2**
ISI_PLMCR	Platform Management Command Responses from the eUICC	**2**
ISI_PMR	Incoming Platform Management Request	**2**
ISI_PRM_POL2	POL2 for Profile	**2**
KEY_PUB	The public component of the asymmetric key pair	**2**
OSI_AACRE	Other SM-SR Authentication and Authorisation Credentials	**2**
OSI_EMC	Outgoing eUICC management commands towards other SM-SR	**2**
OSI_PLMC	Outgoing Platform Management command.	**2**
OSI_PRM_POL2	POL2 for Profile	**2**
OSI_RES	Outgoing information - for example to inform an MNO of the result of a Platform Management operation.	**2**

Table 15 - SM-SR Assets Classification

A.4 SM-DP+ Assets Classification

Code	Asset	Class
MNO_KEY	MNO Cryptographic keys (for example, Ki, OP, OPC, IMSI, ISD and SSD keys)	**1**
ASI_KEY	Clear cryptographic keys/key components protecting class 1 assets for confidentiality and integrity. An asset protected by these cryptographic keys is considered a class 2 asset.	**1**
OSI_PRM	Profile Metadata	**2**
ISI_PRM_PPR	Profile Policy Rule for Profile	**1**
ISI_EIS	Incoming eUICC information.	**2**
ASI_MAD	Other management data. Information on the remote provisioning of eUICCs. This may contain: • Traceability information, which should allow the supplier to identify the person(s) who worked on a request. Audit information related to the remote provisioning history of a eUICC or batch of eUICCs.	**2**
ISI_EIS	Incoming eUICC information.	**2**
OSI_EIS	Outgoing eUICC information.	**2**
ISI_PrMR	Incoming Profile Management Request	**2**
ISI_DPR	Incoming Data Preparation Request	**2**
ISI_DEV	Device Information (IMEI, TAC, Device Capabilities)	**2**
OSI_PrMC	Outgoing Profile Management command.	**1**
OSI_PrMRR	Profile Management Request Responses	**2**
OSI_DPRR	Data Preparation Request Responses	**2**
OSI_PrMCI	Profile Management Command Identifier (Event ID)	**2**
ISI_MPD	Description of the MNO Profile structure to be used to create the personalised Profile in the eUICC (un-personalised Profile).	**2**
KEY_PRI	The private component of the asymmetric key pair	**1**
KEY_PUB	The public component of the asymmetric key pair	**2**

A.5 SM-DS Assets Classification

Code	Asset	Class
ISI_ER	Event Record	**2**
ISI_DSR	Discovery Server Requests	**2**
ISI_EMR	Event Management (Registration or Deletion) Requests	**2**
ISI_AACRE	Remote Entities Authentication and Authorization Credentials	**2**
ASI_CUI	Customer Information	**2**
ASI_MAD	Other Management Data	**2**
ASI_KEY	Clear cryptographic keys/key components protecting class 1 assets for confidentiality and integrity. An asset protected by these cryptographic keys is considered a class 2 asset.	**1**
KEY_PUB	The public component of the asymmetric key pair	**2**

Code	Asset	Class
KEY_PRI	The private component of the asymmetric key pair	**1**
OSI_EMR		**2**
OSI_DSR		**2**
OSI_AACRE	Remote Entities Authentication and Authorization Credentials	**2**
OSI_LOG		**2**

Table 16 - SM-DS Assets Classification

A.6 EIS Asset Details and Classification

Data Level 1 name	Data Level 2 name	Asset Class
Eid		**2**
eum-id		**2**
productionDate		**2**
platformType		**2**
platformVersion		**2**
remainingMemory		**2**
Availablememoryforprofiles		**2**
lastAuditDate		**2**
smsr-id		**2**
isd-p-loadfile-aid		**2**
isd-p-module-aid		**2**
Profiles*		
	Iccid	**2**
	isd-p-aid	**2**
	mno-id	**2**
	fallbackAttribute	**2**
	subscriptionAddress	**2**
	Msisdn	**2**
	Imsi	**2**
	State	**2**
	smdp-id	**2**
	ProfileType	**2**
	allocatedMemory	**2**
	freeMemory	**2**
	pol2	**2**
ISD-R		**1**
ECASD		**2**
eUICC-Capabilities		**2**
	CAT-TP-Support	**2**

Data Level 1 name	Data Level 2 name	Asset Class
	CAT-TP-Version	**2**
	HTTP-Support	**2**
	HTTP-Version	**2**
	secure-packet-version	**2**
	Remote-provisioning-version	**2**
audit trail		**2**
eumCertificateId		**2**
signatureAlgorithm		**2**
Signature		**2**

Table 17 - EIS Asset Details and Classification

* Note Profile classification level inherits the strongest classification level of the data contained.

Annex B Personalisation Flow

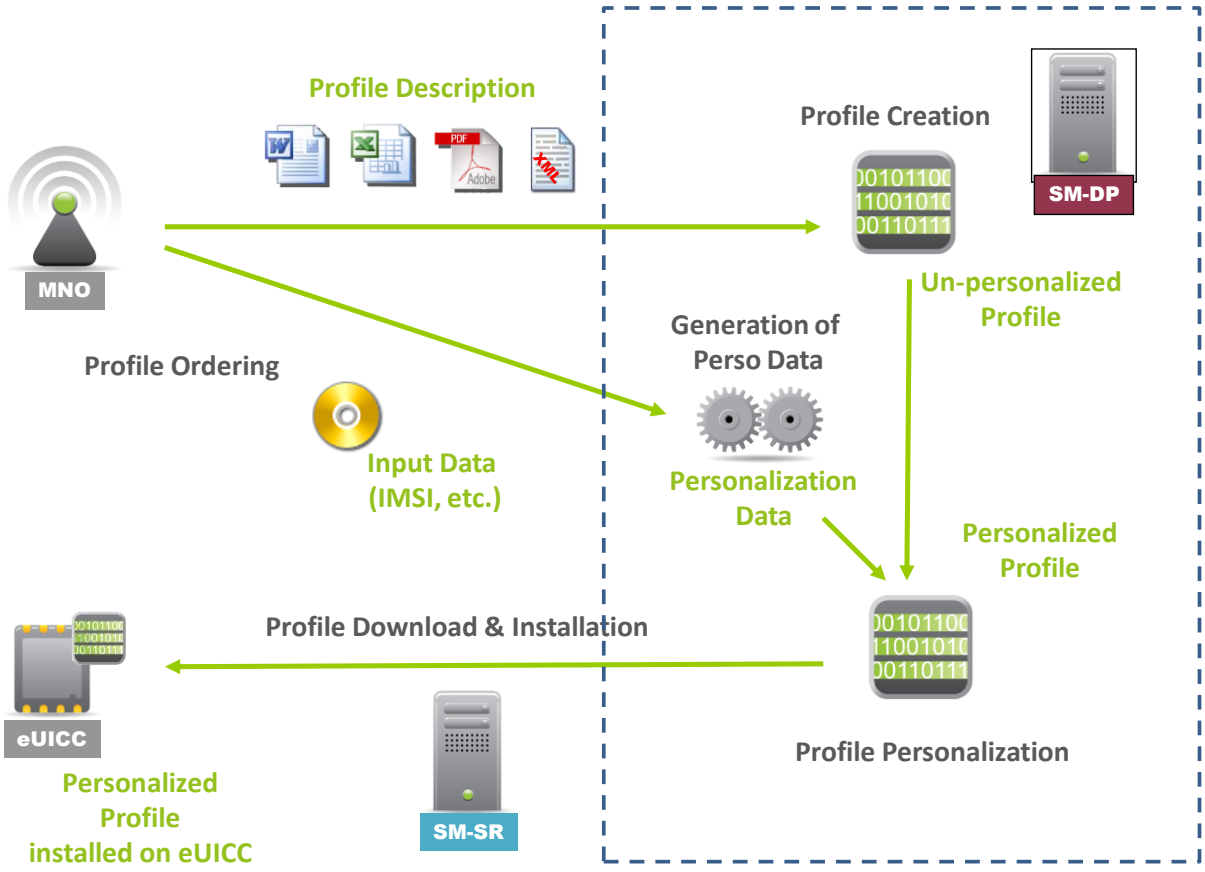


Figure 7 - Personalisation Flow

Annex C Document Management

C.1 Document History

Version	Date	Brief Description of Change	Editor / Company
1.0	13 October 2014	PSMC approved, first release	Arnaud Danree, Oberthur
2.0	13 May 2015	Updated and transferred to FASG	Arnaud Danree, Oberthur
3.0	31 Mar 2017	Updated to reflect use of Consolidated Security Requirements (CSR) and Consolidated Security Guidelines (CSG) for SAS-SM, and extension of SAS-SM to support auditing and certification of SM-DP+ and SM-DS solutions.	RSPSAS subgroup

C.2 Other Information

Type	Description
Document Owner	GSMA Fraud and Security Group
Editor / Company	Saïd Gharout, Orange

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