GSMA SAS Standard for Subscription Manager Roles

Version 2.0

13 May 2015

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) and Subscription Manager – Data Preparation (SM-DP) 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 or SM-SR suppliers. The purpose of the SAS standard is;

- to minimise risks to MNOs introduced by SM-DP or SM-SR functionality and,
- to provide a set of auditable requirements, together with the associated FS.10 [2] and FS.09 [1], to allow SM-DP or SM-SR suppliers provide assurance to their customers that risks are controlled.

Functional requirements and security objectives applicable to organisations in the role of SM-SR and/or SM-SP are herein outlined.

1.2 Background

This SAS standard has been created and developed under the supervision of a GSMA working group comprised of representatives from MNOs and eUICC suppliers. The GSMA is responsible for updating the SAS standard and a review with eUICC suppliers and the appointed auditors will take place annually during the life of the scheme.

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, 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].

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.
- Assets to be protected.
- Risk and threats.
- Security requirements.

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

1.4 Intended Audience

- Security professionals and others within organisations offering SM-DP or SM-SR functionality.
- Responsible for SM-DP or SM-SR SAS implementation and compliance.
- SM-DP or SM-SR SAS Auditors
- MNOs.

1.5 Related Documents

The security objectives and requirements described in this document are supported by FS.09 GSMA SAS Methodology for Subscription Manager Roles [1] and FS.10 GSMA SAS Guidelines for Subscription Manager Roles [2] necessary for SM-DP, SM-SR and Auditors to apply and interpret this SAS standard.

1.6 Definitions

Term	Description
Actor	Person who is involved in, or can affect, the Sensitive Process.
Business Continuity	Capability of the entity performing the role of an SM-DP or SM-SR to continue delivery of SM-DP or SM-SR functionality at acceptable predefined levels following a failure incident. According to SM-DPs or SM-SRs customer requirements.
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.
Environment	Environment of use of the Sensitive Process limited to the security aspects
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
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 to be able to manage the eUICC.
High Security Area	Restricted areas off-limits to unauthorised personnel in which assets are stored and processed
Sensitive Process	The Sensitive Process represents the security evaluation field, covering the processes and the assets within those processes
SM-DP	An entity that provides SM-DP functionality to its customers.
SM-SR	An entity that provides SM-SR functionality to its customers.

1.7 Abbreviations

Term	Description
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
HSM	Hardware Security Module
ISI	Incoming Sensitive Information characterise the process sensitive inputs such as requests, files and keys.
IT	Information Technology
MNO	Mobile Network Operator
OSI	Outgoing Sensitive Information characterise the process sensitive outputs such as responses, files and keys.
SAS-SM	Security Accreditation Scheme for Subscription Management Roles
SGP.nn	Prefix identifier for official documents belonging to GSMA SIM Group
SM-DP	Subscription Manager – Data Preparation
SM-SR	Subscription Manager – Secure Routing
SP	Sensitive Process

1.8 References

Ref	Doc Number	Title
[1]	FS.08	GSMA SAS Methodology for Subscription Manager Roles
[2]	FS.09	GSMA SAS Guidelines for Subscription Manager Roles
[3]	RFC2119	“Key words for use in RFCs to Indicate Requirement Levels”, S. Bradner, March 1997. Available at http://www.ietf.org/rfc/rfc2119.txt
[4]	SGP.01	Embedded SIM Remote Provisioning Architecture
[5]	SGP.02	Remote Provisioning Architecture for Embedded UICC Technical Specification

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 [3].”

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 section 3.3.1 of SGP.01 [4]. Commences when the SM-SR takes responsibility for the eUICC, including the registration of an eUICC to a SM-SR. It also includes MNO request to create, personalise, download and install Profiles to the eUICC. These functions are provided by the SM-DP. Profile transport to eUICC and subsequent Platform Management of the Profiles, such as enabling, disabling, deletion, and master deletion is provided by the SM-SR.
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 standard is defined only for SM-DP or SM-SR 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

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 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.

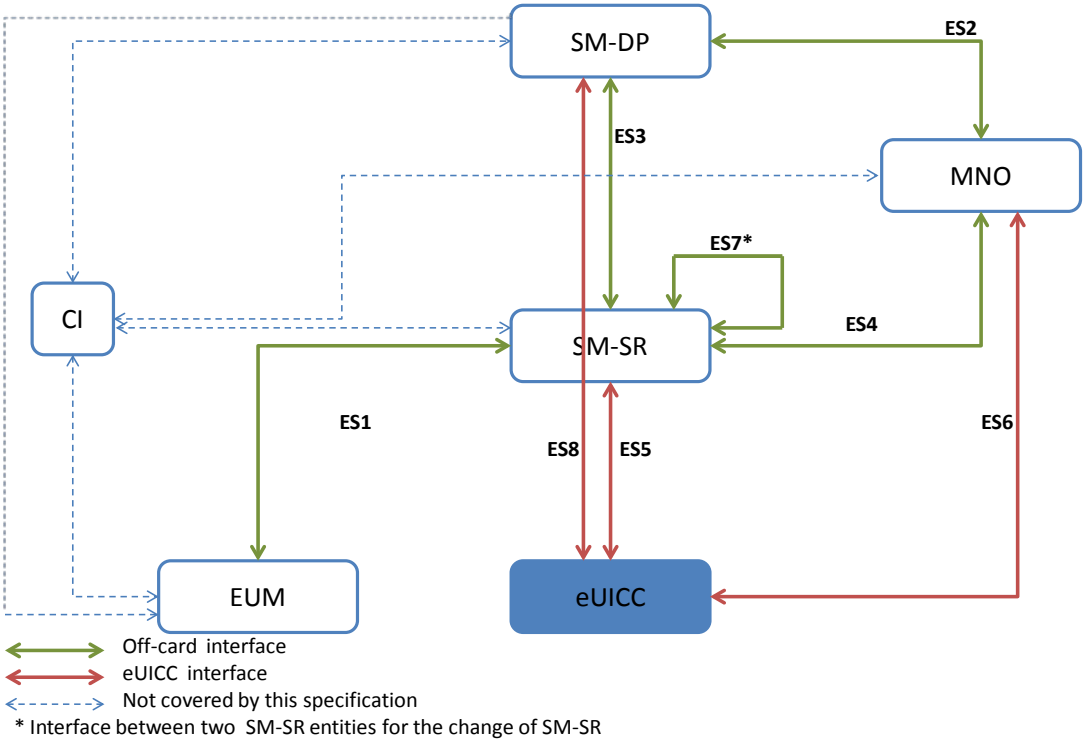

Figure 1: eUICC Remote Provisioning System

3.2 SM-SR Overview

SM-SR enables, disables and deletes Profiles on the eUICC in accordance with the MNO's policy rules. 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.

3.3 SM-SR Processes

SM-SR processes include customer requests in various forms. A high level view of SM-SR processes are indicated in Figure 2.

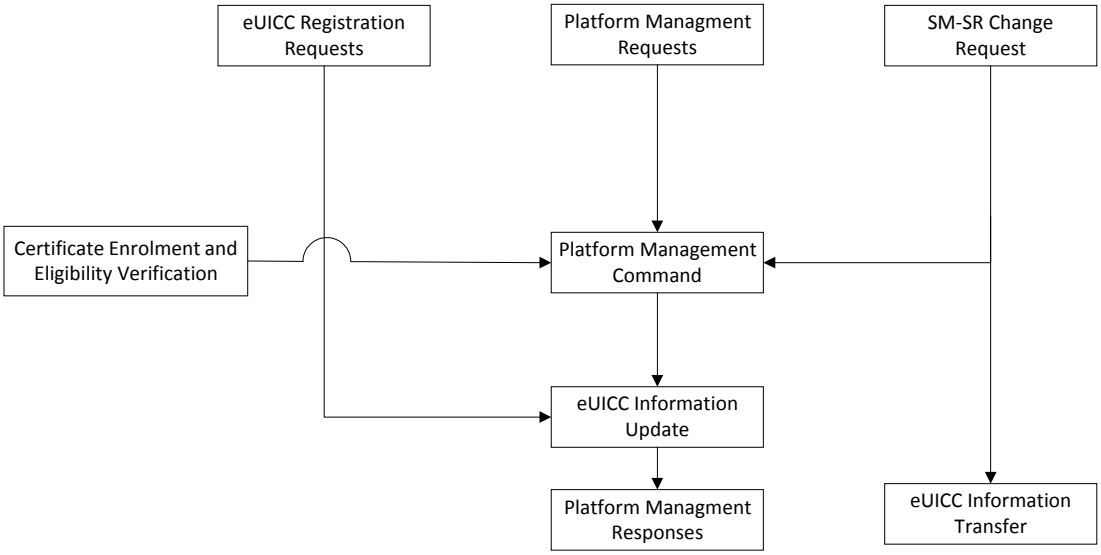

Figure 2: SM-SR Processes

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 2.

3.4 SM-DP Overview

SM-DP acts on behalf of the MNO.

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

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

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.

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.

3.5 SM-DP Processes

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

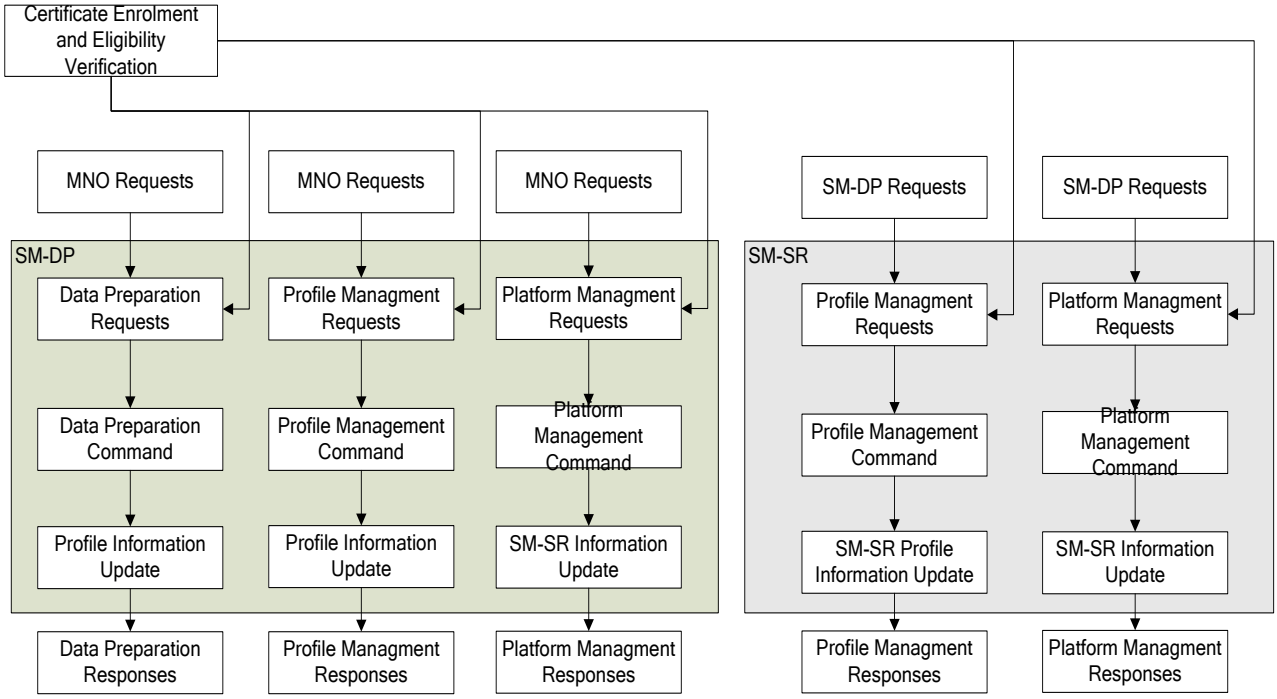

Figure 3: SM-DP Processes

SM-DP processes consist of Data Preparation and Profile and Platform Management. In addition, SM-DP manages the authentication and authorisation of remote entities, indicated as 'Certificate Enrolment and Eligibility Verification' in Figure 3.

Note: when the SM-SR and/or SM-DP are distributed across multiple sites/systems, the certification process must include those sites/systems into the scope (when those components are actively involved in the process of the SM-SR and/or SM-DP).

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 or SM-SR the processes, information assets and SM-DP or SM-SR 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 Section 9.9

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_PMCR)
eUICC Information (ISI_EIS)
Profile Metadata (ISI_PRM)
Remote Entities Authentication and Authorization Credentials (ISI_AACRE)
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)
Outgoing Sensitive Information (OSI)
Platform Management Commands (OSI_PMC)
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)

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 Asset Classification

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

4.5 Asset Characteristics

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

4.6 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**].

4.7 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_PMCR]** whose authenticity, integrity and availability must be protected.

4.8 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.

4.9 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_PMC**] 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.

4.10 Additional Sensitive Information (ASI)

Additional sensitive information (ASI) is:

- Customer information [**ASI_CUI**] from SM-DP or SM-SR 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 or SM-SR 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.

4.11 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 or SM-SR. 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 7.2 and 7.3 independently of the process step concerned.

In the threat description, data means all type of data assets described in Section 6.

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 INT_UNAU EXT_AUTH EXT_UNAU	OSI_PMR OSI_PrMC OSI_PMC	Accidental or deliberate cross-contamination of assets in the SM-DP or SM-SR.
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_PMR	Unauthorized ePlatform Management requests sent to remote entities for example, SM-SR.
T_FAKE_PrlMC	INT_AUTH INT_UNAU	OSI_PrMC OSI_PMC	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 and SM-SR functionality.

Table 6: 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 7: Indirect Threats Description

6 Security Objectives

6.1 Introduction

SM-DP or SM-SR is responsible to ensure that assets are protected 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 or SM-SR 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]
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 8: 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 or SM-SR functionality	T_SEF	To prevent theft, loss or misappropriation of assets

Table 9: 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 considered as minimum-security requirements for the Environment in which the SP is used.

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

It is recognised that it is possible to use mechanisms or tools other than those described in this section if they achieve the same security objective. For a worked example of how the SAS standard could be achieved refer to FS.10 [2].

NOTE: Numbering of the sections and requirements below restarts at (1) and applies independently of other sections in this document.

1 Policy, Strategy and Documentation

The security policy and strategy provides the business and its employees with a direction and framework to support and guide security decisions within the company.

1.1 Policy

1.1.1 A clear direction shall be set and supported by a documented security policy which defines the security objectives and the rules and procedures relating to the security of the SP, sensitive information and asset management.

1.1.2 Employees shall understand and have access to the policy and its application should be checked periodically.

1.2 Strategy

1.2.1 A coherent security strategy must be defined based on a clear understanding of the risks. The strategy shall use periodic risk assessment as the basis for defining, implementing and updating the site security system. The strategy shall be reviewed regularly to ensure that it reflects the changing security Environment through on-going re-assessment of risks.

1.3 Business Continuity Planning

1.3.1 Business Continuity measures must be in place in the event of disaster. The BCP will reflect the content of the customers' service level agreements.

2 Organisation and Responsibility

2.1 Organisation

2.1.1 To successfully manage security, a defined organisation structure shall be established with appropriate allocation of security responsibilities.

2.1.2 The management structure shall maintain and control security through a cross-functional team that co-ordinates identification, collation, and resolution, of security issues, independent of the business structure.

2.2 Responsibility

2.2.1 A security manager shall be appointed with overall responsibility for the issues relating to security in the SP.

2.2.2 Clear responsibility for all aspects of security, whether operational, supervisory or strategic, must be defined within the business as part of the overall security organization.

2.2.3 Asset protection procedures and responsibilities shall be documented throughout the SP.

2.3 Contracts and Liabilities

2.3.1 In terms of contractual liability, responsibility for loss shall be documented. Appropriate controls and insurance shall be in place.

3 Information

The management of sensitive information, including its storage, archiving, deletion and transmission can vary depending on the classification of the asset involved.

3.1 Classification

3.1.1 A clear structure for classification of information and other assets shall be in place with accompanying guidelines to ensure that assets are appropriately classified and treated throughout their lifecycle.

3.2 Data and Media Handling

3.2.1 Access to sensitive information and assets must always be governed by an overall ‘need to know’ principle.

3.2.2 Guidelines shall be in place governing the handling of data and other media, including a clear desk policy. Guidelines should describe the end-to-end ‘lifecycle management’ for sensitive assets, considering creation, classification, processing, storage, transmission and disposal.

4 Personnel Security

A number of security requirements shall pertain to all personnel working within the SP.

4.1 Security in Job Description

4.1.1 Security responsibilities shall be clearly defined in job descriptions.

4.2 Recruitment Screening

4.2.1 An applicant, and employee, screening policy shall be in place where local laws allow.

4.3 Acceptance of Security Rules

4.3.1 All recruits shall sign a confidentiality agreement.

4.3.2 Employees shall read the security policy and record their understanding of the contents and the conditions they impose.

4.3.3 Adequate training in relevant aspects of the security management system shall be provided on an on-going basis.

4.4 Contract Termination

4.4.1 Clear exit procedures shall be in place and observed with the departure of each employee.

5 Physical Security

A building is part of the site where SM-DP or SM-SR functionality is provided, SM-DP or SM-DP systems are deployed and where eUICC, MNO and Profile information are processed or stored. Buildings in which sensitive assets are processed shall be strongly constructed. Constructions and materials shall be robust and resistant to outside attack as manufacturers must ensure that assets are stored within High Security Areas and Restricted Areas by using recognised security control devices, staff access procedures and audit control logs.

5.1 Security Plan

Layers of physical security control shall be used to protect the SP according to a clearly defined and understood strategy. The strategy shall apply controls relevant to the assets and risks identified through risk assessment.

5.1.1 The strategy shall be encapsulated in a security plan that:

(i) defines a clear site perimeter / boundary,

(ii) defines one or more levels of secure area within the boundary of the site perimeter,

(iii) maps the creation, storage and processing of sensitive assets to the secure areas,

(iv) defines physical security protection standards for each level of secure area.

5.2 Physical Protection

5.2.1 The protection standards defined in the security plan shall be appropriately deployed throughout the site, to include:

(i) deterrent to attack or unauthorized entry,

(ii) physical protection of the building and secure areas capable of resisting attack for an appropriate period,

(iii) mechanisms for early detection of attempted attack against, or unauthorized entry into, the secure areas at vulnerable points,

(iv) control of access through normal entry / exit points into the building and SP to prevent unauthorized access,

(v) effective controls to manage security during times of emergency egress from the secure area and building,

(vi) mechanisms for identifying attempted, or successful, unauthorized access to, or within the site,

(vii) mechanisms for monitoring and providing auditability of, authorised and unauthorised activities within the SP.

5.3 Access Control

5.3.1 Clear entry procedures and policies shall exist which cater for the access rights given to employees, visitors and deliveries to enter the SP. These considerations should include the use of identity cards, procedures governing the movement of visitors within the SP, delivery/dispatch checking procedures and record maintenance.

5.3.2 Access to each secure area shall be controlled on a 'need to be there' basis. Appropriate procedures shall be in place to control, authorise, and monitor access to each secure area and within secure areas. Regular audits shall be undertaken to monitor access control to the secure area.

5.4 Security Staff

5.4.1 Security staff are commonly employed or sub-contracted by suppliers. Duties for security staff shall be clearly documented and the necessary tools and training shall be supplied.

6 SM-DP and SM-SR Data Management

SM-DPs or SM-SRs will be responsible for lifecycle management of data used for remote provisioning, management of eUICCs and management of Profiles. Information and IT security controls must be appropriately applied to all aspects of lifecycle management to ensure that data is adequately protected. The overall principle shall be that all data is appropriately protected from the point of receipt through storage, internal transfer, processing and through to secure deletion of the data.

6.1 Data Transfer

6.1.1 SM-DPs or SM-SRs shall take responsibility to ensure that electronic data transfer to other entities in the Embedded UICC eco-system is appropriately secured.

6.2 Access to Sensitive Data

6.2.1 SM-DPs or SM-SRs shall prevent direct access to sensitive SM-DP or SM-DR data. User access to sensitive data shall be possible only where absolutely necessary. All access must be auditable to identify the date, time, activity and person responsible, where audit data must be protected in terms of integrity.

6.3 Cryptographic Keys

6.3.1 Cryptographic keys used for data protection shall be generated, exchanged and stored securely.

6.3.2 The cryptographic computation (derivations, random generations) and storage of keys involved in the protection of the sensitive data shall rely on HSMs that are FIPS 140-2 level 3 certified.

6.3.3 The cryptographic key management process shall be documented and cover the full lifecycle of the keys.

6.4 Public Key Certificates

6.4.1 Public Key Certificates shall be generated, exchanged and stored securely.

6.4.2 The SM (SM-SR and SM-DP) certificate shall be signed by a CI (Certificate Issuer) authorised by and acting on behalf of the GSMA.

6.4.3 The key lengths defined in the SGP.02 [5] shall be used.

6.5 Data Integrity

6.5.1 Controls shall be in place to ensure that the same, authorized, data from the correct source is used for the SM-DP or SM-SR processes and supplied to the SM-DPs or SM-SRs customer.

7 SM-DP and SM-SR Service Management

7.1 Personnel

7.1.1 Clear security rules shall govern the manner in which employees engaged in such activities shall operate within the SP. Relevant guidelines should be in place and communicated to all relevant staff.

7.2 SM-DP and SM-SR Service

7.2.1 Systems used for the remote provisioning, management of eUICCs and management of Profiles shall be compliant in terms of security with SGP.01 [4] and SGP.02 [5].

7.2.2 SM-DPs or SM-SRs must prevent cross-contamination of assets between different MNO customers.

7.3 Remote Entity Authentication

7.3.1 All authorized entities in the SM-DP or SM-SR processes shall be authenticated by appropriate authentication protocols for example, SM-SR, SM-DP, MNO.

8 IT System and Network Management

The secure operation of IT system and network facilities is paramount to the security of data and services. In particular, the processing, storage and transfer of information, which if compromised, could have serious consequences for the MNO, must be considered.

Operation of IT systems and networks must ensure that comprehensive mechanisms are in place to preserve the confidentiality, integrity and availability of data and services. The software implemented on the SM-DP or SM-SR IT system must implement the Profile and Platform Management protocols in terms of security as specified in SGP.01 [4] and SGP.02 [5].

8.1 Policy

8.1.1 A documented IT security policy shall exist which shall be well understood by employees.

8.2 Segregation of Roles and Responsibilities

8.2.1 Responsibilities and procedures for the management and operation of IT systems and networks shall be established. Security related duties shall be segregated from operational activities to minimise risk.

8.3 Access Control

8.3.1 Physical access to sensitive IT system facilities shall be controlled.

8.3.2 An access control policy (including remote access) shall be in place and procedures shall govern the granting of access rights with a limit placed on the use of special privilege users. Logical access to IT services shall be via a secure logon procedure.

8.3.3 Passwords shall be managed effectively and strong authentication shall be deployed where remote access is granted.

8.3.4 Remote access shall only be permitted from an authorised site.

8.4 Network Security

8.4.1 Systems and data networks used for the processing and storage of sensitive data should be housed in an appropriate Environment and logically or physically separated from other networks. Data transfer between secure and insecure networks must be strictly controlled according to a documented policy defined on a principle of minimum access.

8.4.2 The system shall implement a 3 tier dedicated security architecture.

8.4.3 The system shall be implemented using appropriately configured and managed firewalls incorporating appropriate intrusion detection systems.

8.5 IT Security

8.5.1 Data Management

(i) Multi-tenant SM-DP or SM-SR solutions on the same physical hardware shall ensure customer data is logically segregated between different customers.

(ii) Database administration must be strictly controlled and managed. Each access to databases shall be authenticated, authorized and irreversibly logged.

(iii) Data shall be stored encrypted in the database according to the assets classification.

(iv) Exchange of sensitive data within the SM-DP or SM-SR IT system shall be end-to-end encrypted.

(v) A data retention policy shall be defined.

8.5.2 System configuration and maintenance

(i) Security requirements of systems shall be identified at the outset of their procurement and these factors shall be taken into account when sourcing them.

(ii) All system components and software shall be protected from known vulnerabilities by having the latest vendor-supplied security patches installed.

(iii) System components configuration shall be hardened in accordance with industry best practice.

(iv) Change control processes and procedures for all changes to system components shall be in place.

(v) Processes and procedures to identify newly discovered security vulnerabilities and to test all system components for security vulnerabilities shall be in place.

(vi) Comprehensive virus detection and prevention measures shall be deployed across all systems vulnerable to viruses and other malicious software.

(vii) Unattended terminals shall timeout to prevent unauthorised use and appropriate time limits shall be in place.

(viii) Decertification/decommissioning of assets (such as IT Systems) used as part of the SP shall be documented and performed in a secure manner.

8.5.3 System back-up

(i) Back-up copies of critical business data shall be taken regularly. Back-ups shall be stored appropriately to ensure confidentiality and availability.

8.6 Software Development

8.6.1 The software development processes for the SM-DP or SM-SR shall follow industry best practices for development of secure systems.

8.7 External Facilities Management

8.7.1 If any sub-contracted external facilities or management services are used appropriate security controls shall be in place. Such facilities and services shall be subject to the requirements stated in this document.

9 Control, Audit and Monitoring

9.1 General Principles

9.1.1 Controls deployed shall be clearly documented and up-to-date.

9.1.2 Controls shall be subject to a rigorous programme of internal monitoring, audit and maintenance to ensure their continued correct operation.

9.1.3 The controls apply to the different sections 5, 6 and 8.

9.2 Audit Trails

9.2.1 The SP shall be logged in an audit trail that provides a complete record of, and individual accountability for:

(i) Profile Management, Platform Management, IT system and eUICC Management procedures

(ii) Access to sensitive data

9.2.2 The audit trail shall:

(i) ensure that all assets created, processed and deleted are completely accounted for,

(ii) ensure that the responsible individuals are traceable and can be held accountable.

9.2.3 The audit trail shall be protected in terms of integrity and the retention period must be defined. The audit trail shall not contain sensitive data.

10 Incident Response and Reporting

10.1 An escalation process shall be in place where a security breach is revealed on SM-DP and SM-SR process.

10.2 Reporting procedures shall be in place.

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**
OSI_PRM	Profile Metadata	**1**
ISI_EIS_CLASS1	Incoming eUICC information.	**1**
OSI_EIS_CLASS1	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_CLASS2	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**
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 10: SM-SP 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_PMCR	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_PMC	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 11: SM-SR Assets Classification

A.4 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**
	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 12: EIS Asset Details and Classification

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

Annex B Personalisation Flow

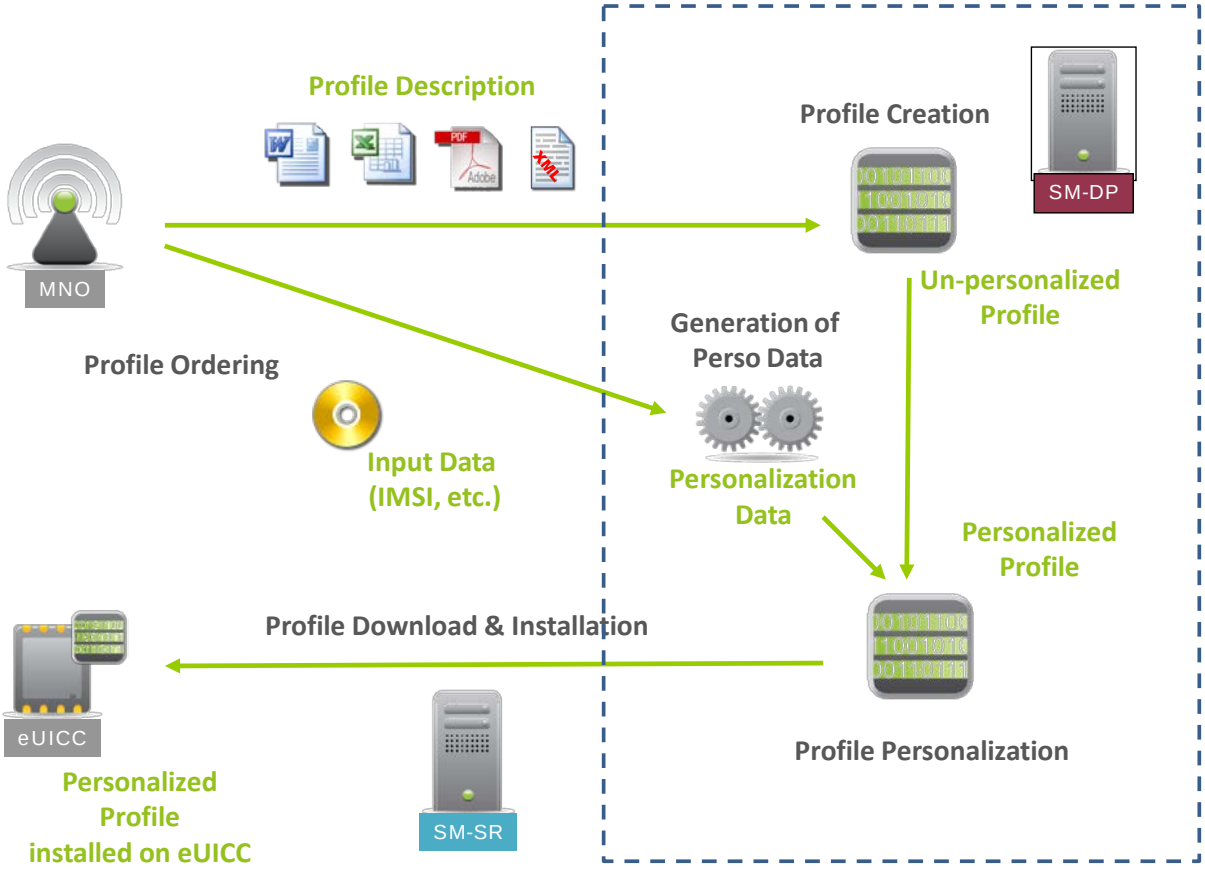

Figure 4: Personalisation Flow

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

C.2 Other Information

Type	Description
Document Owner	Fraud and Security Group
Editor / Company	Arnaud Danree, Oberthur

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.1