SGP.41 eSIM IFPP Architecture and Requirements

Version 1.0

28 February 2025

Security Classification: Non-Confidential

Copyright Notice

Disclaimer

Compliance Notice

The information contain herein is in full compliance with the GSMA Antitrust Compliance Policy.

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

Table of Contents

1 Introduction 4
1.1 Overview 4
1.2 Scope 4
1.3 Intended Audience 4
1.4 Definition of Terms 5
1.5 Abbreviations 5
1.6 References 6
1.7 Conventions 6
2 Roles 7
2.1 Mobile Service Provider, Operator 7
2.2 eUICC Manufacturer, Device Manufacturer 7
3 Architecture 7
3.1 Architecture Diagram 7
3.2 Architecture Elements 7
3.2.1 SM-DPf 7
3.2.2 Device Manufacturer 8
3.2.3 FPA 9
3.3 eUICC Architecture 9
3.3.1 eUICC Architecture Overview 9
3.4 Interfaces 10
3.4.1 Operator – SM-DPf (ES2f) 10
3.4.2 SM-DPf – Device Manufacturer (Esbpp) 10
3.4.3 Device Manufacturer – FPA (Esfac) 11
3.4.4 FPA – FPA Services (ES10f) 11
3.4.5 SM-DPf – eUICC (ES8f) 11
3.4.6 eSIM CA – EUM / SM-DPf (Esci) 11
3.4.7 EUM – eUICC (Eseum) 11
3.4.8 EUM – SM-DPf (Esed1) 11
3.4.9 EUM – Device Manufacturer (Esed2) 12
4 Requirements 12
4.1 Functional Requirements 12
4.1.1 General Functional Requirements 12
4.1.2 eUICC Functional Requirements 12
4.1.3 SM-DPf Functional Requirements 13
4.1.4 Device Manufacturer Functional Requirements 13
4.2 Security Requirements 13
4.2.1 General Security Requirements 13
4.2.2 SM-DPf Security Requirements 14
4.2.3 EUM Security Requirements 14
5 Procedures 14
5.1 In-Factory Profile Provisioning Procedure using BPPs for Consumer and IoT 14

5.2 In-Factory Profile Provisioning Procedure for M2M 17
Annex A Use Cases (Informative) 18
A.1 Consumer Devices Use Case 18
A.2 IoT Devices Use Case 18
A.3 On-demand Profile loading during the Device Production Process - Use Case 18
A.4 Device Inventory Management Use Case 19
Annex B Threats and Risks (Informative) 19
B.1 Malicious or compromised IFPP entity 19
B.2 Cryptographic Related Risks 19
B.3 Quality of Service 19
B.4 Non-human or Unpredictable 20
Annex C In-factory provisioning flow (Informative) 20
Annex D Document Management 22
D.1 Document History 22
D.2 Other Information 26

1 Introduction

1.1 Overview

This document specifies an architecture and requirements for the in-factory provisioning of Bound Profile Packages.

1.2 Scope

This document defines a common framework to enable the provisioning of Bound Profile Packages on eUICCs in a Device factory environment. This framework aims to provide the basis for global interoperability among actors in in-factory provisioning scenarios.

The scope of this document focuses on:

- The re-use of the architectures defined in SGP.01, SGP.21 and SGP.31 as much as possible, minimising the impact on the existing components and interfaces.
- The re-use of the proven security solutions established in SGP.01, SGP.21 and SGP.31.

NOTE: Architecture and requirements for IFPP for M2M (SGP.01) are FFS.

This document applies equally to Discrete eUICCs and Integrated eUICCs. For both, the start condition is that the eUICC operating system, configured for IFPP, is already loaded. The loading of the operating system and of the eUICC individual data (e.g. EID, eUICC Certificate and related private key,…) into the ECASD of an eUICC using the Two-Step Personalisation Process as per GSMA FS.18 [8] happens in a step preceding the loading and installation of the first Profile Package. This step is out of scope of this specification.

In the scope of this document the Device contains at least an eUICC, but it might not be a final product to be used by the customer.

1.3 Intended Audience

Technical experts within Operators, eUICC solution providers, Subscription Management providers, Device vendors, standards organisations, solution providers, Mobile Service Providers and other impacted industry bodies.

1.4 Definition of Terms

Term	Description
Bound Profile Package	As defined in SGP.21 [1].
Consumer Device	Device as defined in SGP.21 [1].
Device	Either a Consumer Device or an IoT Device, or partial realization of these.
Device Manufacturer	As defined in SGP.21 [1].
Device Production Process	Production or modification of (parts of) the Device that takes place in the premises of the Device Manufacturer or its designated 3rd party production site.
Discrete eUICC	As defined in SGP.21 [1].
End User	As defined in SGP.21 [1].
eUICC	As defined in SGP.21 [1].
eUICC Manufacturer	As defined in SGP.21 [1].
Event	As defined in SGP.21 [1].
Event Record	As defined in SGP.21 [1].
Factory Profile Assistant	Hardware and/or software on the Device that interfaces between the Device Manufacturer and the eUICC
Integrated eUICC	As defined in SGP.21 [1].
IoT	As defined in SGP.31 [2].
IoT Device	As defined in SGP.31 [2].
Mobile Service Provider	As defined in SGP.21 [1].
One-time Key	A key that is only used once.
Operator	As defined in SGP.21 [1].
Profile	As defined in SGP.21 [1].
Profile Description	As defined in SGP.21 [1]
Profile Installation Result	As defined in SGP.22 [7].
Profile Loading Report	Set of information related to successful or unsuccessful Profile loading and installation into one or more eUICCs.
Profile Owner	As defined in SGP.21 [1].
Profile Package	As defined in SGP.21 [1].
Protected Profile Package	As defined in SGP.21 [1].
Subscription Manager Data Preparation + (SM-DP+)	As defined in SGP.21 [1].
Subscription Manager Data Preparation factory (SM-DPf)	The RSP architecture element that prepares Profiles for provisioning into an eUICC at the Device Manufacturer.

1.5 Abbreviations

Term	Description
BPP	Bound Profile Package

Term	Description
ECASD	eUICC Controlling Authority Security Domain
EID	eUICC Identifier
EUM	eUICC Manufacturer
FPA	Factory Profile Assistant
HSM	Hardware Security Module
IFPP	In-Factory Profile Provisioning
IPA	IoT Profile Assistant
ISD-P	Issuer Security Domain – Profile
LPA	Local Profile Assistant
RSP	Remote SIM Provisioning
SM-DP+	Subscription Manager Data Preparation +
SM-DPf	Subscription Manager Data Preparation factory

1.6 References

Ref	Doc Number	Title
[1]	SGP.21 V2.2 or higher	RSP Architecture
[2]	SGP.31 V1.1 or higher	eSIM IoT Architecture and Requirements
[3]	SGP.01 V4.2	Embedded SIM Remote Provisioning Architecture
[4]	RFC 2119	“Key words for use in RFCs to Indicate Requirement Levels”, S. Bradner https://www.ietf.org/rfc/rfc2119.txt
[5]	RFC 8174	Ambiguity of Uppercase vs Lowercase in RFC 2119 Key Words https://www.rfc-editor.org/rfc/rfc8174.txt
[6]	TCA eUICC Profile Package v3.1 or higher	eUICC Profile Package: Interoperable Format Technical Specification
[7]	SGP.22 V2.2 or higher	RSP Technical Specification
[8]	GSMA FS.18	Security Accreditation Scheme - Consolidated Security Requirements and Guidelines

1.7 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 RFC 2119 [4] and clarified by RFC 8174 [5]**Error! Reference source not found.**, when, and only when, they appear in all capitals, as shown here.

2 Roles

2.1 Mobile Service Provider, Operator

The roles Mobile Service Provider and Operator are used as defined in SGP.21 [1].

2.2 eUICC Manufacturer, Device Manufacturer

The roles eUICC Manufacturer and Device Manufacturer are used as defined in SGP.21 [1].

3 Architecture

This section contains the functional description of the system architecture for IFPP.

3.1 Architecture Diagram

The following architecture diagrams describe the roles and interfaces (Figure 1).

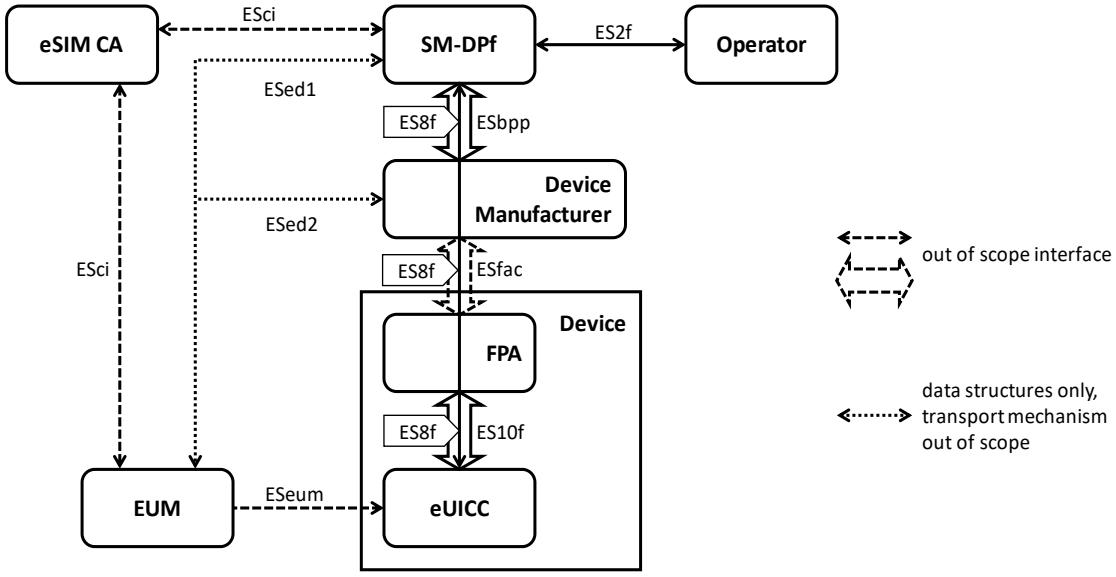

Figure 1: IFPP Functional Architecture for Consumer and IoT Devices

FFS

Figure 2: IFPP Functional Architecture for M2M Devices

3.2 Architecture Elements

3.2.1 SM-DPf

The SM-DPf is responsible for the generation, protection and delivery of Profiles for IFPP.

The following diagram shows the functions of an SM-DPf that are enabled to provide Profiles for IFPP:

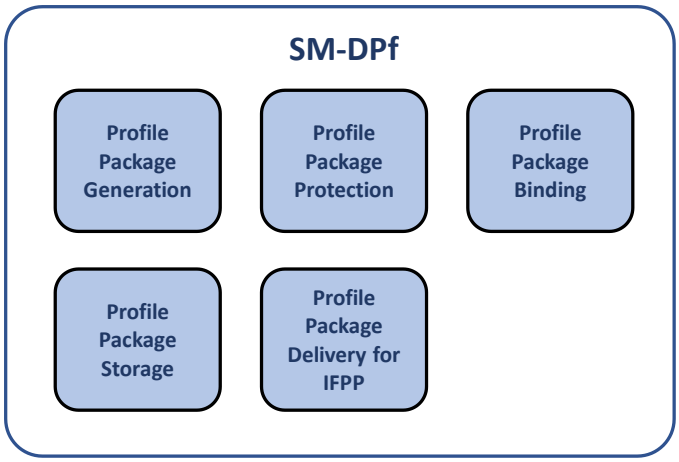

Figure 3: SM-DPf Functions

Function name	Description
Profile Package Generation	Creates Profile Packages (i.e. Profiles including IMSI, K, ICCID,…) from Profile Descriptions agreed with Operators. This can be an off-line batch or synchronous process.
Profile Package Protection	Secures each Profile Package according to the security process creating the Protected Profile Package.
Profile Package Binding	Binds the Protected Profile Package to a target eUICC using the security process thus creating the Bound Profile Package.
Profile Package Storage	Temporarily stores Protected Profile Packages or Bound Profile Packages for subsequent delivery.
Profile Package Delivery for IFPP	Transmits the Bound Profile Package to the Device Manufacturer for installation onto the eUICC.

3.2.2 Device Manufacturer

The Device Manufacturer receives protected Profiles from one or several SM-DPf and provisions them into the eUICC during production, via the FPA.

In the context of this document, the Profile provisioning is a step in the Device production/configuration and happens in the premises of the Device Manufacturer (or its contracting parties), before the Devices reach the Consumer/End User.

The interfaces of the Device Manufacturer fall into different categories:

- Esed2 and Esbpp require communication with external entities, whereas
- everything around Esfac, which is directly related to the handling of the Devices during the Device Production Process, may require a setup that is disconnected from the outside world.

While the Device Manufacturer is shown in the architecture as one box, its internal structure required to handle these interfaces is out of scope of this document.

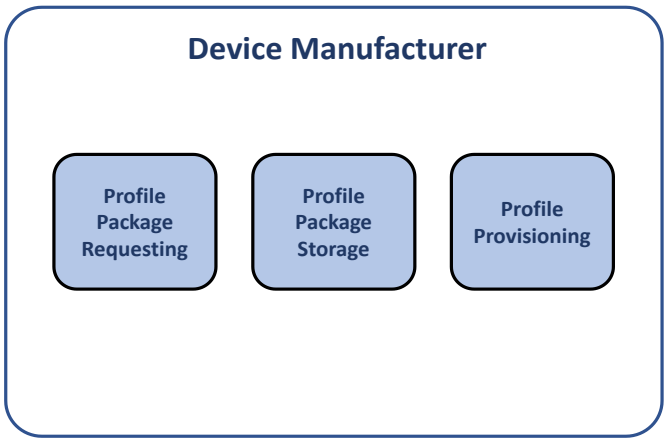

Figure 4: Device Manufacturer Functions

Function name	Description
Profile Package Requesting	Requests Bound Profile Packages from the SM-DPf and sends Profile Loading Reports to the SM-DPf
Profile Package Storage	Temporarily stores Bound Profile Packages for subsequent delivery to the eUICC
Profile Provisioning	Transmits the Bound Profile Package to the FPA for installation onto the eUICC during the Device Production Process.

3.2.3 FPA

The FPA sends the BPP and related data to the eUICC and returns the response(s) following the protocols defined for IFPP.

As the interface between the Device Manufacturer and the FPA is out of scope, the functional split between both entities is irrelevant and does not affect this specification.

The FPA can e.g. be implemented as hardware solution, as low-level driver or as LPA or IPA running in a factory mode.

3.3 eUICC Architecture

3.3.1 eUICC Architecture Overview

3.3.1.1 High-level architecture of the eUICC

The eUICC architecture is similar to the one of SGP.21 [1]. Only the interfaces required for IFPP are shown.

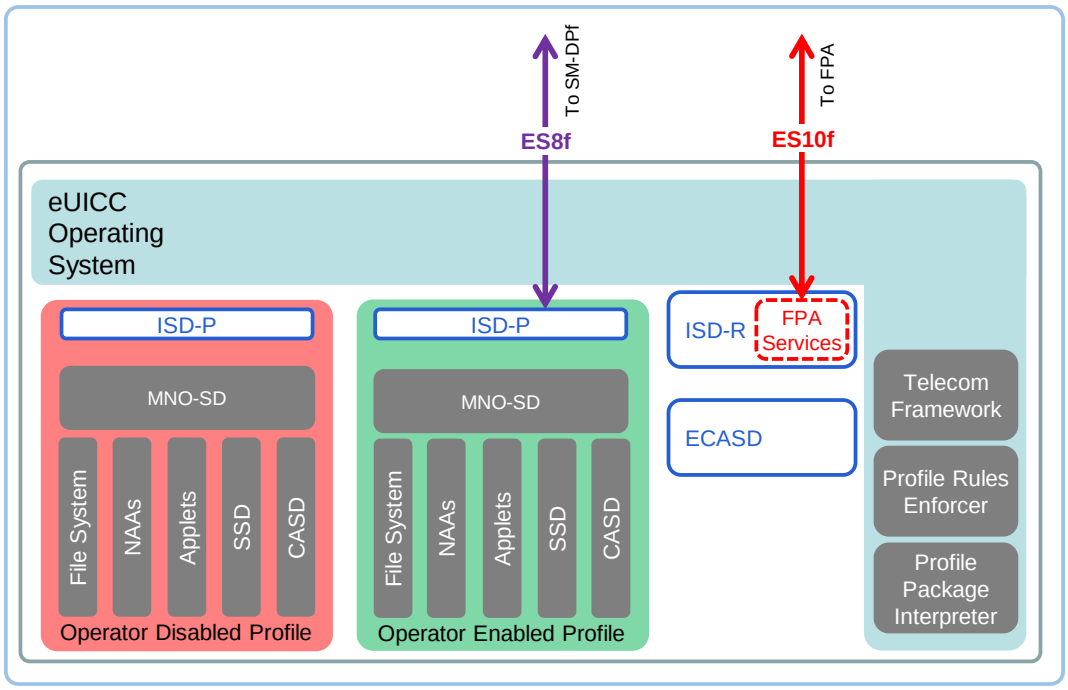

Figure 5: Schematic Representation of the eUICC

3.3.1.2 FPA Services

The FPA Services provide access to the services and data required by the FPA functions (ES10f) for the transfer of the Bound Profile Package.

3.4 Interfaces

This section defines the interfaces used in this specification. Interfaces as defined in SGP.21 [1] will be referenced as appropriate.

3.4.1 Operator – SM-DPf (ES2f)

This interface is between the Operator and the SM-DPf e.g., for the ordering of Profiles Packages to be provisioned on eUICCs according to the IFPP mechanisms and for the subsequent notifications related to the result of these provisionings. As such, the ES2f interface is similar in purpose to the ES2+ interface defined in SGP.21 [1]. Thus, it is expected that the processes that the Operator might have put in place for the ES2+ interface can be reused for the processes related to the ES2f interface.

3.4.2 SM-DPf – Device Manufacturer (Esbpp)

This interface is used by the SM-DPf to send BPPs and related data to the Device Manufacturer. It may also be used by the Device Manufacturer to send eUICC data to the SM-DPf when requesting Profiles, and to forward the Profile Loading Report to the SM-DPf.

Req no.	Description
ESBPP01	The data structure for providing one or more Profile Packages to the Device Manufacturer SHALL be specified.
ESBPP02	The data structure for providing eUICC data of one or more eUICCs to the SM-DPf when requesting Profile Packages SHALL be specified.

Req no.	Description
ESBPP03	The data structure for providing the Profile Loading Report to the SM-DPf SHALL be specified. It SHALL be able to contain: • one or more Profile Installation Results generated by the eUICCs, • Reports for Profile(s) that have not generated Profile Installation Results (e.g. due to an eUICC not accessible or physically damaged, or the FPA returning BPP execution errors).
ESBPP04	At least one optional transport mechanism for the data structures according to ESBPP01, ESBPP02 and ESBPP03 SHALL be specified.

3.4.3 Device Manufacturer – FPA (Esfac)

This interface is used by the Device Manufacturer to send BPPs and related data to the FPA, and to retrieve the Profile Installation Results.

This interface is out of scope of this document and depends on how the FPA is implemented.

3.4.4 FPA – FPA Services (ES10f)

This interface is used by the FPA to forward Profiles and related data to the eUICC, and to retrieve the Profile Installation Results. It may re-use functions already defined for ES10 in SGP.21 [1]. This interface also encapsulates ES8f messages.

3.4.5 SM-DPf – eUICC (ES8f)

This interface provides a secure end-to-end channel between the SM-DPf and the eUICC for the administration of the ISD-P and the associated Profile during download and installation. It may re-use functions already defined for ES8+ in SGP.21 [1].

3.4.6 eSIM CA – EUM / SM-DPf (Esci)

This interface is used to provide certificates to the EUM and the SM-DPf. It is also used by the SM-DPf to retrieve the certificate revocation status.

This interface is out of scope of this document.

3.4.7 EUM – eUICC (Eseum)

Eseum is the interface between the EUM and the eUICC. Compared to SGP.21 [1], it is also used to provision additional key material into the eUICC during eUICC manufacturing.

This interface is out of scope of this specification.

3.4.8 EUM – SM-DPf (Esed1)

This interface is used to provide eUICC data to the SM-DPf.

eUICC data required for IFPP may include:

- the eUICC certificate
- pre-loaded One-time public Key(s)
- Static eUICC data, such as eUICC capabilities, for use during eligibility checks

Req no.	Description
ESED101	The data structure for providing eUICC data of one or more eUICCs SHALL be specified. The transport mechanism for this data structure is out of scope.
ESED102	Static eUICC data, such as eUICC capabilities MAY be present within the data structure.

3.4.9 EUM – Device Manufacturer (Esed2)

This interface is used to provide eUICC data required for IFPP as described in 3.4.8 to the Device Manufacturer. It is an alternative way, which may be used instead of Esed1.

Req no.	Description
ESED201	The data structure for providing eUICC data of one or more eUICCs SHALL be specified. The transport mechanism for this data structure is out of scope.
ESED202	Static eUICC data, such as eUICC capabilities MAY be present within the data structure.

4 Requirements

This specification is based on the SGP.21 [1], SGP.31 [2] and SGP.01 [3] architectures. It will refer to these specifications where appropriate. This implies that to cover the whole range of requirements for IFPP, SGP.41 MUST be used together with SGP.21 [1], SGP.31 [2] and SGP.01 [3].

4.1 Functional Requirements

4.1.1 General Functional Requirements

Req no.	Description
GENF01	There SHALL be a means for the Device Manufacturer to provision one or more Profiles from the same or from different SM-DPfs on the same eUICC.
GENF02	Loading and installation of Profiles SHALL NOT require any End User interaction (e.g., User Intent, Confirmation Request, or Confirmation Code entry) as defined in SGP.21 [1].
GENF03	A Profile SHALL only be set in Enable state using either the LPA (as defined in SGP.21 [1]), the IPA (as defined in SGP.31 [2]), or the means defined in EUICCF05.

4.1.2 eUICC Functional Requirements

Req no.	Description
EUICCF01	The eUICC SHALL be able to store one or multiple pre-provisioned keys as per GENS07/GENS08.
EUICCF02	The eUICC SHALL provide a secure mechanism for the Device Manufacturer to authorise the use of the FPA Services.
EUICCF03	The eUICC SHALL provide a mechanism to the Device Manufacturer to delete all the One-time Keys used for Profile binding as per GENS07/GENS08.
EUICCF04	The eUICC SHALL only authorise the use of the LPA Services (as defined in SGP.21 [1]) or the IPA Services (as defined in SGP.31 [2]) if there is no One-time Key as per GENS07/GENS08.

EUICCF05	The eUICC MAY provide a means to the Device Manufacturer to test the connectivity of a Profile during the Device Production Process.

4.1.3 SM-DPf Functional Requirements

Req no.	Description
DPFF01	Profile Package generation SHALL only be performed by the SM-DPf.
DPFF02	Profile Package protection SHALL only be performed by the SM-DPf.
DPFF03	Storage of Protected Profile Packages SHALL only be performed by the SM-DPf.
DPFF04	Profile Package binding SHALL only be performed by the SM-DPf.
DPFF05	The SM-DPf SHALL be able to receive a Profile Loading Report from the Device Manufacturer.
DPFF06	The SM-DPf SHALL verify integrity and authenticity of data signed by the eUICC (e.g. Profile Installation Results) in a Profile Loading Report, if any.
DPFF07	After successful verification, as per DPFF06, and if requested by the Mobile Service Provider, the SM-DPf SHALL provide to the Mobile Service Provider the results of the profile loading and installation of profiles into eUICCs.
DPFF08	The SM-DPf SHALL be able to support a function that enables the Device Manufacturer to request Profile Packages for a list of eUICCs over the Esbpp interface.
DPFF09	The SM-DPf SHALL be able to perform an eUICC eligibility check as instructed by the Profile Owner.
DPFF10	The SM-DPf SHALL verify the integrity and the authenticity of the eUICC data prior to the binding of a Profile.

4.1.4 Device Manufacturer Functional Requirements

Req no.	Description
DMF01	The provisioning procedure SHALL allow the step of loading and installation of the BPPs onto the eUICCs to happen offline, i.e., in an environment of the Device Manufacturer that has no internet connectivity.
DMF02	The Device Manufacturer SHALL be able to retrieve Profile Installation Results generated by the eUICCs.
DMF03	The Device Manufacturer SHOULD delete all the remaining One-Time Keys within the eUICC, as per GENS07/GENS08, before the end of the Device Production Process.
DMF04	With regards to DMF03, the Device Manufacturer MAY use the mechanism in EUICCF03 to delete all the remaining One-Time Keys within the eUICC.

4.2 Security Requirements

4.2.1 General Security Requirements

Req no.	Description
GENS01	There SHALL be an option where Profile provisioning related security accreditation (e.g., GSMA SAS) is not required for the Device Manufacturer.
GENS02	There SHALL be an option where an HSM at the Device Manufacturer is not required.
GENS03	Profile Package confidentiality and integrity SHALL be preserved at any point in time.

Req no.	Description
GENS04	There SHALL be a means that ensures that a Profile Package is loaded to only one eUICC (avoid cloning).
GENS05	The private key of the SM-DPf used for Profile Binding with an eUICC and cryptographic operations performed with this key SHALL be protected and stored in an HSM that is certified as required by GSMA SAS.
GENS06	Each Profile binding SHALL incorporate Perfect Forward Secrecy (PFS).
GENS07	One-time Keys used for Profile binding SHALL be randomly generated.
GENS08	Each One-time Key SHALL be used to load only one Profile.
GENS09	At the Device Manufacturer, the clear-text Profile Package SHALL only exist inside the eUICC.
GENS10	The Device Manufacturer SHALL never have access to the clear-text private/secret keys used for binding of Profile Packages.
GENS11	The process for the generation of Bound Profile Packages SHALL be covered by GSMA SAS.
GENS12	There SHALL be a mechanism to ensure that a One-time Key used for Profile binding belongs to an eUICC.
GENS13	The FPA Services SHALL only be available during the Device Production Process. NOTE: How this requirement is fulfilled is Device Manufacturer and/or EUM specific.
GENS14	With regards to GENS07, One-time Keys SHALL only be generated and loaded in a SAS-UP environment.

4.2.2 SM-DPf Security Requirements

Req no.	Description
DPFS01	The SM-DPf SHALL be accredited according to GSMA SAS.

4.2.3 EUM Security Requirements

Req no.	Description
EUMS01	The EUM SHALL be accredited according to GSMA SAS.

5 Procedures

This section contains the high-level description of the procedures.

5.1 In-Factory Profile Provisioning Procedure using BPPs for Consumer and IoT

This procedure describes the preparatory steps, the Profile delivery, the Profile loading during the Device Production Process and the final reporting for IFPP.

The procedure is shown for one Profile per eUICC from one SM-DPf only. However, the procedure may be repeated for an eUICC to load several Profiles from one or several SM-DPfs.

```
@startuml
skinparam monochrome true
skinparam ArrowColor Black

hide footbox
```

```
participant "EUM" as EUM #FFFFFF
participant "MSP" as MSP #FFFFFF
participant "SM-DPf" as DP #FFFFFF
participant "Device\nManufacturer" as DM #FFFFFF
participant "FPA" as FPA #FFFFFF
participant "eUICC" as eUICC #FFFFFF

group Profiles preparation
MSP -> DP: [1] prepare Profiles request
end group

group eUICCs delivery
EUM -> DM: [2] eUICCs
alt  EUM provides eUICC data to SM-DPf
EUM -> DP: [3] eUICC data (e.g., keys)
else EUM provides eUICC data to Device Manufacturer
EUM -> DM: [4] eUICC data (e.g., keys)
end
end group


group Profile delivery
DM -> DP: [5] request for BPPs\n [with eUICC data]
rnote over DP: [6] create BPPs
DP -> DM: [7] send BPPs
end group

group Profile loading
DM -> FPA: [8] BPP
FPA -> eUICC: [9] BPP
rnote over eUICC: [10] Profile installation
eUICC -> FPA: [11] Profile Installation Result
FPA -> DM: [12] Profile Installation Result
end group

Opt If Profile Installation Result option is chosen
rnote over DM: [13] Generate Profile Loading Report
DM -> DP: [14] Profile Loading Report
rnote over DP: [15] Verify Profile Installation Results
DP -> MSP: [16] [Report]
end

@enduml
```

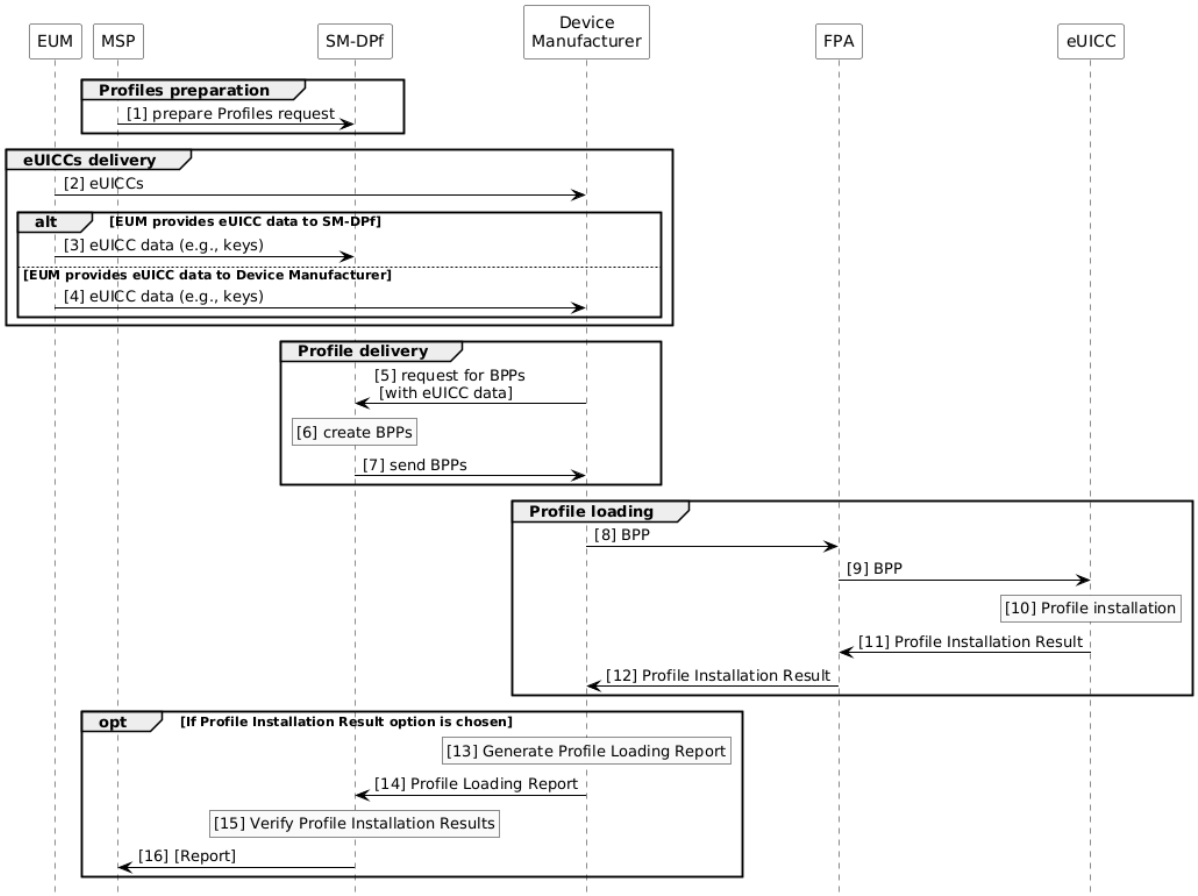

Figure 6: IFPP Procedure

Start Conditions:

The fully personalised eUICC (having an EID, eUICC keys and certificates, etc.) is prepared for Profile loading during the Device Production Process (e.g., with relevant key material) by the EUM.

The Device Manufacturer has ordered eUICCs from the EUM. Optionally, the Device Manufacturer may have indicated to the EUM an SM-DPf as recipient for the eUICC data. The Device Manufacturer has ordered Profiles from the Mobile Service Provider.

Procedure:

Steps 1 to 7 are required to prepare for loading of Profiles during the Device Production Process. As long as the preconditions for each step are fulfilled, they can be performed in a different order other than specified below, e.g., step 2 can happen after step 7.

1. The Mobile Service Provider requests the SM-DPf to prepare Profiles.
2. The EUM provides IFPP-capable eUICCs to the Device Manufacturer.
3. The EUM sends the eUICC data (e.g., certificates and keys, capabilities) required for IFPP for each eUICC that are intended to be loaded with (a) Profile(s) to the SM-DPf on behalf of the Device Manufacturer.

4. As an alternative to step 3, the EUM provides the eUICC data to the Device Manufacturer.

5. The Device Manufacturer requests a Profile(s) from the SM-DPf. If the eUICC data were sent to the Device Manufacturer according to step 3, the request includes these data.

6. The SM-DPf creates BPPs and related SM-DPf data (e.g., certificates).

7. BPPs and related SM-DPf data are forwarded to the Device Manufacturer.

The following steps happen during the Device Production Process itself for each Profile to be loaded onto an eUICC. These steps can happen any time after completing Steps 1 to 7.

> NOTE: The number of Profiles requested at steps 5 may be a part or the totality of the Profiles requested at step 1. This allows the SM-DPf to optimize the generation (e.g. in big quantities) and actual binding (e.g. in smaller quantities), and the Device Manufacturer to optimize its stock management according to flexible procurement of eUICCs and flexible Device inventory management.

8. The Device Manufacturer sends the BPP together with the related SM-DPf data to the FPA.

9. The FPA transmits the BPP together with the related SM-DPf data to the eUICC.

10. The eUICC loads and installs the Profile.

11. The eUICC returns the Profile Installation Result to the FPA.

12. The FPA forwards the Profile Installation Result to the Device Manufacturer.

The following steps may happen after the loading of the Profiles. Alternatively, Device and eUICC may send Notifications or re-send the Profile installation result after first power up in the field to inform a pre-configured SM-DP+ about successful installation.

13. The Device Manufacturer generates a Profile Loading Report.

14. The Device Manufacturer forwards the Profile Loading Report to the SM-DPf.

15. The SM-DPf checks the integrity and the authenticity of the Profile Installation Results.

16. The SM-DPf delivers reports to the Mobile Service Provider on the loading of Profiles.

End Conditions:

The eUICCs are provisioned with Profiles at the end of the Device Production Process.

If the reporting option is chosen, the Mobile Service Provider has full information of which of its Profiles are loaded in which eUICC after Device manufacturing.

5.2 In-Factory Profile Provisioning Procedure for M2M

FFS

Annex A Use Cases (Informative)

A.1 Consumer Devices Use Case

Device maker HappyDevice produces consumer Devices. HappyDevice does not allow any online connection from within its Device production facility to the outside world. However, HappyDevice would like to produce and ship Devices that are already pre-provisioned with a Profile that helps consumer's onboarding.

In order to allow HappyDevice to provision a Profile into the eUICC residing within their Consumer Devices, HappyDevice needs to get Bound Profile Packages beforehand, store them into their production environment until the time the Device gets its individual data loaded and install the Profile into the eUICC during this final phase of the Device production.

A.2 IoT Devices Use Case

Device maker CheapDevice produces IoT Devices in large volumes. CheapDevices production facility is optimised, and production of IoT Devices needs to be fast. The way of provisioning using SGP.21/22, i.e., requiring an online connection to the SM-DP+, and several round trips for the installation of the Profile causes long delays in its production chain. These delays are to be optimised with the IFPP solution. CheapDevice does not want its production facility constrained by strong additional security requirements, e.g., get a SAS certification for its production facility.

In order to allow CheapDevice to provision a Profile into the eUICC residing within their IoT Devices, CheapDevice needs to get Bound Profile Packages beforehand, store them into their production environment until the time the Device gets its individual data loaded and install the Profile into the eUICC during this final phase of the Device production.

A.3 On-demand Profile loading during the Device Production Process - Use Case

A device maker produces devices destined for different regions of the world and thereby uses a two-stage process:

1. Manufacturing step: The device is built and then placed into stock, for example a PC motherboard or a smart meter used by electricity, gas, and water distribution companies.

2. Configuration step: The device is configured for the customer including adding the Profile from the Mobile Service Provider decided by e.g. the customer and location it is going to be used in. For example, a modem with eUICC is added to the PC motherboard from stock and a profile downloaded to it; or a smart meter with a Profile depending on its shipping location. This means the Mobile Service Provider, serial number of the device or the EID of the eUICC are not known until configuration time.

All data exchanges with external systems are strictly controlled, preventing any online or external real-time interchanges.

The profiles are shipped to the device maker in advance and are kept in stock in the premises of the Device Manufacturer or its designated 3rd party production site until the time the Device gets its individual data loaded and a Profile is installed into the eUICC during this final phase of the Device Production Process.

A.4 Device Inventory Management Use Case

Requested by a customer ABC, Device Maker HappyDevice produces 5 Million Devices that are already pre-provisioned with a Profile using IFPP. Later, before the HappyDevice ships those 5 Million Devices to ABC, ABC changes the quantity of products in this order from 5 Million to 4 Million.

To allow HappyDevice to sell the remaining 1 Million Devices to other customers, HappyDevice puts those 1 Million Devices back to its facilities in the premises of the Device Manufacturer or its designated 3rd party production site and removes all ABC's configuration including the pre-provisioned Profiles. HappyDevice sends a report to the Mobile Service Provider and/or ABC that those 1 Million Profiles were deleted. HappyDevice can configure those 1 Million Devices for another customer, potentially including the provisioning of a Profile using IFPP.

Annex B Threats and Risks (Informative)

This section lists and describes the risks that are considered by the IFPP architecture.

B.1 Malicious or compromised IFPP entity

Risk no.	Risk description
MCE01	Malicious or compromised IFPP entity uses privileged position or obtains eUICC data in order to push unsolicited Profiles to IoT or Consumer Devices.
MCE02	Malicious or compromised IFPP entity is able to tamper with Esbpp communications or eUICC data.

Table 1: Malicious or compromised IFPP entity

B.2 Cryptographic Related Risks

Risk no.	Risk description
INO1	Loss or theft of private keys in one or several Profile Management components leading to the loss of confidentiality on the whole chain.
INO2	Inability to revoke compromised Certificates leading to the loss of trust on the whole Certificate chain.
INO3	Local law enforcement requests leading to the forceful disclosure of key material.
INO4	Local law enforcement requests leading to the forceful compromise of key components.
INO5	Malicious or accidental revocation of Certificates leading to the denial of service on the whole provisioning Certificate chain.
INO6	Use of temporary symmetric cryptographic or “generic” key material during the Profile creation, temporary storage, transport, or long-term storage leading to single point of failure and attack being created.

Table 2: Cryptographic Related Risks

B.3 Quality of Service

Risk no.	Risk description
QoS1	Profile creation burst leading to the inability for the SM-DPf to deliver expected service level.

QoS2	Denial of service on IFPP entities leading to the inability to deliver expected service level.
QoS3	Inability to recover from management communication failures leading to a temporary or permanent inability to deliver a Profile.

Table 3: Quality of Service Risks

B.4 Non-human or Unpredictable

Risk no.	Risk description
EXC1	Catastrophic event such as floods, earthquakes, etc. leading to the destruction of a datacentre.
EXC2	Geopolitical/Human events leading to the destruction of a datacentre.
EXC3	Change of regulation leading to partial or total loss of trust for an actor of the provisioning delivery chain (Operator, OEM, EUM…).

Table 4: Non-human or Unpredictable Risks

Annex C In-factory provisioning flow (Informative)

The in-factory provisioning flow is intended to help a factory personnel rather than eSIM experts understand how in-factory provisioning of Profiles works. It outlines the series of steps in a descriptive way with the sender, receiver and architectural block used to send the information.

eUICC pre-condition:

- The eUICCs are ordered by the Device Manufacturer from the EUM, provisioned with an agreed number of private One-time Keys. The number of One-time Keys determines how many in-factory provisioned Profiles can be loaded during the Device Production Process.
  The EUM sends the One-time public Keys of the eUICCs to the Device Manufacturer or the SM-DPf, together with some data related to the batch of eUICCs (eUICC Info 2, eUICC certificates, EUM certificate chain) using an interoperable package over Esed2 or Esed1.

Assumed connectivity between companies:

1. The EUM is connected to the Device Manufacturer using some transport path (Esed2) over a path compliant with the EUM and Device Manufacturer requirements e.g. secured email.

2. The Device Manufacturer is connected to the SM-DPf of the Operator that will provide the Profiles over a path compliant with the Operator and Device Manufacturer requirements (Esbpp).

3. The Device Manufacturer has an ordering interface into the Operator to allow them to pass information about the Device and customer to the Operator's internal systems. The definition of the interface and data is out of scope and so this interface is not shown in section 3.1.

In-factory provisioning flow:

1. The customer orders the device, selecting the Operator and offer type that needs to be provisioned during the Device Production Process and agrees to the contractual and financial terms of the Operator.

2. The Device Manufacturer having received the Operator and Profile request from the system serving the customer and knowing the information about the system to be built for the Device Production Process, then sends the required data (one One-time Key and eUICC certificate(s) for each Profile) to the SM-DPf via Esbpp. (eUICC Info 2 and the EUM certificate chain only needs to be provided once.)

3. The Operator, having checked the contractual and financial terms of the Device Manufacturer and the customer uses the SM-DPf to create Bound Profile Packages, which are Profile Packages protected by the One-time public Keys tied to the One-time private Keys in the eUICCs to bind and encrypt the Profile Package to a single pre-known eUICC.

4. The Bound Profile Package is loaded into the in-factory provisioning system of the Device Manufacturer together with the certificate chain of the SM-DPf.

5. When the Production line is ready to load the Bound Profile into the Device, the in-factory provisioning system sends to the FPA in the Device over Esfac the Bound Profile Package. Some additional data (which includes the certificate chain of the SM-DPf) needs to be sent as well.

6. When the FPA/eUICC has completed the operation, the eUICC via the FPA sends a Profile Installation Result to the factory provisioning system. The in-factory provisioning system will then, at some point, send the Profile Installation Result to the SM-DPf via the Esbpp interface.

Annex D Document Management

D.1 Document History

Version	Date	Additions	Approval Authority	Editor / Company

V1.0	28/02/2025	CR0004R01 CR0005R01 CR0006R01 CR0007R01 CR0008R03 CR0009R01 CR0010 CR0013 CR0014 CR0012R03 CR0015R02 CR0017R01 CR0018R01 CR0019R01 CR0020R00 CR0011R06 CR0021R04 CR0022R01 CR0023R01 CR0026R05 CR0030R01 CR0031R01 CR0032R02 CR0034R02 CR0035R00 CR0036R04 CR0037R01 CR0016R07 CR0039R03 CR0041R02 CR0042R01 CR0043R00 CR0024R05 CR0033R07 CR0045R01 CR0046R01 CR0047R03 CR0048R01 CR0049R01 CR0055R00 CR0056R03 CR0059R02 CR0065R01 CR0052R02 CR0058R03	ISAG	Kangjin Yoon, Samsung

		CR0063R01 CR0062R04 CR0027R09 CR0068R02 CR0069R03 CR0073R00 CR0075R00 CR0076R01 CR0077R01 CR0079R01 CR0080R02 CR0081R01 CR0082R01 CR0083R00 CR0084R01 CR0086R00 CR0088R01 CR0072R03 CR0078R02 CR0091R04 CR0092R01 CR0096R03 CR0098R01 CR0066R11 CR0094R04 CR0103R01 CR0104R01 CR0089R01 CR0101R02 CR0105R03 CR0106R02 CR0108R02 CR0109R01 CR0110R01 CR0111R02 CR0124R07 CR0128R01 CR0127R04 CR0130R01 CR0131R00 CR0132R02 CR0135R01 CR131R00		

D.2 Other Information

Type	Description
Document Owner	eSIMWG1
Editor / Company	Kangjin Yoon, Samsung

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.