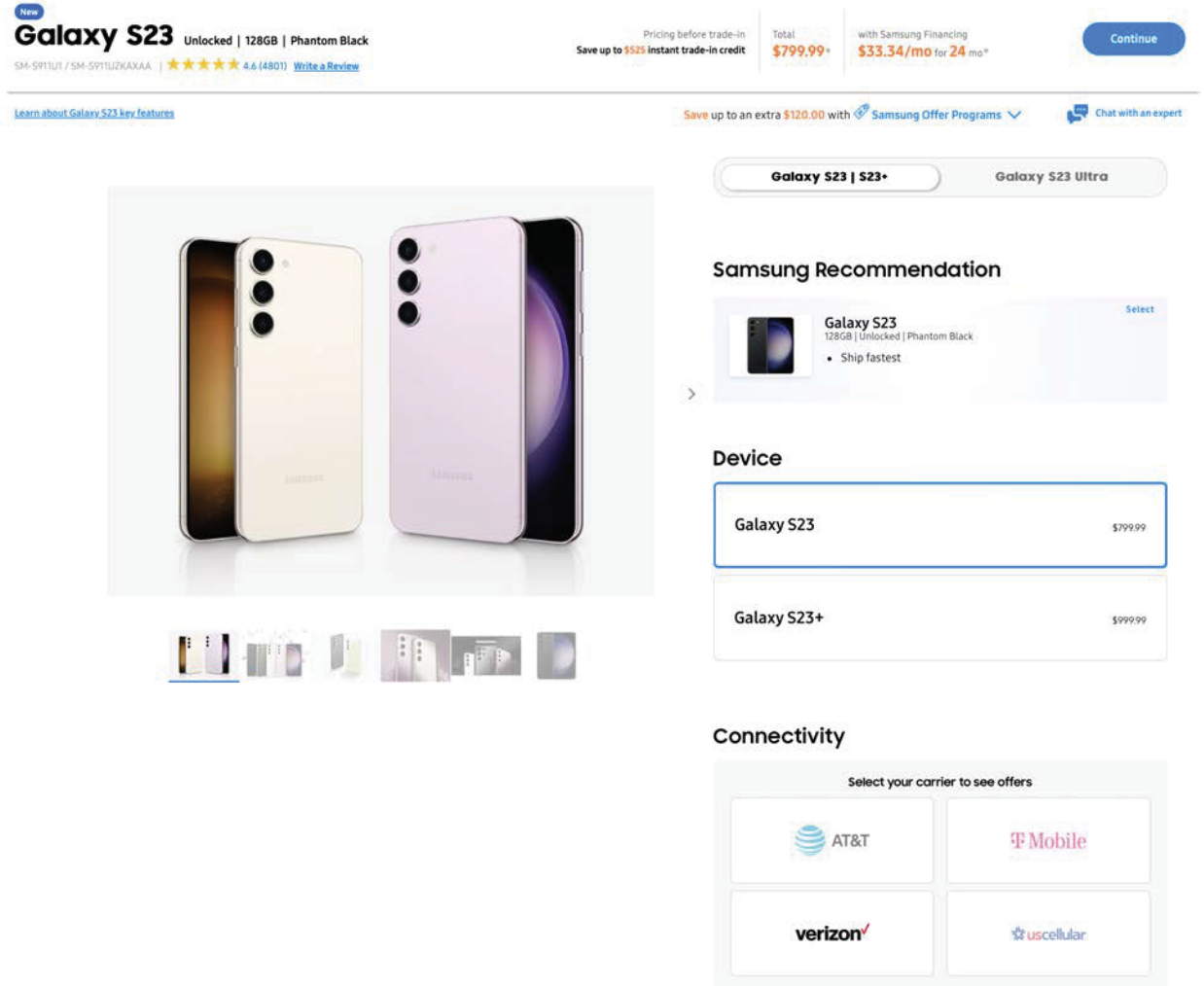
U.S. Patent No. 9,609,510 ("'510 Patent")

Accused Devices: Samsung phones, tablets, watches, and other eSim-enabled devices and all versions and variations thereof since the issuance of the asserted patent.

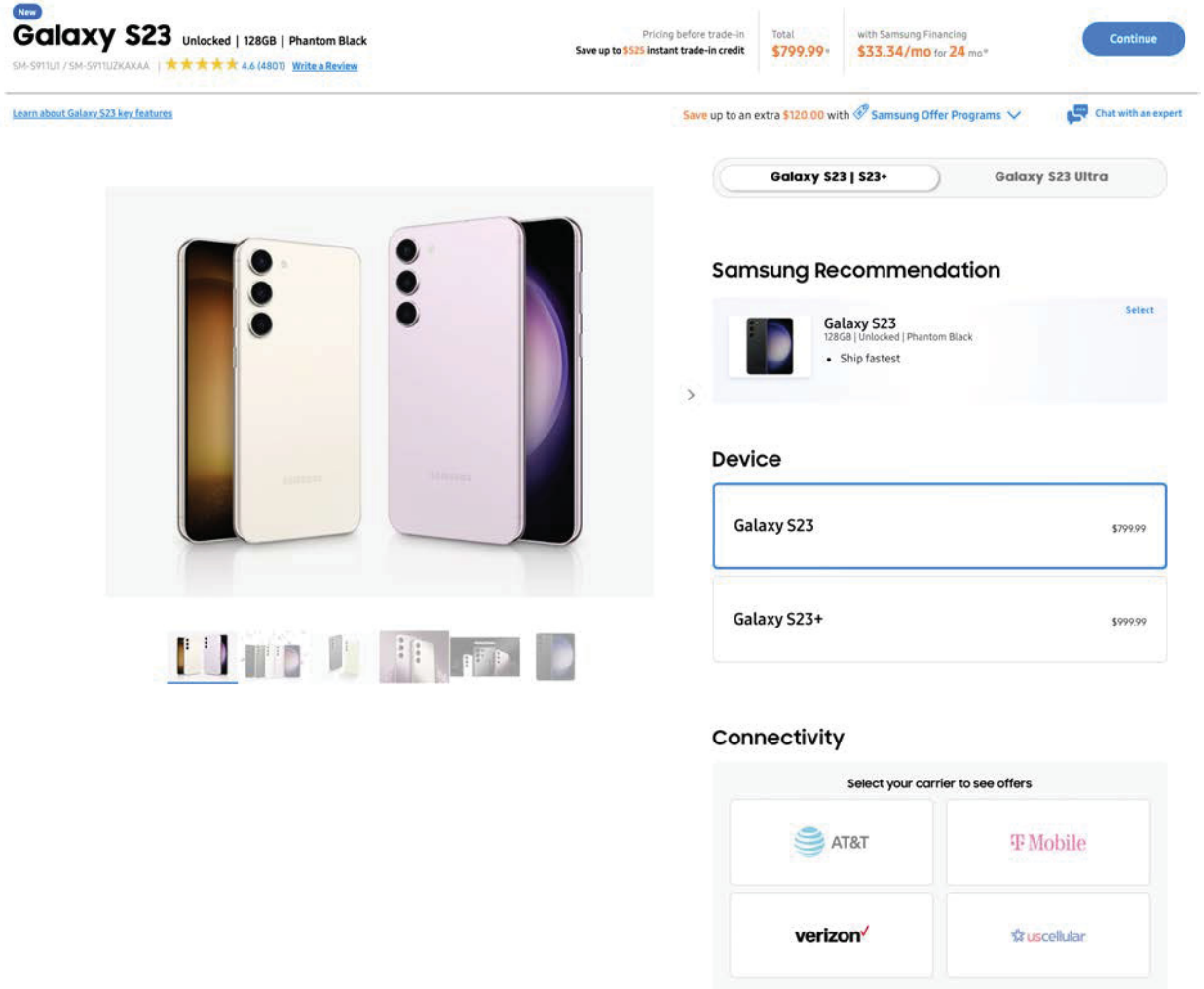
Claim 1

Issued Claim(s)	Public Documentation
1. A wireless device, comprising:	Samsung phones, tablets, watches, and other eSim-enabled devices are each "a wireless device." For example, the Galaxy S23 is a "wireless device." *See, e.g.,* https://www.samsung.com/us/smartphones/galaxy-s23/buy/galaxy-s23-128gb-unlocked-sm-s911uzkaxaa/

Exhibit 1171
Samsung v. Headwater
IPR2025-00483

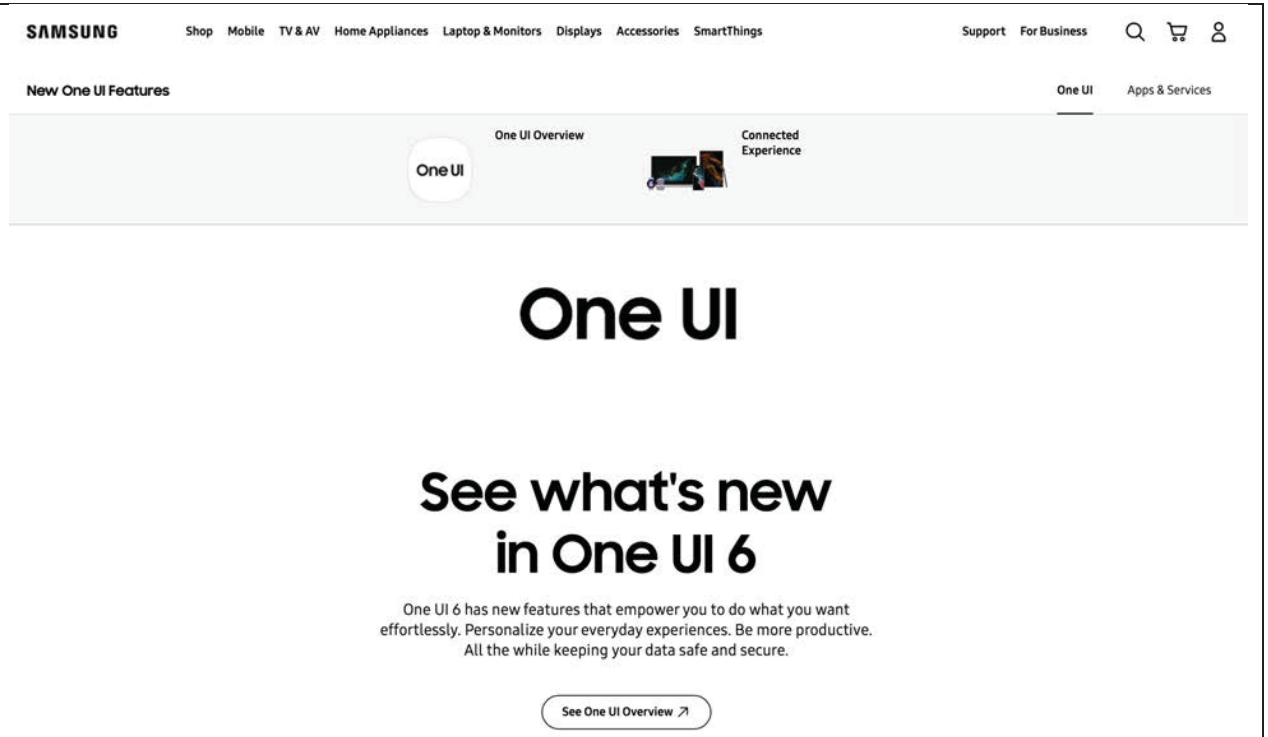
	
[1a] a user interface;	Samsung Galaxy phones and tablets each comprise "a user interface." *See, e.g.,* https://www.samsung.com/us/smartphones/galaxy-s23/buy/galaxy-s23-128gb-unlocked-sm-s911uzkaxaa/

2



; https://www.samsung.com/in/one-ui/features/:

3

4	 ; https://downloadcenter.samsung.com/content/UM/202404/20240418062905861/SAM_S911_S916_S918_EN_UG_OS14_041624_FINAL_REV_1.1.pdf:

5

SIM manager

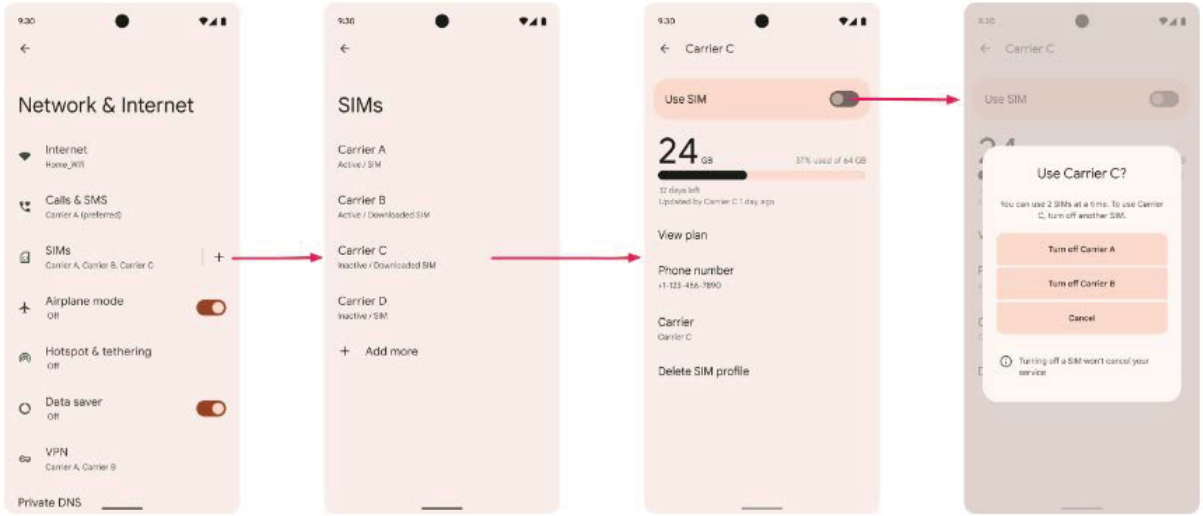
Your wireless service provider and service plan may support the ability to use a dual SIM (two physical SIM cards) or an eSIM (embedded SIM) so that you can manage two mobile accounts without carrying two devices. Options may vary by service provider.

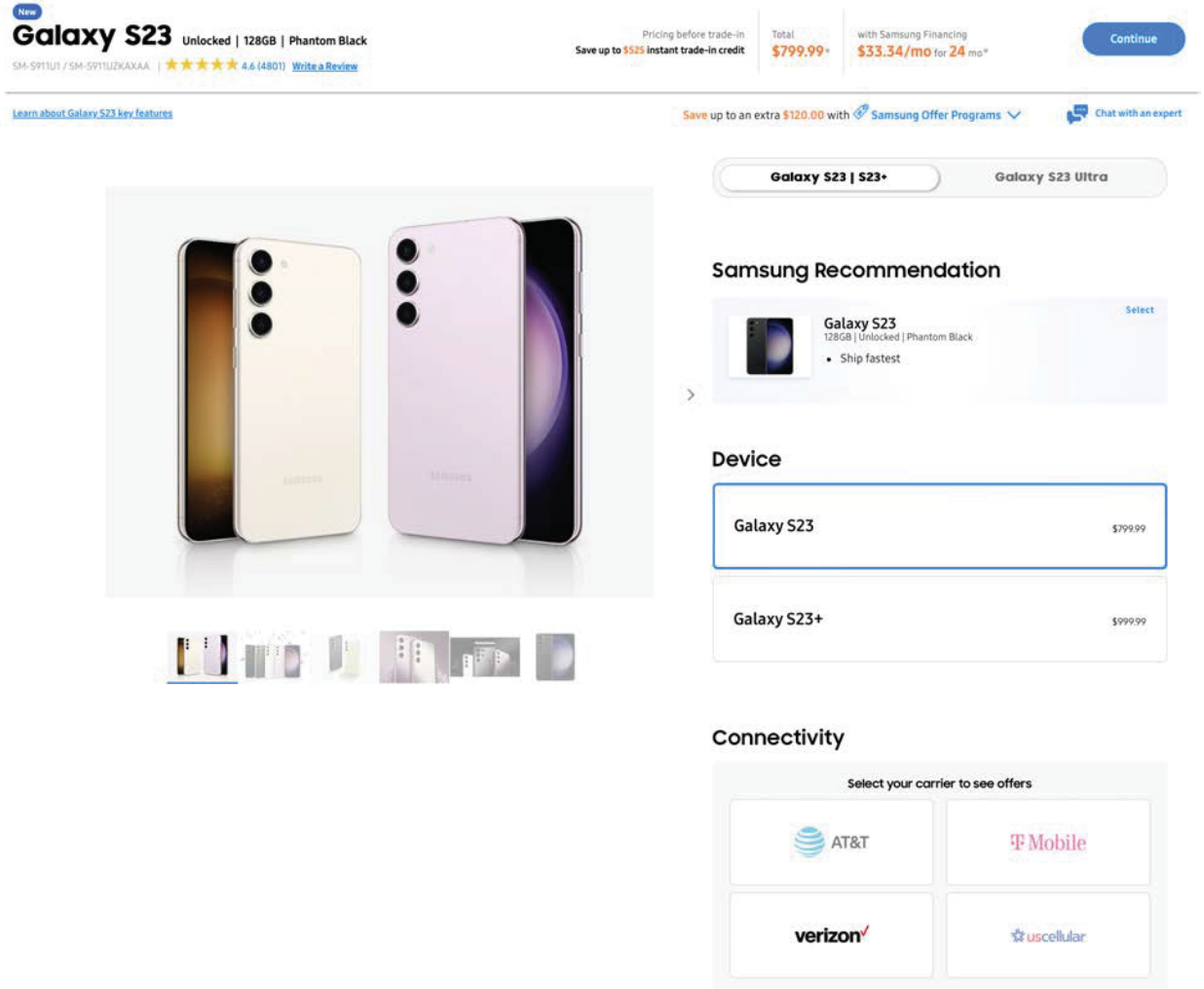
Devices that support dual SIM contain two SIM card slots. It may also have a microSD card slot for expandable storage if supported. Devices that support dual SIM will receive software updates that enable the built-in dual SIM capability after launch.

Devices that support an eSIM can be programmed to work independently of the physical SIM card in the device. This allows for either the eSIM or the physical SIM card to be used for voice call/text and data. Devices that support eSIM will receive software updates that enable the built-in eSIM capability after launch.

- From Settings, tap **Connections** > **SIM manager** for the following options:
  - **SIM cards**: Enable, disable, or rename installed physical SIM cards in your device.
  - **eSIMs**: Tap **Add eSIM** to sign up for a new eSIM mobile plan or to add a plan from an old device.
  - **Primary SIM**: When using multiple SIM cards, set a primary card to be used for calls, texts, and data.
  - **More SIM settings**: Tap to explore additional management options for your SIM cards.

See also https://source.android.com/docs/core/connect/esim-overview; https://source.android.com/docs/core/connect/esim-euicc-api; https://source.android.com/docs/core/connect/esim-error-handling; https://source.android.com/docs/core/connect/esim-mep:

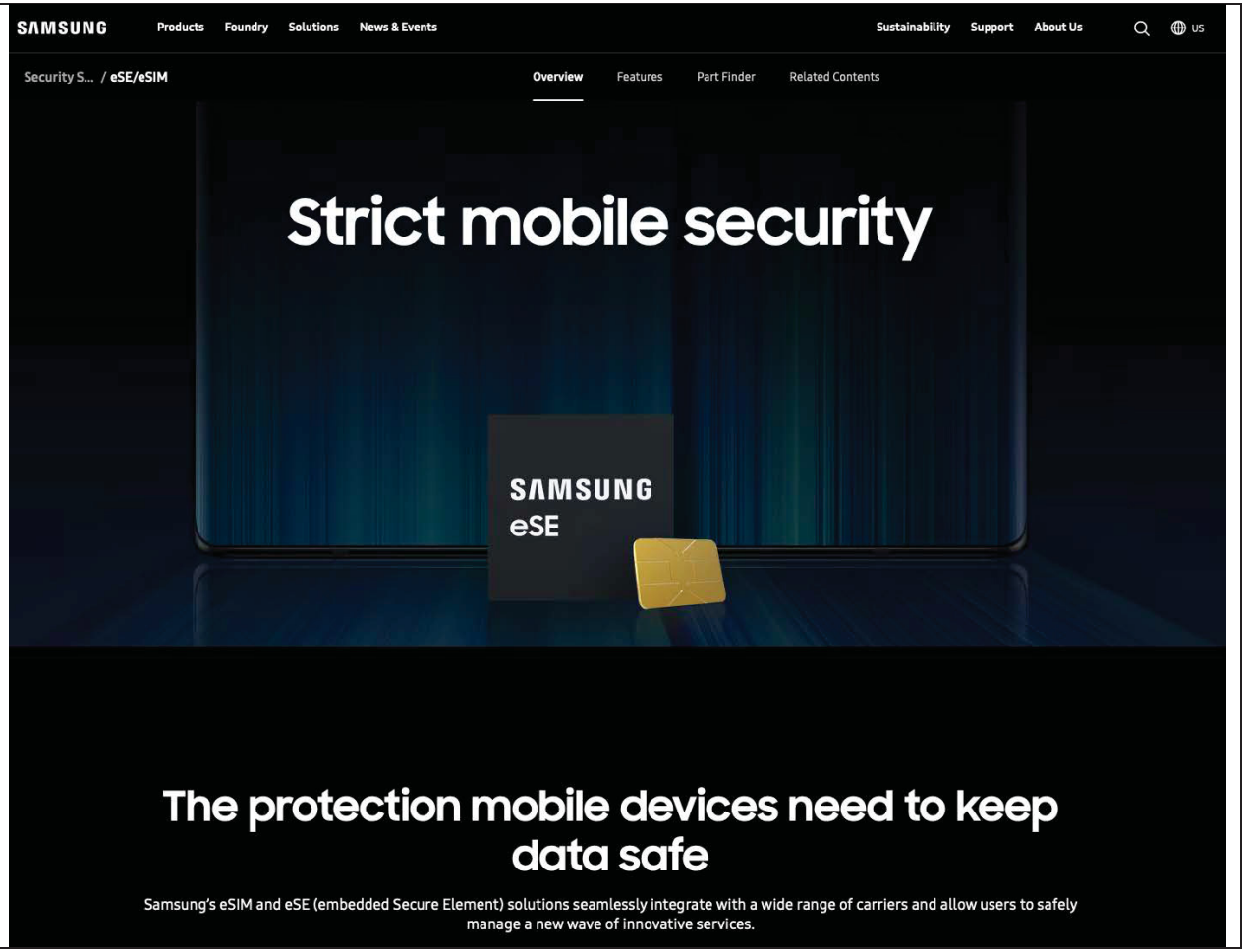
	User interface To resolve the ambiguity of eSIM port selection, on devices supporting MEP, users must be able to disable one of the active subscriptions to enable a new subscription. In Android 13, AOSP includes a user flow with a three-choice dialog that can be applied to subscription enabling user flows from the Settings app. Figure 6 shows an example of this UX flow.  **Figure 6.** User flow for enabling SIM subscription
[1b] memory configured to store:	Samsung Galaxy phones and tablets comprise "memory configured to store." For example, the Galaxy S23 comprises at least memory, storage, and SIM capabilities. *See, e.g.,* https://www.samsung.com/us/smartphones/galaxy-s23/buy/galaxy-s23-128gb-unlocked-sm-s911uzkaxaa/

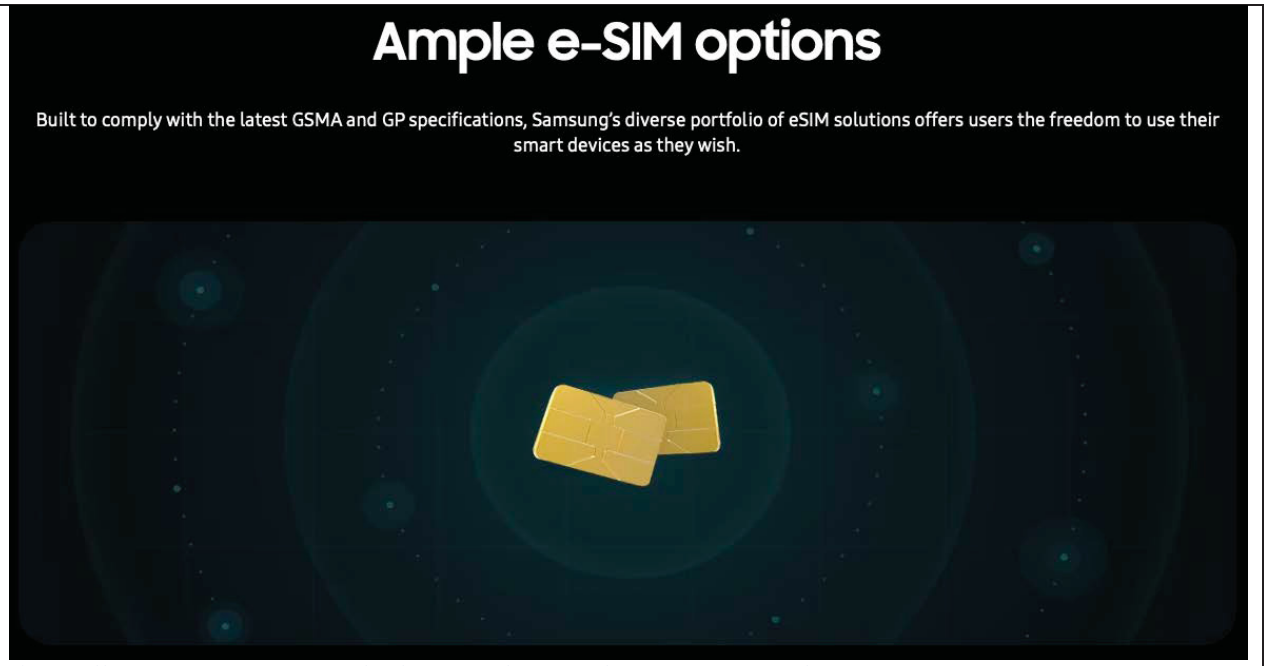


; https://www.samsung.com/us/smartphones/galaxy-s23/specs/:

	Galaxy S23 Ultra	Galaxy S23+	Galaxy S23
Storage			
	-	-	128GB
	256GB	256GB	256GB
	512GB	512GB	-
	1TB	-	-

; https://semiconductor.samsung.com/us/security-solution/ese-esim/:


SAMSUNG
Products
Foundry
Solutions
News & Events
Sustainability
Support
About Us
US
Security S... / eSE/eSIM
Overview
Features
Part Finder
Related Contents
Strict mobile security
SAMSUNG
eSE
The protection mobile devices need to keep data safe
Samsung's eSIM and eSE (embedded Secure Element) solutions seamlessly integrate with a wide range of carriers and allow users to safely manage a new wave of innovative services.

	 https://www.samsung.com/us/support/answer/ANS00079039/:

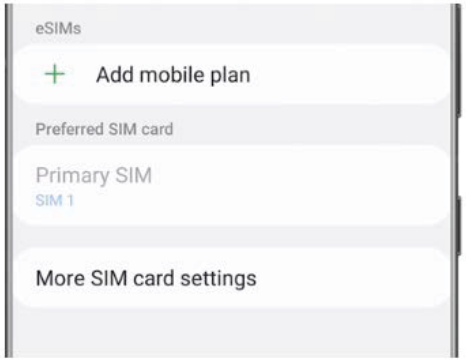
10

Using the eSIM

An eSIM is an embedded version of the physical SIM card on the phone. The eSIM provides connection to your carrier's network, however instead of inserting a card, you will activate it with your carrier account information. You can also use the eSIM alongside a physical SIM to add a second phone number or carrier to your phone.

Manage your SIM and eSIM

1. Open **Settings** and then tap **Connections**.
2. Tap **SIM card manager**.



From here you can tap the **switch** next to your physical SIM, or activated eSIM to enable or disable their connections. You can also tap **Primary SIM** to change the default connection for making calls, sending texts, and using data.

To start using the eSIM, you will need to follow your carrier's instructions.

- **T-Mobile activation**
- **Verizon activation**
- **AT&T activation**

; https://www.samsung.com/ph/support/mobile-devices/how-to-activate-esim-on-a-galaxy-device/:

12

How to activate eSIM on a Galaxy device

Last Update date : Jul 24. 2023

Your device includes an eSIM which functions as a SIM card. You can use the mobile network after activating the eSIM or installing a nano-SIM card. You can both activate the eSIM and install a nano-SIM card so you can have two phone numbers or service providers for a single device.

In some areas, data transfer speeds may be slower if two SIM cards are inserted in the device than when one SIM card is inserted.

Before you try out the below recommendations as to your solution, be sure to check if your device's software is updated with the latest version. Please check how to update your mobile device's software in the following order.

Step 1. Go to **Settings > Software update**.

Step 2. Tap on **Download and install**.

Step 3. Follow the on-screen instructions.

How to add your mobile plan on your smartphone with eSIM

To add your mobile network plan on an eSIM, you can scan a QR code that your carrier provided or install a pre-assigned plan automatically. Before adding your plan, make sure your Galaxy smartphone is connected to a wi-fi or mobile data network.

Note: Device screenshots and menus may vary depending on the device model and software version.

; https://www.samsung.com/us/support/search/?query=galaxy+activate+esim&referrerPageUrl=https%3A%2F%2Fwww.samsung.com%2Fus%2Fsupport%2F&tabOrder=index.html%2Cfaqs%2Canswers%2Ctroubleshooting_guides%2Csupport_videos%2Cresources%2Ccommunity_posts%2Clinks%2Cproducts&facetFilters=%7B%7D&filters=%7B%7D&verticalUrl=faqs.html:

SAMSUNG Shop Mobile TV & Audio Appliances Computing Displays Accessories SmartThings Explore Support For Business

galaxy activate esim

All FAQs Answers Troubleshooting Guides Videos Resources Community Posts More

1 - 10 of 11

What is a hybrid eSIM card and how does it work?

What is an eSIM card and how does it differ from a physical SIM card?

An eSIM card, or embedded SIM card, is a digital SIM that is built directly into a device, eliminating the need for a physical SIM card. Instead of inserting a physical card, the device's eSIM connects to a cellular network remotely by downloading the necessary information from the network provider. This allows for greater flexibility, as users can switch between different carriers without physically changing the SIM card.

Important: Your network provider/mobile carrier (i.e. AT&T, Verizon, T-Mobile, etc.) is your best resource for carrier-specific information such as transferring your phone number from one sim card to another. Visit your providers online support content for more carrier-specific details:

- AT&T SIM card support content
- Verizon SIM card support content
- Xfinity/Comcast SIM card support content
- T-Mobile SIM card support content
- Charter Spectrum SIM card support content

Can I transfer my existing mobile number to an eSIM or hybrid eSIM card?

Can I use an eSIM or hybrid eSIM card in any device?

Can I activate a Windows AAOEM license on a virtual machine

What should I do if I encounter activation issues with a Windows AAOEM license?

How do I redeem a promotion for a subscription service?

What is a Windows AAOEM license?

After inserting a new SIM card my phone is asking for a PIN or Unlock Code

Help with Google Factory Reset Protection (FRP)

; https://www.att.com/search/?q=sim%20card&catField=Support; https://www.verizon.com/onesearch/search?q=sim%20card&ES=support&src=wireless; https://www.t-mobile.com/search?q=sim%20card&category=support; *see also, e.g.,* https://www.gsma.com/esim/wp-content/uploads/2022/10/SGP.22-v3.0-1.pdf:

4.3 eUICC Information

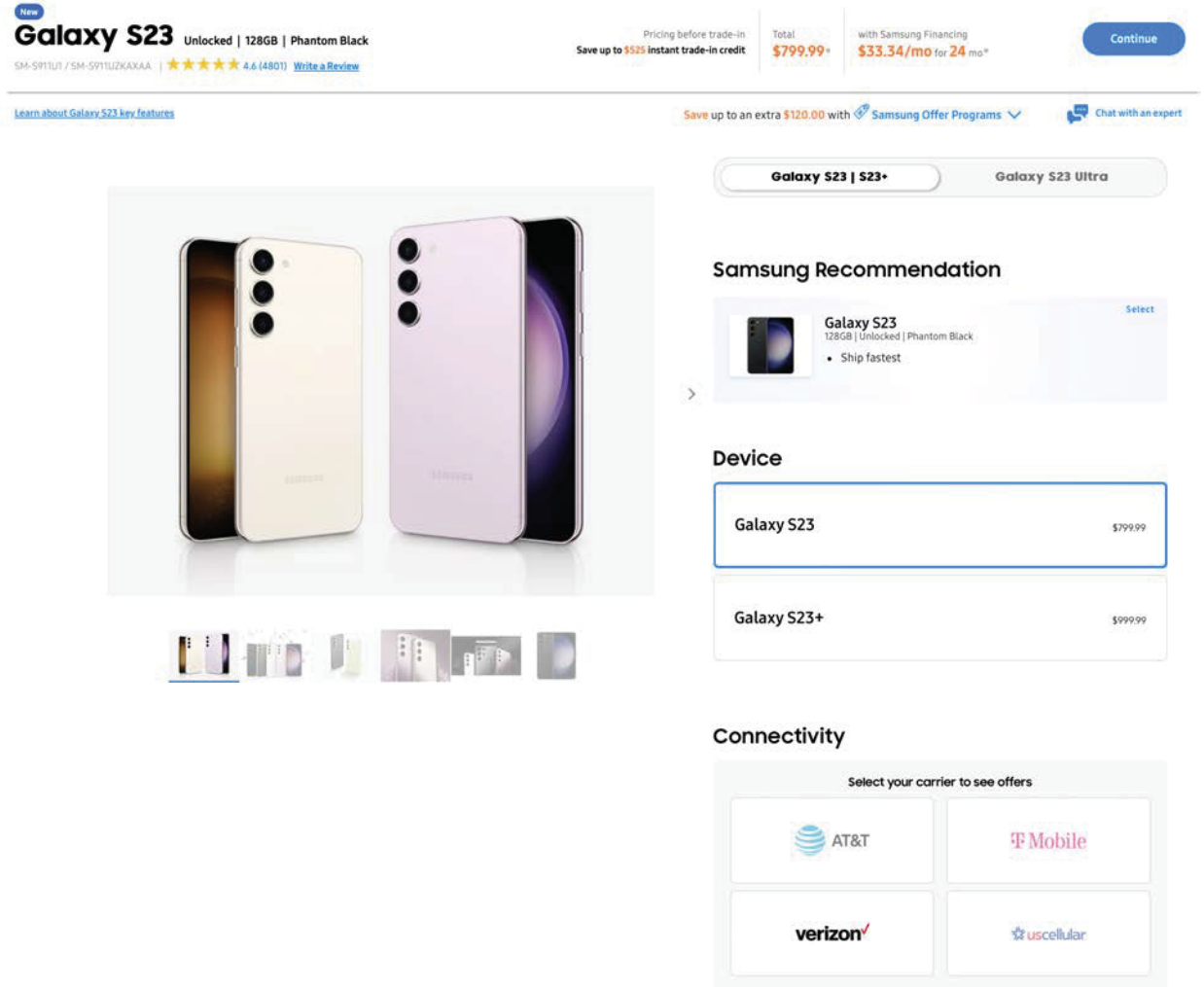
The eUICC information comprises EUICCInfo1 and EUICCInfo2. EUICCInfo1 is a subset of EUICCInfo2, designed to be sent to an RSP Server before it is authenticated. EUICCInfo2 contains the full eUICC information and is disclosed to an RSP Server only after it is authenticated.

The eUICC information SHALL be generated by the eUICC and MAY be requested by the LPA at any point in time.

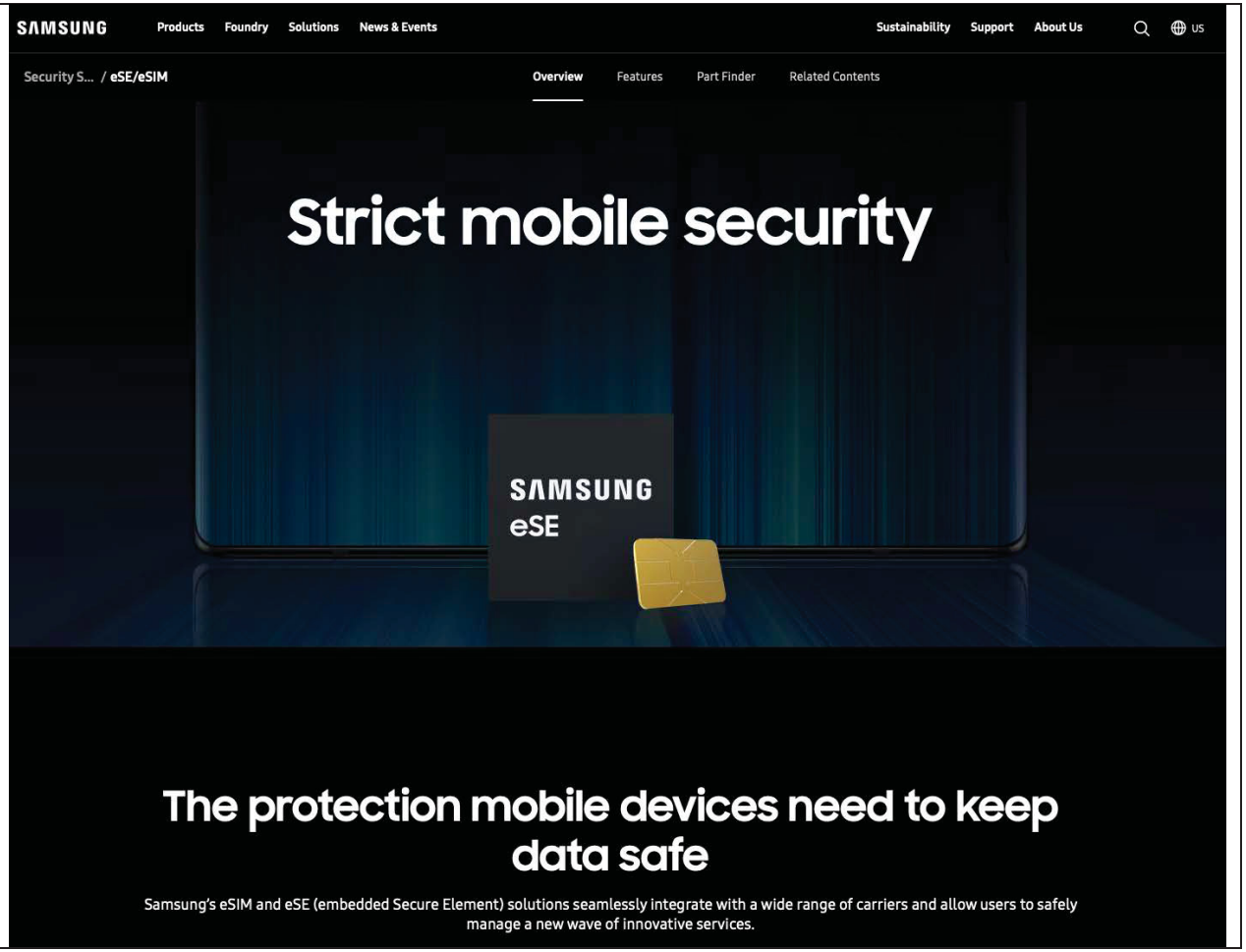
The eUICC information includes:

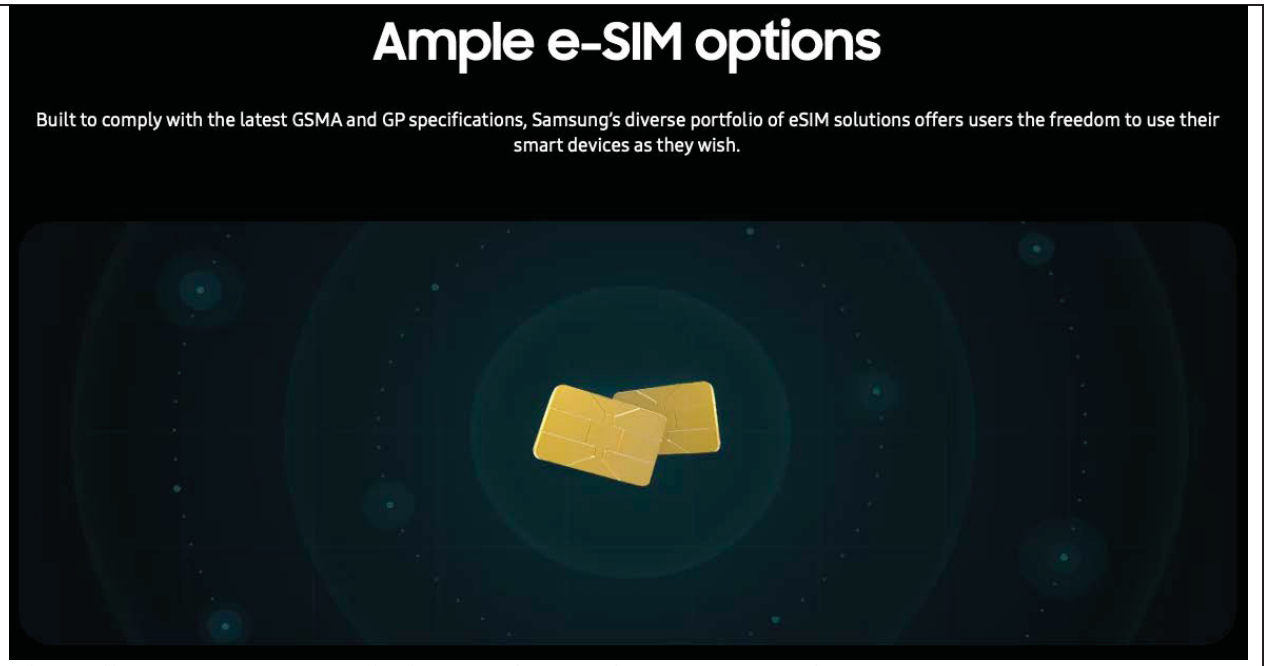
- Profile Package Versions
- Specification Version Numbers
- Firmware version
- Available amount of non-volatile memory
- UICC capabilities
- ETSI TS 102 241 version
- GlobalPlatform version
- RSP capabilities
- Lists of supported eSIM CA RootCA Public Key Identifiers
- eUICC Category
- Forbidden PPRs
- Protection Profile version
- SAS Accreditation Number
- Certification Data Object
- TRE properties
- TRE product reference
- LPA Mode
- EUM specific information

	2.4.4 ISD-P The ISD-P is the on-card representative of the SM-DP+ and is a secure container (Security Domain) for the hosting of a Profile. The ISD-P is used for the Profile download and installation in collaboration with the Profile Package Interpreter for the decoding/interpretation of the received Profile Package. An ISD-P hosts a unique Profile. No component outside the ISD-P SHALL have visibility or access to any Profile Component with the exception of the ISD-R, which SHALL have access to Profile Metadata. A Profile Component SHALL NOT have any visibility of, or access to, components outside its ISD-P. An ISD-P SHALL NOT have any visibility of, or access to, any other ISD-P. Deletion of a Profile SHALL remove the containing ISD-P and all Profile Components of the Profile. *See also* https://source.android.com/docs/core/connect/esim-euicc-api; https://source.android.com/docs/core/connect/esim-error-handling; https://source.android.com/docs/core/connect/esim-mep; https://source.android.com/docs/core/connect/esim-overview.
[1c] one or more credentials associated with the wireless device, the one or more credentials for authorizing the wireless device to use a wireless access network to access one or more services, and	Samsung Galaxy phones and tablets comprise "one or more credentials associated with the wireless device, the one or more credentials for authorizing the wireless device to use a wireless access network to access one or more services." For example, Samsung Galaxy phones and tablets such as the Galaxy S23 each have unique identifiers corresponding to each device's eSim capability as well as eSim activation software including. *See, e.g.,* https://www.samsung.com/us/smartphones/galaxy-s23/buy/galaxy-s23-128gb-unlocked-sm-s911uzkaxaa/



; https://www.samsung.com/us/smartphones/galaxy-s23/specs/; https://semiconductor.samsung.com/us/security-solution/ese-esim/:


SAMSUNG
Products
Foundry
Solutions
News & Events
Sustainability
Support
About Us
US
Security S... / eSE/eSIM
Overview
Features
Part Finder
Related Contents
Strict mobile security
SAMSUNG
eSE
The protection mobile devices need to keep data safe
Samsung's eSIM and eSE (embedded Secure Element) solutions seamlessly integrate with a wide range of carriers and allow users to safely manage a new wave of innovative services.

	 ; https://www.samsung.com/us/support/answer/ANS00079039/:

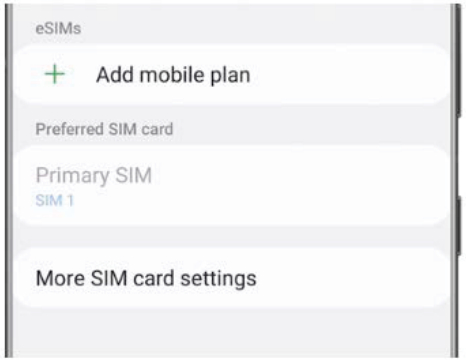
18

Using the eSIM

An eSIM is an embedded version of the physical SIM card on the phone. The eSIM provides connection to your carrier's network, however instead of inserting a card, you will activate it with your carrier account information. You can also use the eSIM alongside a physical SIM to add a second phone number or carrier to your phone.

Manage your SIM and eSIM

1. Open **Settings** and then tap **Connections**.
2. Tap **SIM card manager**.



From here you can tap the **switch** next to your physical SIM, or activated eSIM to enable or disable their connections. You can also tap **Primary SIM** to change the default connection for making calls, sending texts, and using data.

To start using the eSIM, you will need to follow your carrier's instructions.

- **T-Mobile activation**
- **Verizon activation**
- **AT&T activation**

; https://www.samsung.com/ph/support/mobile-devices/how-to-activate-esim-on-a-galaxy-device/:

How to activate eSIM on a Galaxy device

Last Update date : Jul 24. 2023

Your device includes an eSIM which functions as a SIM card. You can use the mobile network after activating the eSIM or installing a nano-SIM card. You can both activate the eSIM and install a nano-SIM card so you can have two phone numbers or service providers for a single device.

In some areas, data transfer speeds may be slower if two SIM cards are inserted in the device than when one SIM card is inserted.

Before you try out the below recommendations as to your solution, be sure to check if your device's software is updated with the latest version. Please check how to update your mobile device's software in the following order.

Step 1. Go to **Settings > Software update**.

Step 2. Tap on **Download and install**.

Step 3. Follow the on-screen instructions.

How to add your mobile plan on your smartphone with eSIM

To add your mobile network plan on an eSIM, you can scan a QR code that your carrier provided or install a pre-assigned plan automatically. Before adding your plan, make sure your Galaxy smartphone is connected to a wi-fi or mobile data network.

Note: Device screenshots and menus may vary depending on the device model and software version.

; https://www.samsung.com/us/support/search/?query=galaxy+activate+esim&referrerPageUrl=https%3A%2F%2Fwww.samsung.com%2Fus%2Fsupport%2F&tabOrder=index.html%2Cfaqs%2Canswers%2Ctroubleshooting_guides%2Csupport_videos%2Cresources%2Ccommunity_posts%2Clinks%2Cproducts&facetFilters=%7B%7D&filters=%7B%7D&verticalUrl=faqs.html:

SAMSUNG Shop Mobile TV & Audio Appliances Computing Displays Accessories SmartThings Explore Support For Business

galaxy activate esim

All FAQs Answers Troubleshooting Guides Videos Resources Community Posts More

1 - 10 of 11

What is a hybrid eSIM card and how does it work?

What is an eSIM card and how does it differ from a physical SIM card?

An eSIM card, or embedded SIM card, is a digital SIM that is built directly into a device, eliminating the need for a physical SIM card. Instead of inserting a physical card, the device's eSIM connects to a cellular network remotely by downloading the necessary information from the network provider. This allows for greater flexibility, as users can switch between different carriers without physically changing the SIM card.

Important: Your network provider/mobile carrier (i.e. AT&T, Verizon, T-Mobile, etc.) is your best resource for carrier-specific information such as transferring your phone number from one sim card to another. Visit your providers online support content for more carrier-specific details:

- AT&T SIM card support content
- Verizon SIM card support content
- Xfinity/Comcast SIM card support content
- T-Mobile SIM card support content
- Charter Spectrum SIM card support content

Can I transfer my existing mobile number to an eSIM or hybrid eSIM card?

Can I use an eSIM or hybrid eSIM card in any device?

Can I activate a Windows AAOEM license on a virtual machine

What should I do if I encounter activation issues with a Windows AAOEM license?

How do I redeem a promotion for a subscription service?

What is a Windows AAOEM license?

After inserting a new SIM card my phone is asking for a PIN or Unlock Code

Help with Google Factory Reset Protection (FRP)

; https://www.att.com/search/?q=sim%20card&catField=Support; https://www.verizon.com/onesearch/search?q=sim%20card&ES=support&src=wireless; https://www.t-mobile.com/search?q=sim%20card&category=support.

Samsung Galaxy phones and tablets comply with the GSMA eSim specification. https://semiconductor.samsung.com/us/security-solution/ese-esim/; https://research.samsung.com/blog/eSIM-and-the-Latest-eSIM-V3-0-Release:

22

The procedure of remotely provisioning a Profile into an eSIM is called as "Remote SIM Provisioning" (RSP) in the GSMA eSIM specifications, and Figure 2 illustrates the overall RSP architecture.

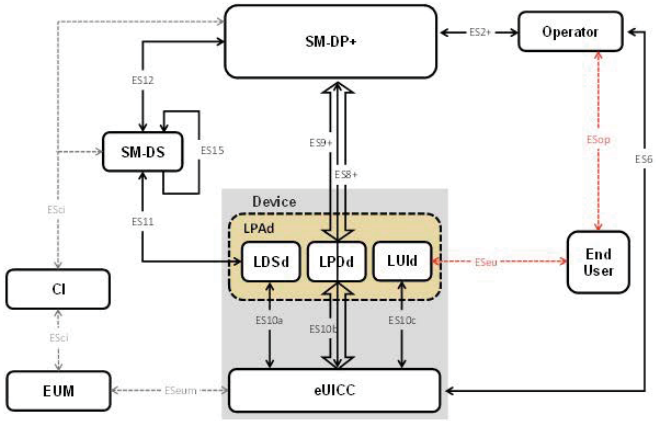


Figure 2. Overall RSP architecture [1]

https://www.gsma.com/esim/wp-content/uploads/2022/10/SGP.22-v3.0-1.pdf:

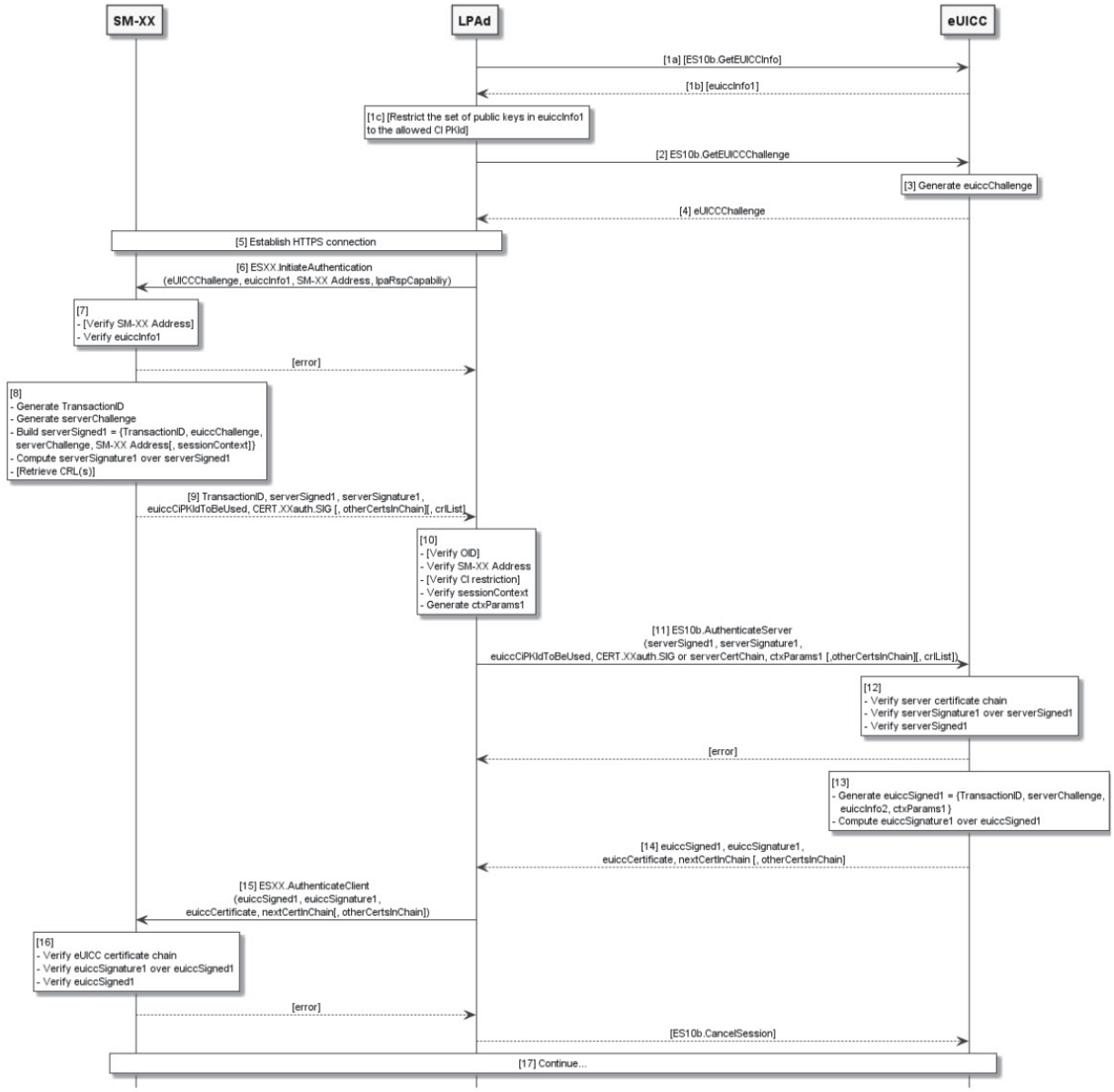


Figure 8a: Common Mutual Authentication Procedure

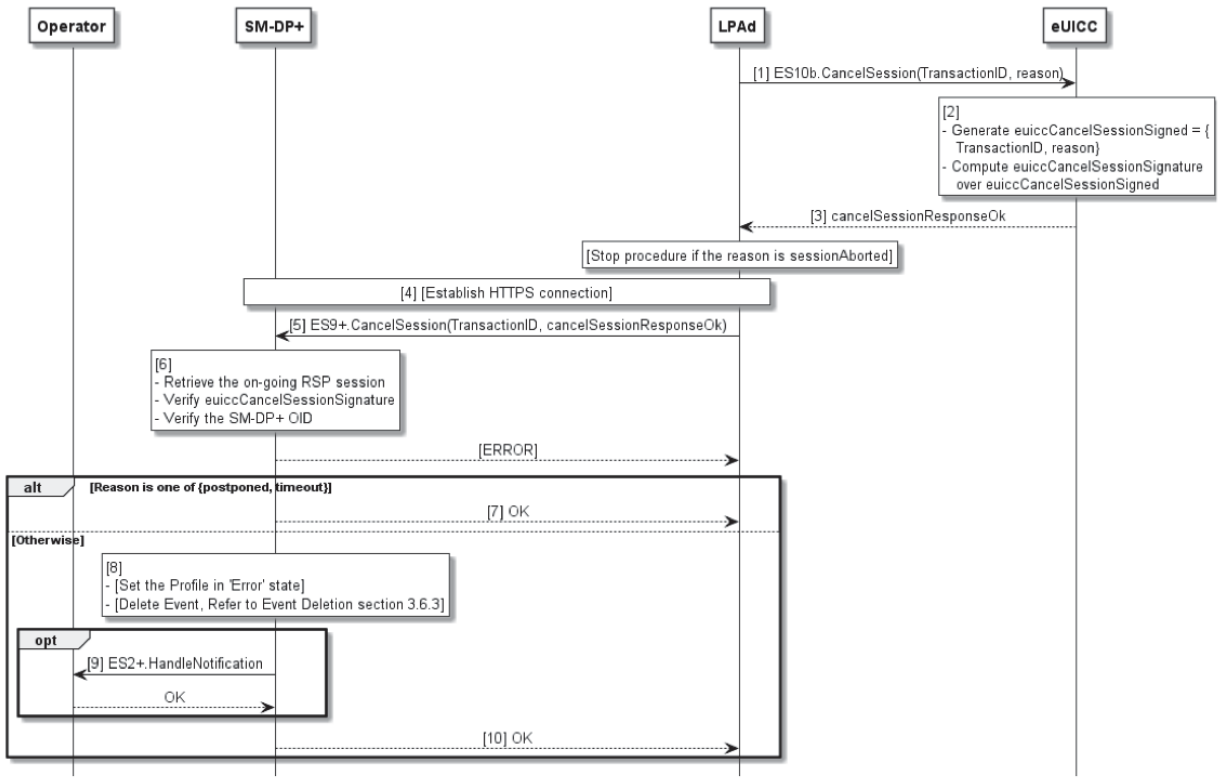


Figure 8b: Common Cancel Session Procedure

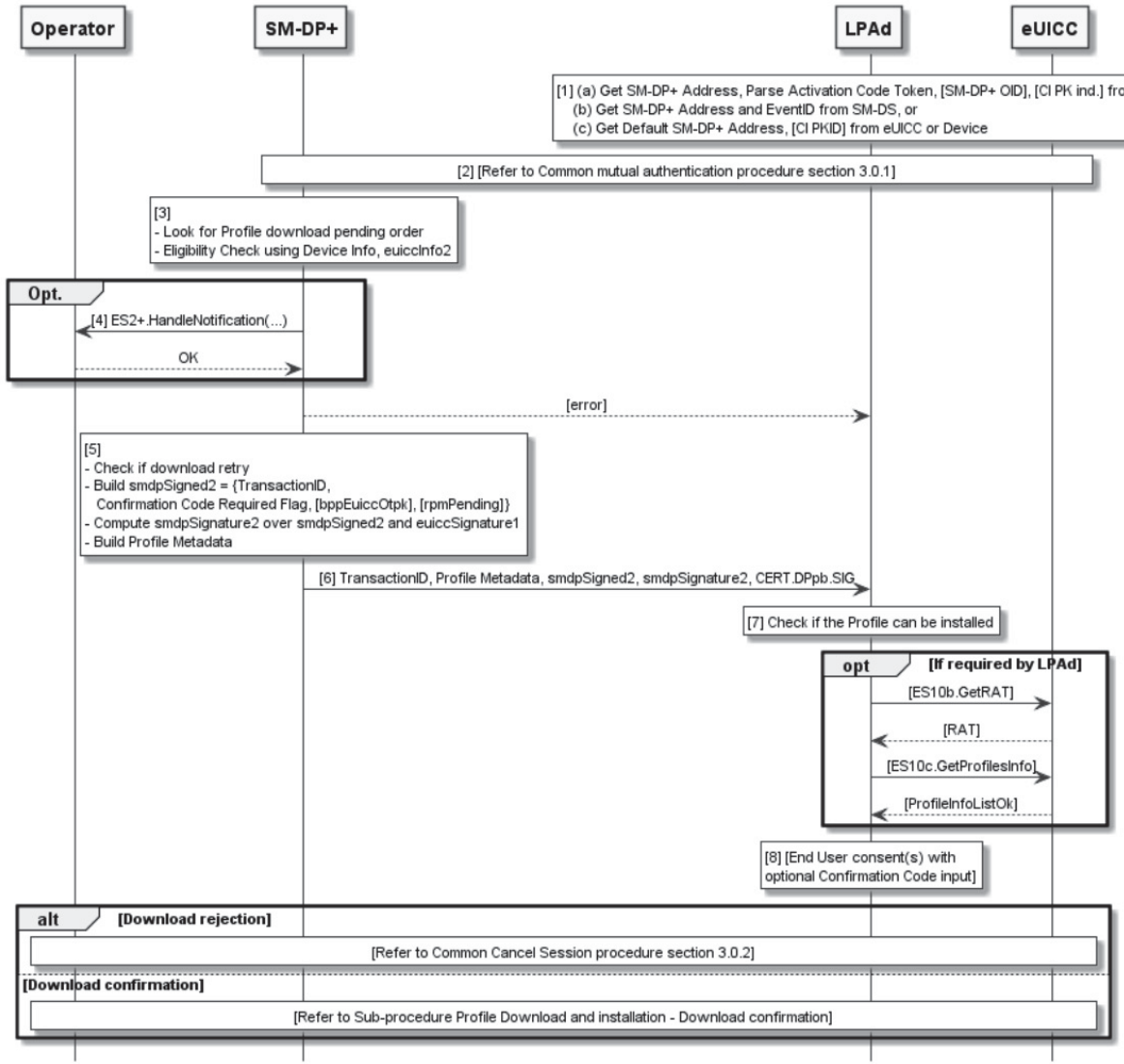


Figure 11: Profile Download and Installation

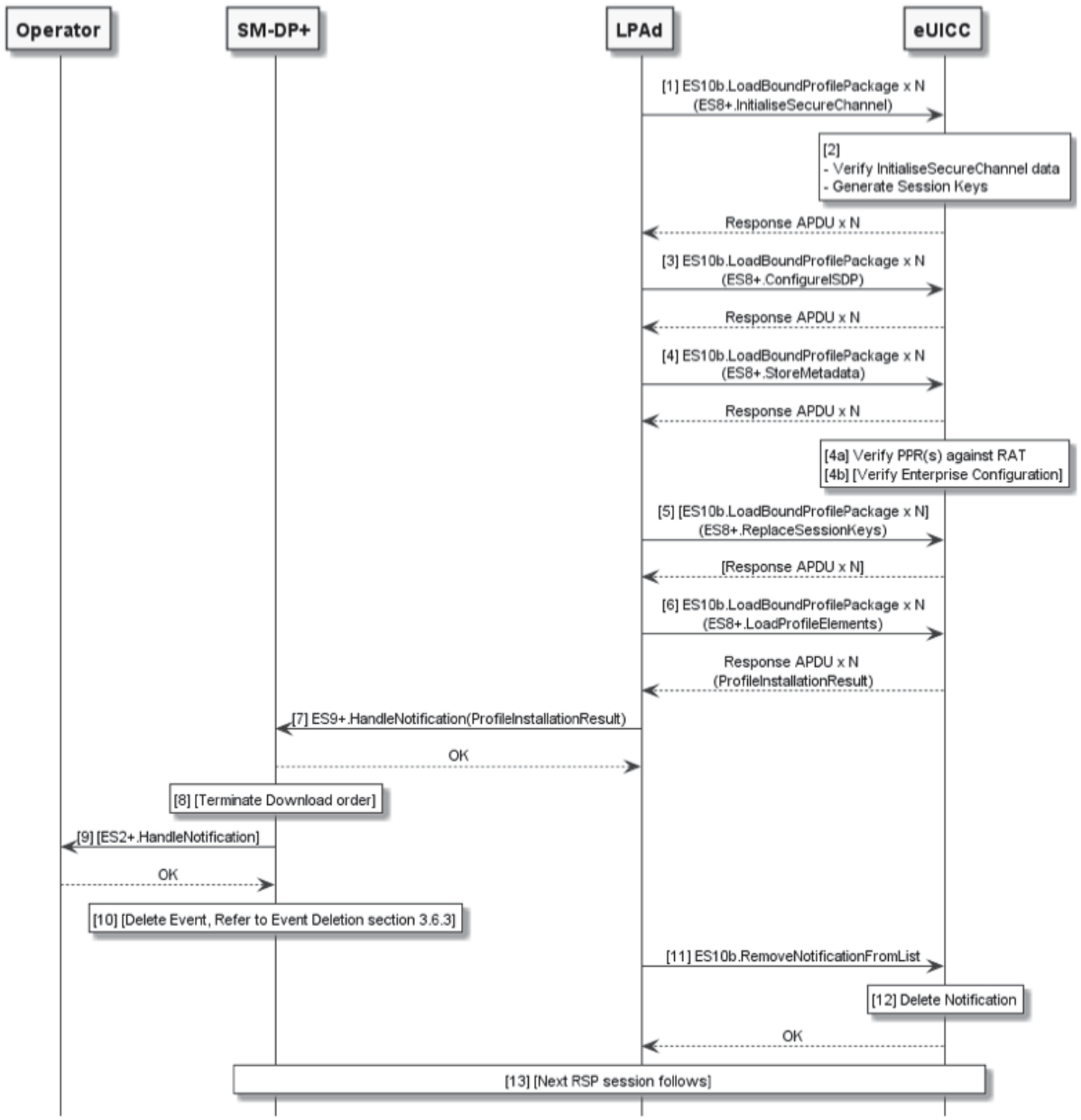


Figure 14: Sub-procedure Profile Installation

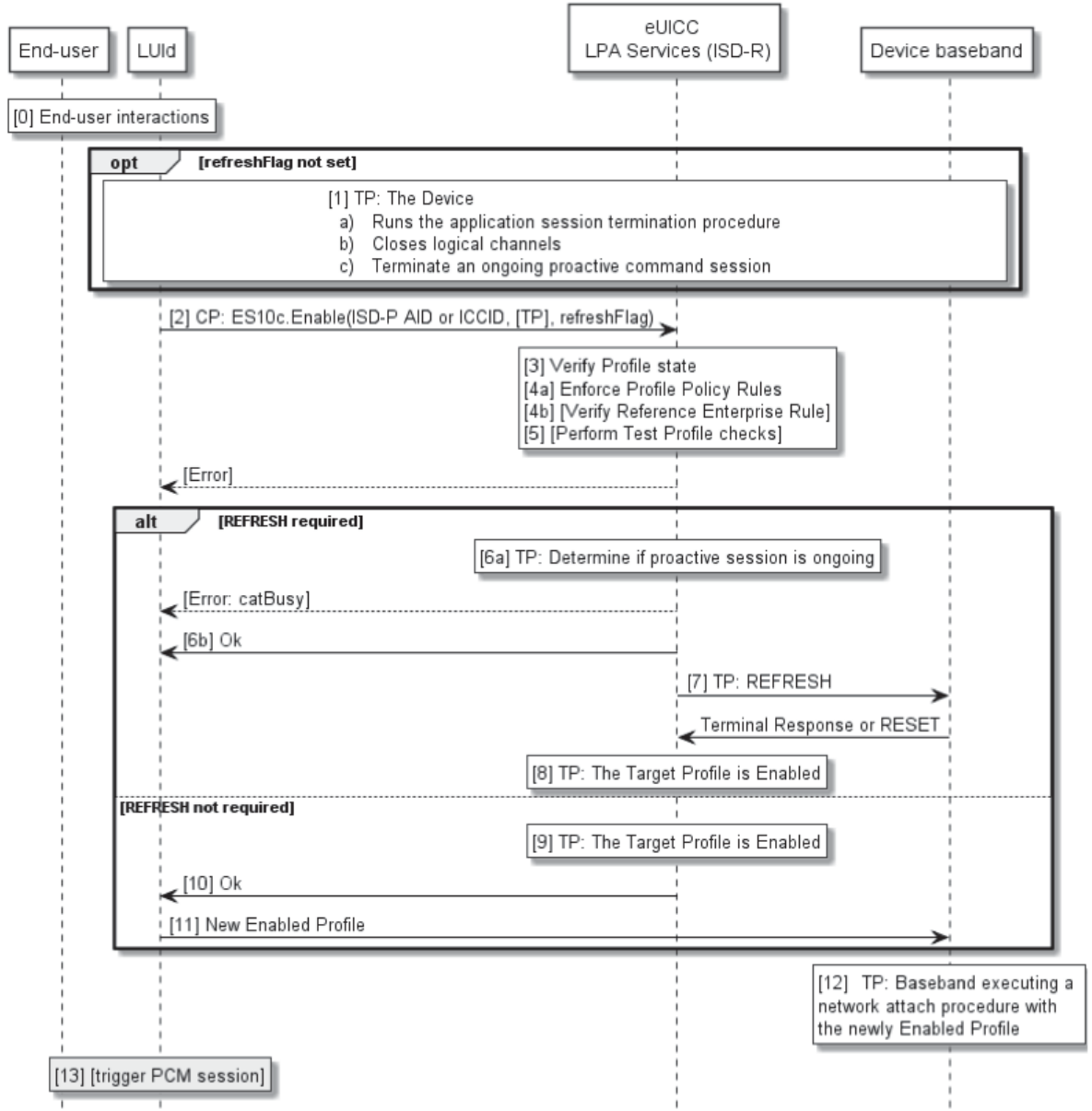


Figure 16: Enable Profile

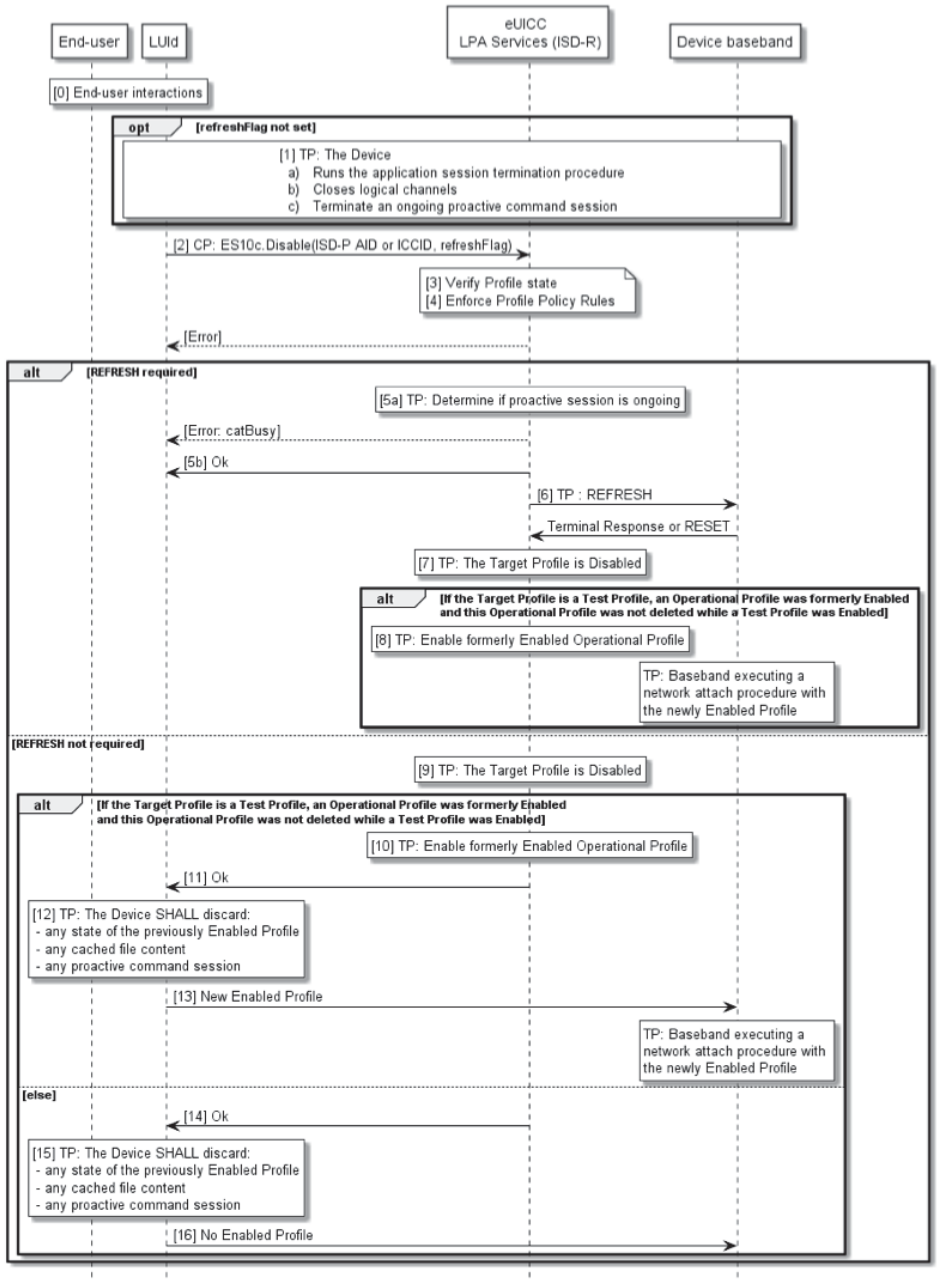


Figure 17: Disable Profile

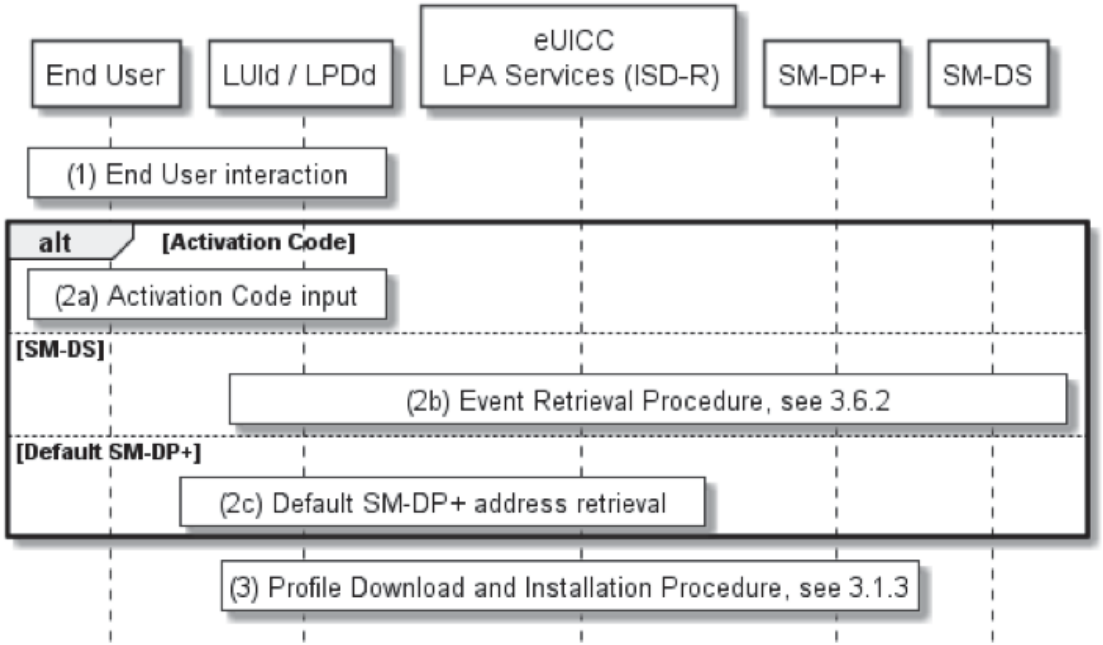


Figure 20: Add Profile

3.7 Remote Profile Management

The Operator initiates Remote Profile Management (RPM) procedure using the ES2+ interface.

RPM is executed by a Managing SM-DP+. A Profile MAY be configured to allow RPM by several Managing SM-DP+s. This specification assumes that a Managing SM-DP+ that prepares an RPM Package has full knowledge of the state of a Profile. How this state is synchronised among multiple Managing SM-DP+s, or procedures where a Managing SM-DP+ does not have full knowledge of the state of a Profile are out of the scope of this specification.

The LPA downloads an RPM Package using the ES9+ interface as described in section 3.7.2. An RPM Package MAY contain one or more RPM Commands.

Each RPM Command SHALL require Confirmation Request enforced by the LPA as described in section 3.7.2. The specific implementation of Confirmation Request by the LPA is out of scope of this specification.

Confirmation Request on multiple RPM Commands for consecutive operations MAY be combined to simplify the user experience and avoid repeated input steps for the End User. For instance, when executing two RPM Commands in an RPM Package, the Strong Confirmation for the first RPM Command and the Simple Confirmation for the second RPM Command MAY be combined. In the case of combined Confirmation Requests, it SHALL be clear to the End User what RPM Commands will be executed, and the highest Confirmation Level SHALL be obtained.

If End User accepts the execution of the RPM Package, the LPA transfers the RPM Package to the eUICC as described in section 3.7.3. The eUICC executes the RPM Command(s) contained in the RPM Package in the received order and generates the Load RPM Package Result specified in section 2.10.2.

Upon completing the execution of an RPM Package, the Operator receives the Load RPM Package Result. Based upon the outcome, the Operator can choose to initiate additional RPM operations. For instance, if a 'Contact PCMP' command resulted in a `noLprConfiguration` error, the Operator could request a new RPM Package containing both an 'Update Metadata' command with `pcmpAddress` and a 'Contact PCMP' command.

3.7.1 RPM Initiation

This procedure is used by Operator to issue an RPM Command(s).

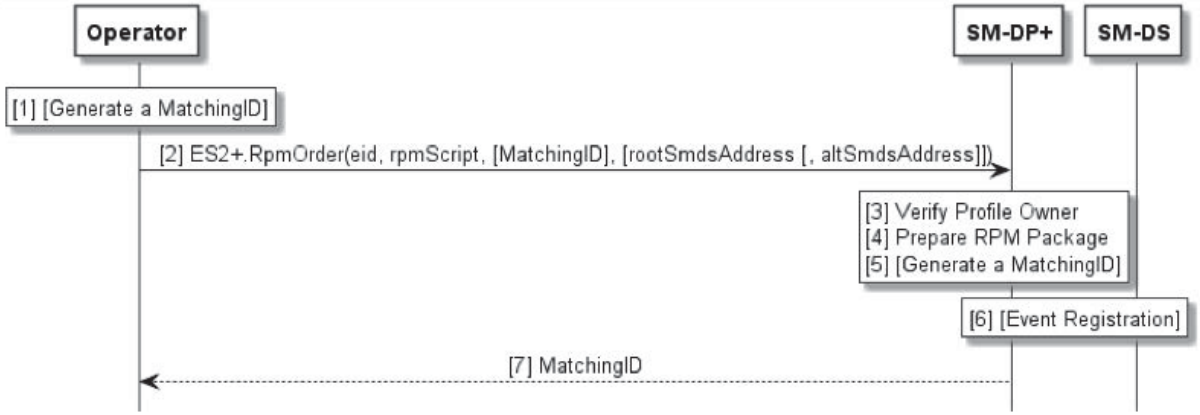


Figure 29a: RPM Initiation

Start Condition:

- The target eUICC has already installed a Profile from the Operator.
- The SM-DP+ is a Managing SM-DP+ of the target Profile.

3.7.2 RPM Download

This procedure is used by LPA to download an RPM Package and to get End User consent on RPM Execution.

The procedure applies for SEP and MEP. The following applies for Command Port:

	Command Port
MEP-A1/A2	0
MEP-B	>=0
SEP	Physical interface

All communication between the LPA and the eUICC in the RPM Download procedure SHALL use the Command Port.

3.7.3 RPM Execution

This procedure is used by LPA to transfer RPM Package to eUICC. The eUICC sequentially executes the RPM Command(s) contained in the RPM Package.

The procedure applies for SEP and MEP. The following applies for Command Port and Target Port:

	Command Port	Target Port
MEP-A1/A2	0	>0
MEP-B	As selected in the RPM Download procedure	>=0, identical to or different from Command Port
SEP	Physical interface	Physical interface

The Target Port is selected in the procedure depending on the presence of Disable or Enable commands.

3.8 Remote Management by the Operator

3.8.1 Metadata Update via ES6

This procedure is used by the Profile Owner to update Metadata of an enabled Profile.

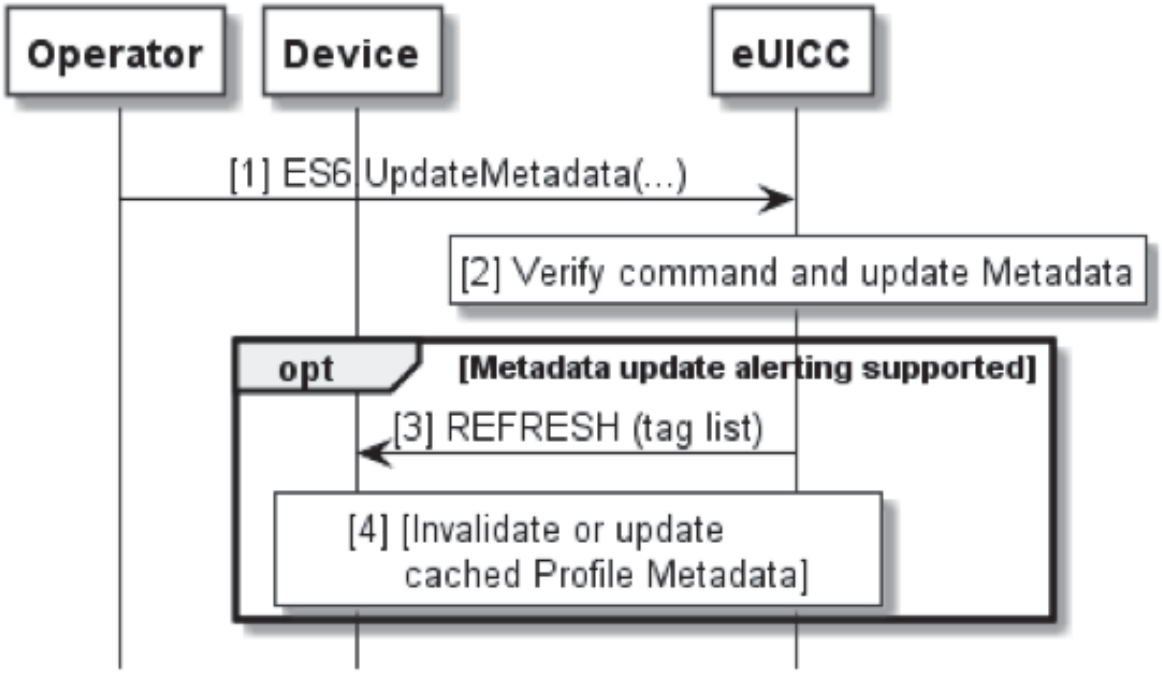


Figure 29j: Metadata Update

3.9 Profile Content Management

This procedure applies when a PCM session is triggered.

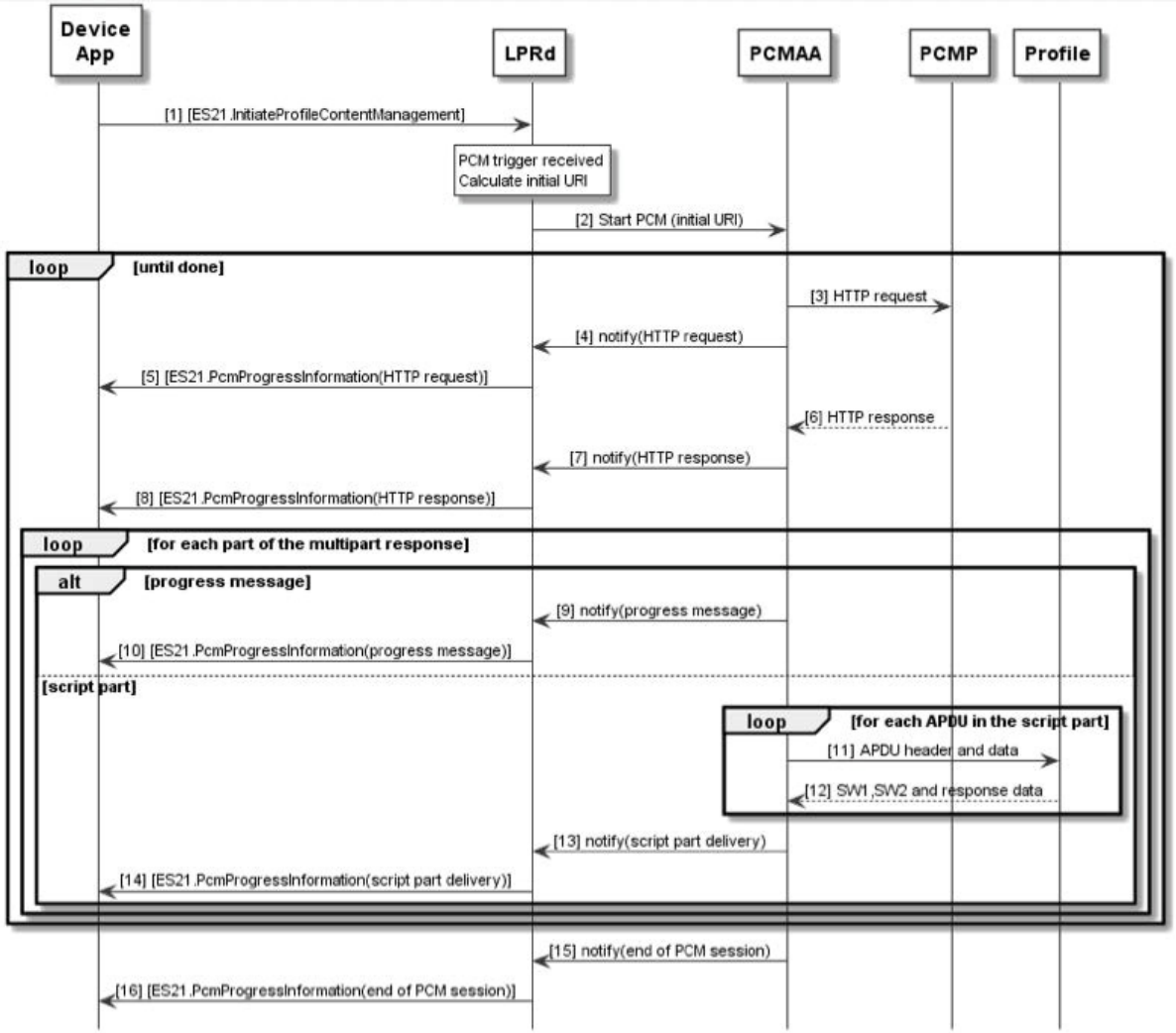


Figure 29I: Profile Content Management

	3.11 Device Change and Profile Recovery **3.11.1 Device Change** This procedure will allow the End User having a Profile in the old Device to add a Profile related to the same Subscription in the new Device. This procedure can further enable the downloaded Profile upon End User consent, which consequently MAY disable a currently Enabled Profile of the new Device (if any). Network connectivity is assumed.

3.1.6 Profile Lifecycle at SM-DP+

The previous sections provide detailed procedures associated with Remote Provisioning. Each Profile has state information on the SM-DP+ associated with it during the provisioning into an eUICC. The Profile lifecycle state can be one of the states listed in the following table.

Additional states and additional or customised ES2+ functions MAY be agreed between the Operator and the SM-DP+.

State Name	Description
Available	The Profile is available in the inventory of the SM-DP+.
Allocated	The Profile is reserved for downloading without being linked to an EID.
Linked	The Profile is reserved for downloading and is linked to an EID.
Confirmed	The Profile is reserved for downloading (linked or not linked to an EID) with Matching ID and Confirmation Code if required.
Released	The Profile is ready for download and installation after Network Configuration by the Operator (e.g.: HLR Registration).
Downloaded	The Bound Profile was delivered to the LPA.
Installed	The Profile was successfully installed on the eUICC.
Error	The Profile has not been installed because of one of the following error cases: - Confirmation Code Retry Limit exceeded - Download Retry Limit exceeded - End User Rejection - Permanent error during download and installation
Unavailable	The Profile cannot be reused anymore by the SM-DP+.

Table 6b: Profile State in the SM-DP+

2.9.3 Profile Policy Enabler

The Profile Policy Enabler on the eUICC has two functions:

- Verification that a Profile containing PPRs is authorised by the RAT.
- Enforcement of the PPRs of a Profile.

2.9 Profile Policy Management

Profile Policy Management provides mechanisms by which Profile Owners can enforce the conditions of use under which services are provided.

Profile Policy Management comprises three main elements:

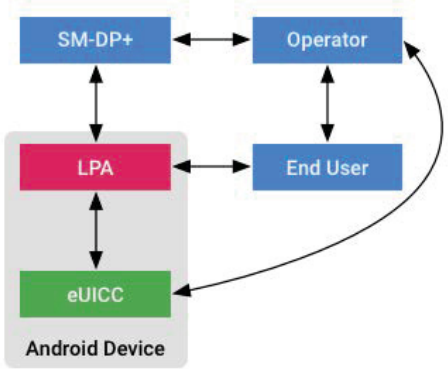
- Profile Policy Rules (PPR)
- Rules Authorisation Table (RAT)
- Profile Policy Enabler (PPE)

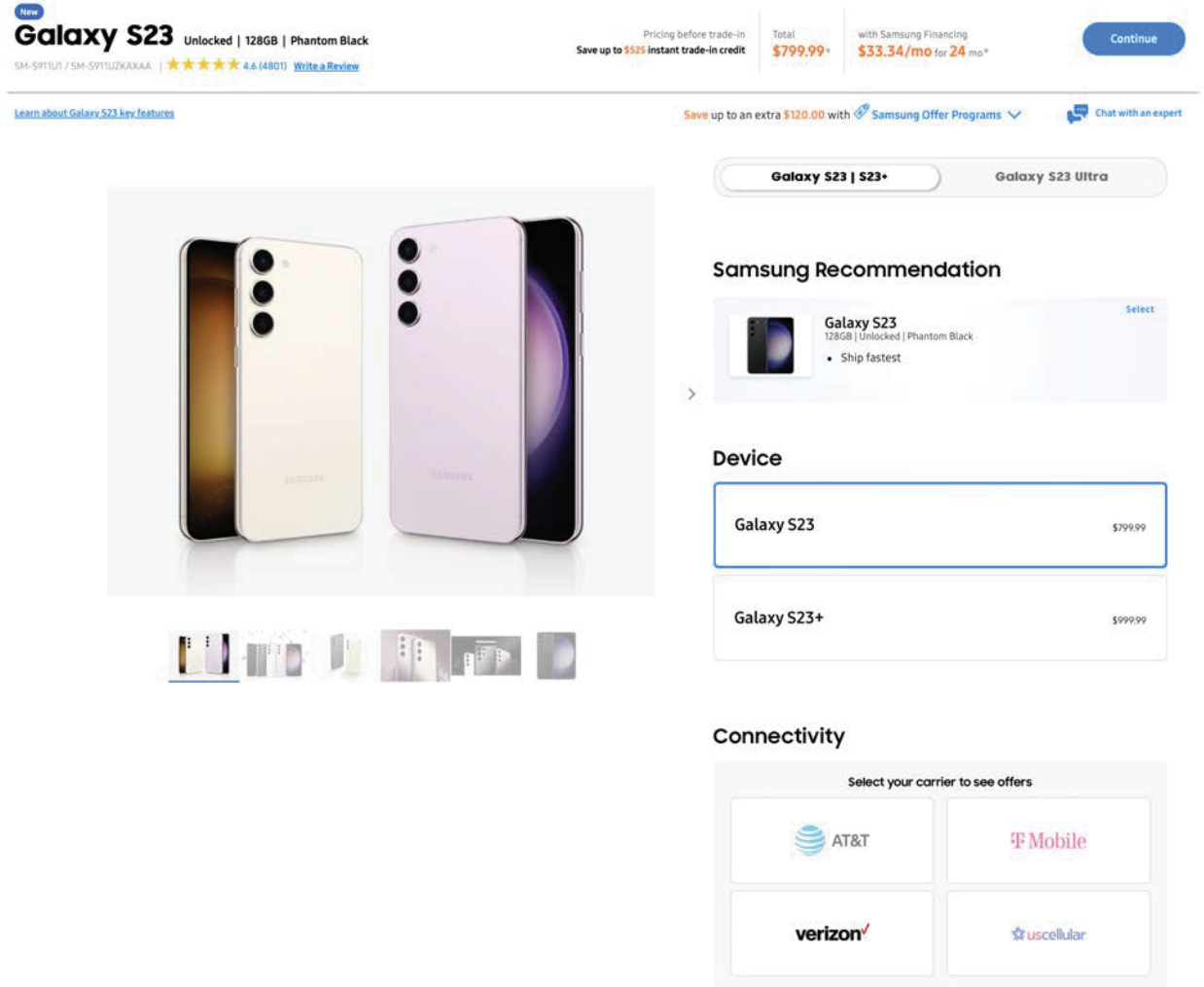
More details are provided in the next sub sections.

2.9.1 Profile Policy Rules

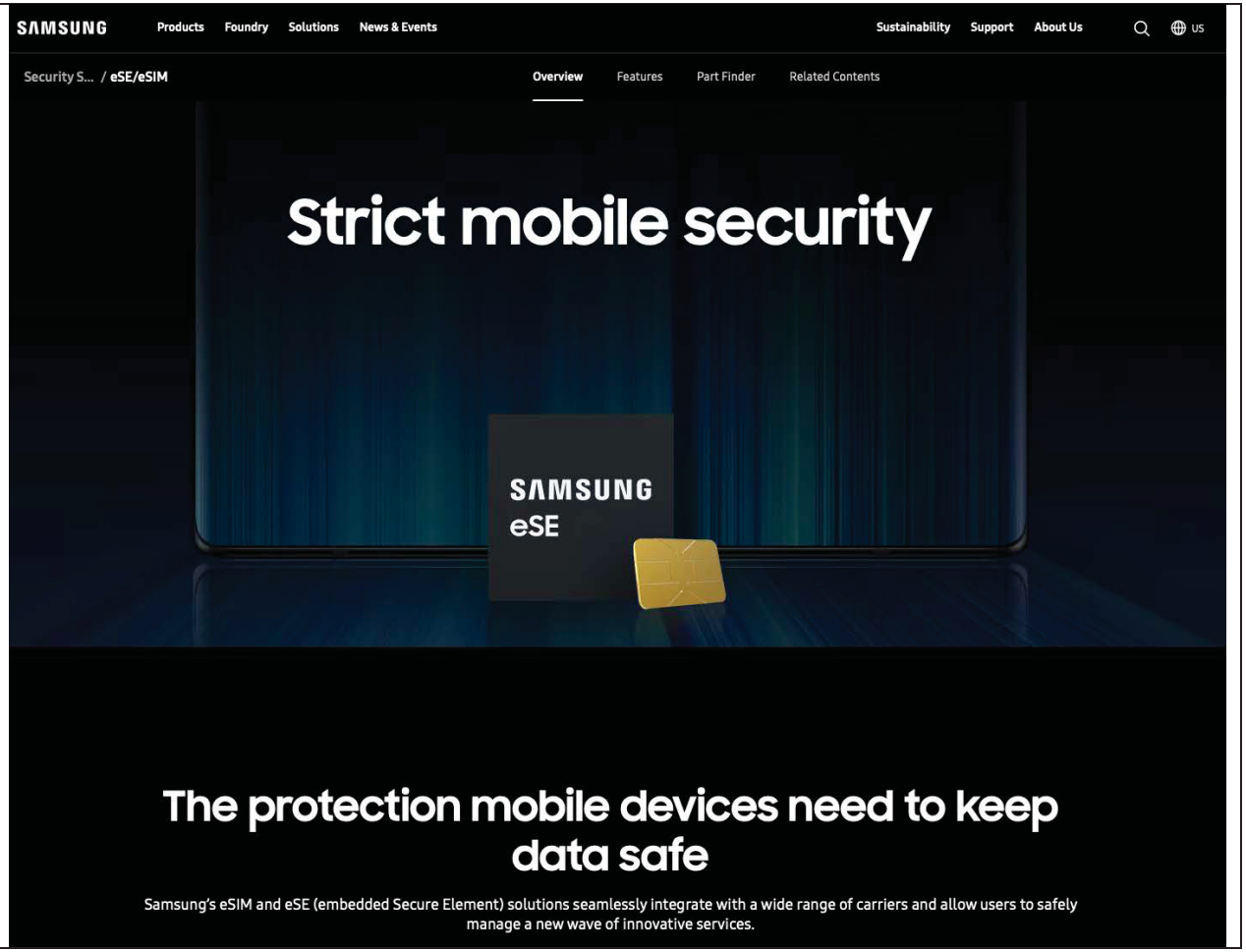
The Profile Policy Rules (PPRs) are defined by the Profile Owners and set by the SM-DP+ in the Profile Metadata. They are also accessible by the LPA for verification or display to the End User.

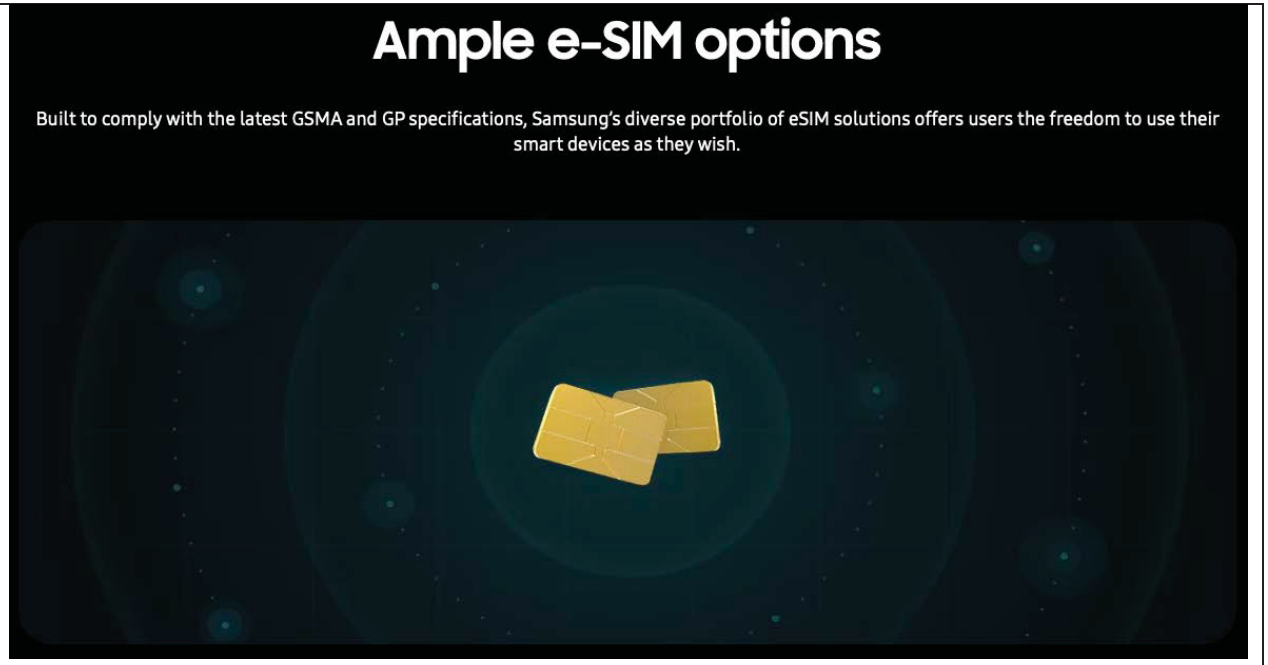
See also https://source.android.com/docs/core/connect/esim-euicc-api; https://source.android.com/docs/core/connect/esim-error-handling; https://source.android.com/docs/core/connect/esim-mep; https://source.android.com/docs/core/connect/esim-overview:

	Implement eSIM Embedded SIM (eSIM, or eUICC) technology allows mobile users to download a carrier profile and activate a carrier's service without having a physical SIM card. It's a global specification driven by the GSMA that enables remote SIM provisioning (RSP) of any mobile device. Starting with Android 9, the Android framework provides standard APIs for accessing eSIM and managing subscription profiles on the eSIM. These *eUICC APIs* enable third parties to develop their own carrier apps and local profile assistants (LPAs) on eSIM-enabled Android devices. The LPA is a standalone, system app that should be included in the Android build image. Management of the profiles on the eSIM is generally done by the LPA, as it serves as a bridge between the SM-DP+ (remote service that prepares, stores, and delivers profile packages to devices) and the eUICC chip. The LPA APK can optionally include a UI component, called the LPA UI or LUI, to provide a central place for the end user to manage all embedded subscription profiles. The Android framework automatically discovers and connects to the best available LPA, and routes all the eUICC operations through an LPA instance.  **Figure 1.** Simplified RSP architecture
[1d] a target credential; and	Samsung Galaxy phones and tablets comprise "a target credential." For example, Samsung Galaxy phones and tablets such as the Galaxy S23 each have unique identifiers corresponding to each device's eSim capability as well as eSim activation software including. *See, e.g.,* https://www.samsung.com/us/smartphones/galaxy-s23/buy/galaxy-s23-128gb-unlocked-sm-s911uzkaxaa/



; https://www.samsung.com/us/smartphones/galaxy-s23/specs/; https://semiconductor.samsung.com/us/security-solution/ese-esim/:


SAMSUNG
Products
Foundry
Solutions
News & Events
Sustainability
Support
About Us
US
Security S... / eSE/eSIM
Overview
Features
Part Finder
Related Contents
Strict mobile security
SAMSUNG
eSE
The protection mobile devices need to keep data safe
Samsung's eSIM and eSE (embedded Secure Element) solutions seamlessly integrate with a wide range of carriers and allow users to safely manage a new wave of innovative services.

	 ; https://www.samsung.com/us/support/answer/ANS00079039/:

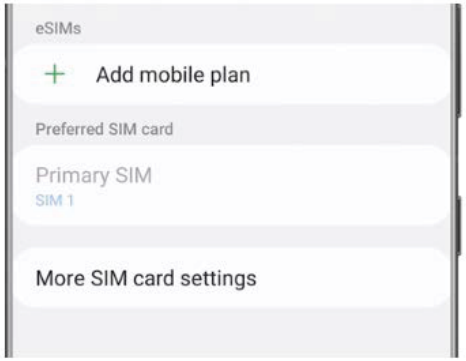
41

Using the eSIM

An eSIM is an embedded version of the physical SIM card on the phone. The eSIM provides connection to your carrier's network, however instead of inserting a card, you will activate it with your carrier account information. You can also use the eSIM alongside a physical SIM to add a second phone number or carrier to your phone.

Manage your SIM and eSIM

1. Open **Settings** and then tap **Connections**.
2. Tap **SIM card manager**.



From here you can tap the **switch** next to your physical SIM, or activated eSIM to enable or disable their connections. You can also tap **Primary SIM** to change the default connection for making calls, sending texts, and using data.

To start using the eSIM, you will need to follow your carrier's instructions.

- **T-Mobile activation**
- **Verizon activation**
- **AT&T activation**

; https://www.samsung.com/ph/support/mobile-devices/how-to-activate-esim-on-a-galaxy-device/:

	# How to activate eSIM on a Galaxy device Last Update date : Jul 24. 2023 **Your device includes an eSIM which functions as a SIM card. You can use the mobile network after activating the eSIM or installing a nano-SIM card. You can both activate the eSIM and install a nano-SIM card so you can have two phone numbers or service providers for a single device.** **In some areas, data transfer speeds may be slower if two SIM cards are inserted in the device than when one SIM card is inserted.** Before you try out the below recommendations as to your solution, be sure to check if your device's software is updated with the latest version. Please check how to update your mobile device's software in the following order. **Step 1.** Go to **Settings > Software update**. **Step 2.** Tap on **Download and install**. **Step 3**. Follow the on-screen instructions. ## How to add your mobile plan on your smartphone with eSIM To add your mobile network plan on an eSIM, you can scan a QR code that your carrier provided or install a pre-assigned plan automatically. Before adding your plan, make sure your Galaxy smartphone is connected to a wi-fi or mobile data network. **Note:** Device screenshots and menus may vary depending on the device model and software version. ; https://www.samsung.com/us/support/search/?query=galaxy+activate+esim&referrerPageUrl=https%3A%2F%2Fwww.samsung.com%2Fus%2Fsupport%2F&tabOrder=index.html%2Cfaqs%2Canswers%2Ctroubleshooting_guides%2Csupport_videos%2Cresources%2Ccommunity_posts%2Clinks%2Cproducts&facetFilters=%7B%7D&filters=%7B%7D&verticalUrl=faqs.html:

SAMSUNG Shop Mobile TV & Audio Appliances Computing Displays Accessories SmartThings Explore Support For Business

galaxy activate esim

All FAQs Answers Troubleshooting Guides Videos Resources Community Posts More

1 - 10 of 11

What is a hybrid eSIM card and how does it work?

What is an eSIM card and how does it differ from a physical SIM card?

An eSIM card, or embedded SIM card, is a digital SIM that is built directly into a device, eliminating the need for a physical SIM card. Instead of inserting a physical card, the device's eSIM connects to a cellular network remotely by downloading the necessary information from the network provider. This allows for greater flexibility, as users can switch between different carriers without physically changing the SIM card.

Important: Your network provider/mobile carrier (i.e. AT&T, Verizon, T-Mobile, etc.) is your best resource for carrier-specific information such as transferring your phone number from one sim card to another. Visit your providers online support content for more carrier-specific details:

- AT&T SIM card support content
- Verizon SIM card support content
- Xfinity/Comcast SIM card support content
- T-Mobile SIM card support content
- Charter Spectrum SIM card support content

Can I transfer my existing mobile number to an eSIM or hybrid eSIM card?

Can I use an eSIM or hybrid eSIM card in any device?

Can I activate a Windows AAOEM license on a virtual machine

What should I do if I encounter activation issues with a Windows AAOEM license?

How do I redeem a promotion for a subscription service?

What is a Windows AAOEM license?

After inserting a new SIM card my phone is asking for a PIN or Unlock Code

Help with Google Factory Reset Protection (FRP)

; https://www.att.com/search/?q=sim%20card&catField=Support; https://www.verizon.com/onesearch/search?q=sim%20card&ES=support&src=wireless; https://www.t-mobile.com/search?q=sim%20card&category=support.

Samsung Galaxy phones and tablets comply with the GSMA eSim specification. https://semiconductor.samsung.com/us/security-solution/ese-esim/; https://research.samsung.com/blog/eSIM-and-the-Latest-eSIM-V3-0-Release.

https://research.samsung.com/blog/eSIM-and-the-Latest-eSIM-V3-0-Release:

The procedure of remotely provisioning a Profile into an eSIM is called as "Remote SIM Provisioning" (RSP) in the GSMA eSIM specifications, and Figure 2 illustrates the overall RSP architecture.

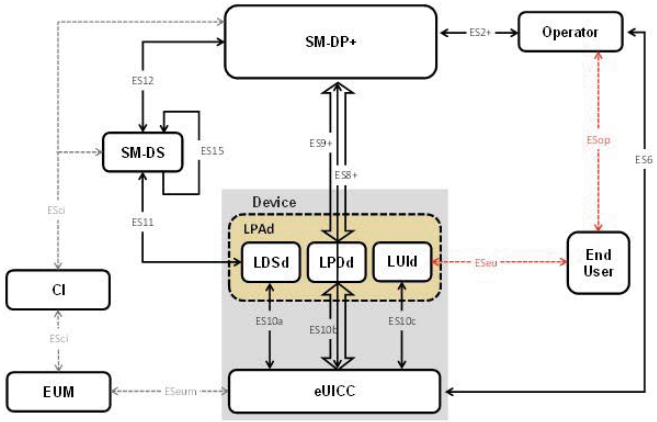


Figure 2. Overall RSP architecture [1]

https://www.gsma.com/esim/wp-content/uploads/2022/10/SGP.22-v3.0-1.pdf:

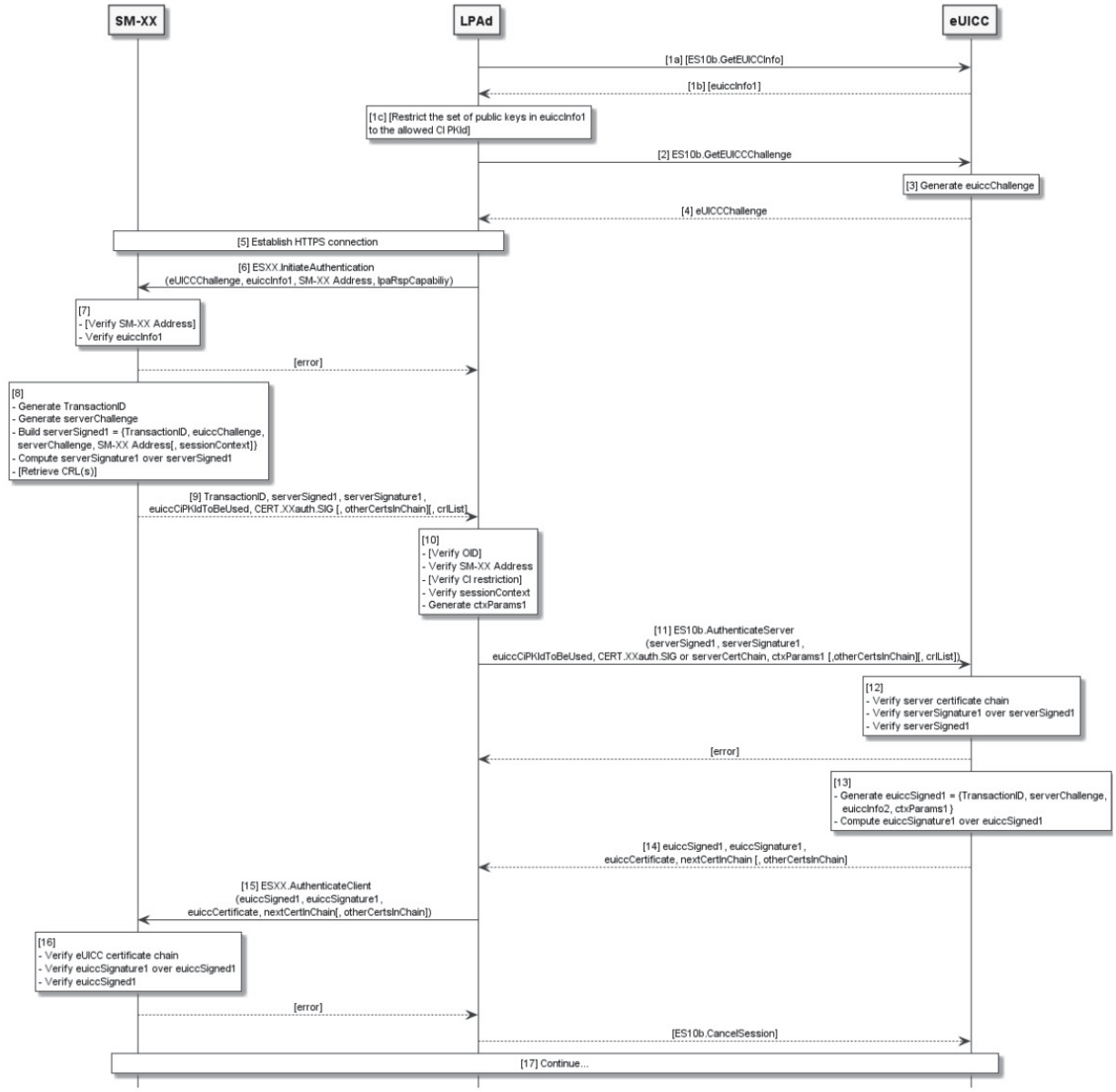


Figure 8a: Common Mutual Authentication Procedure

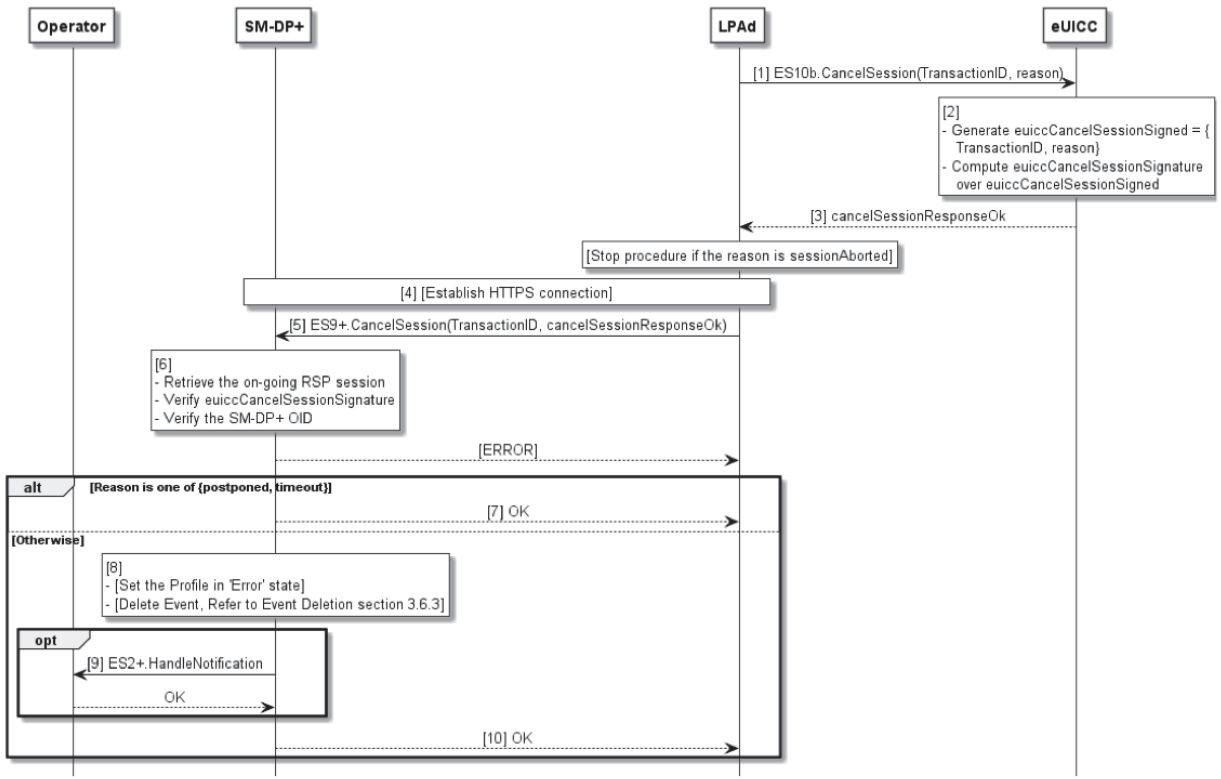


Figure 8b: Common Cancel Session Procedure

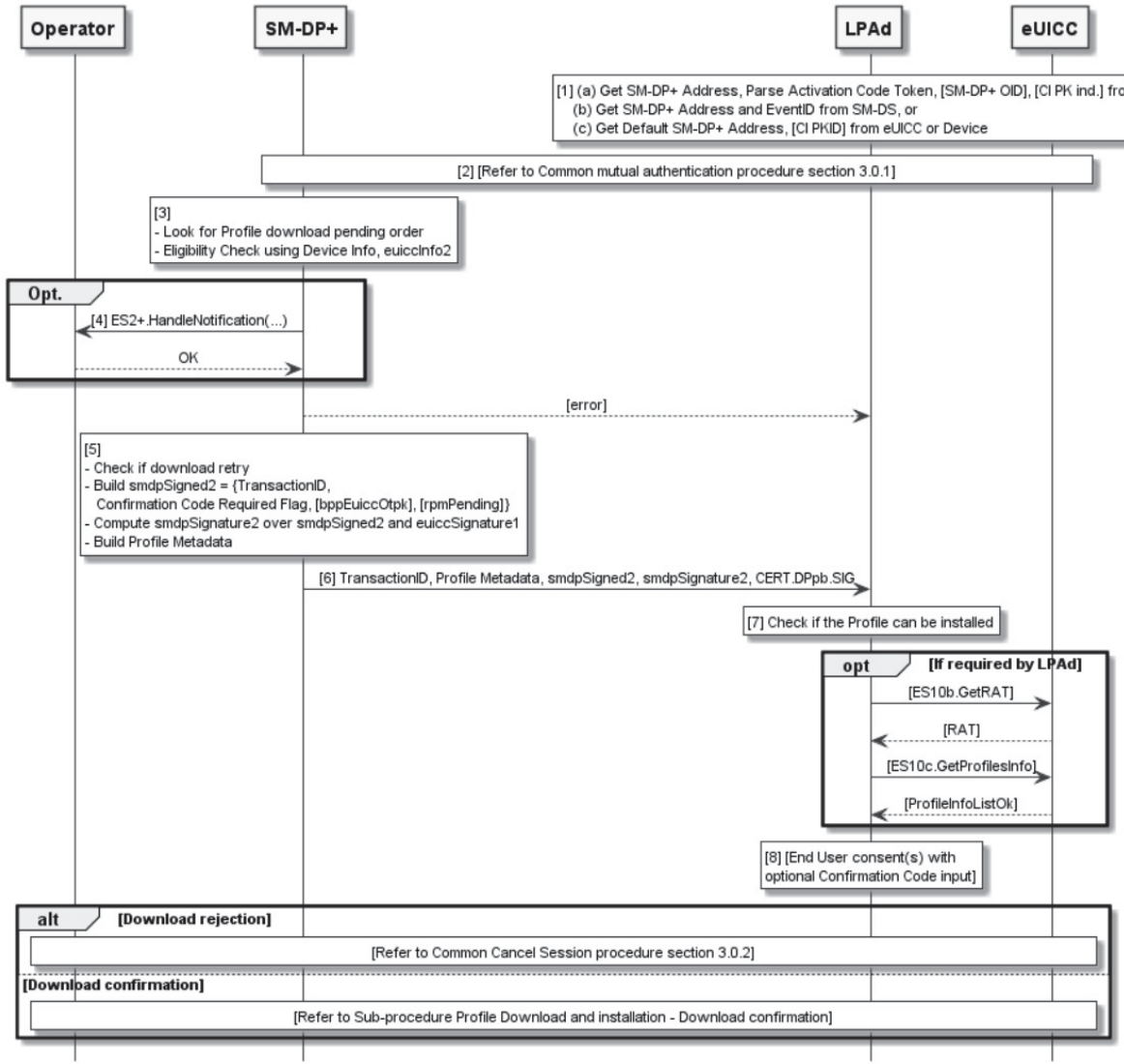


Figure 11: Profile Download and Installation

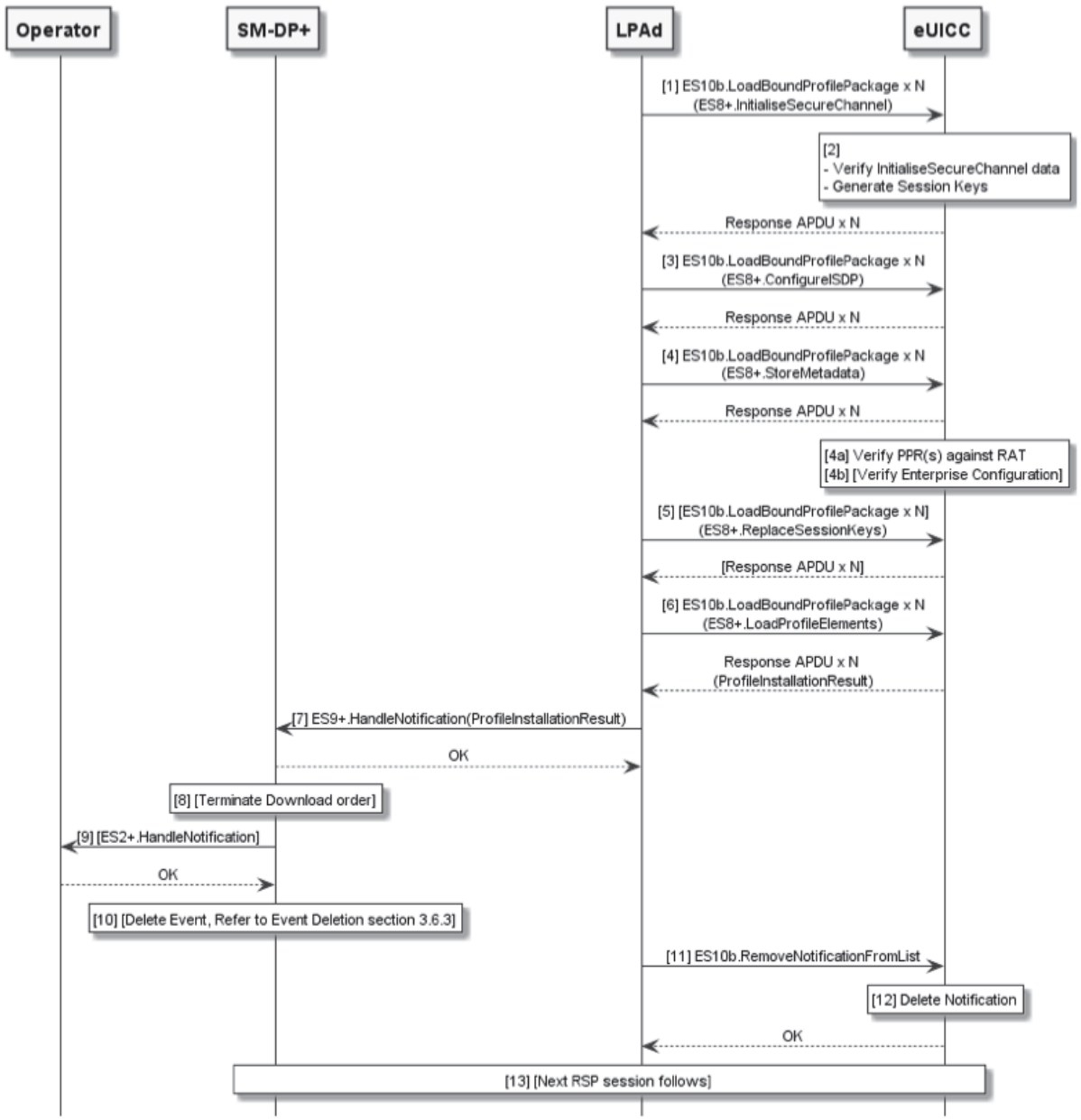


Figure 14: Sub-procedure Profile Installation

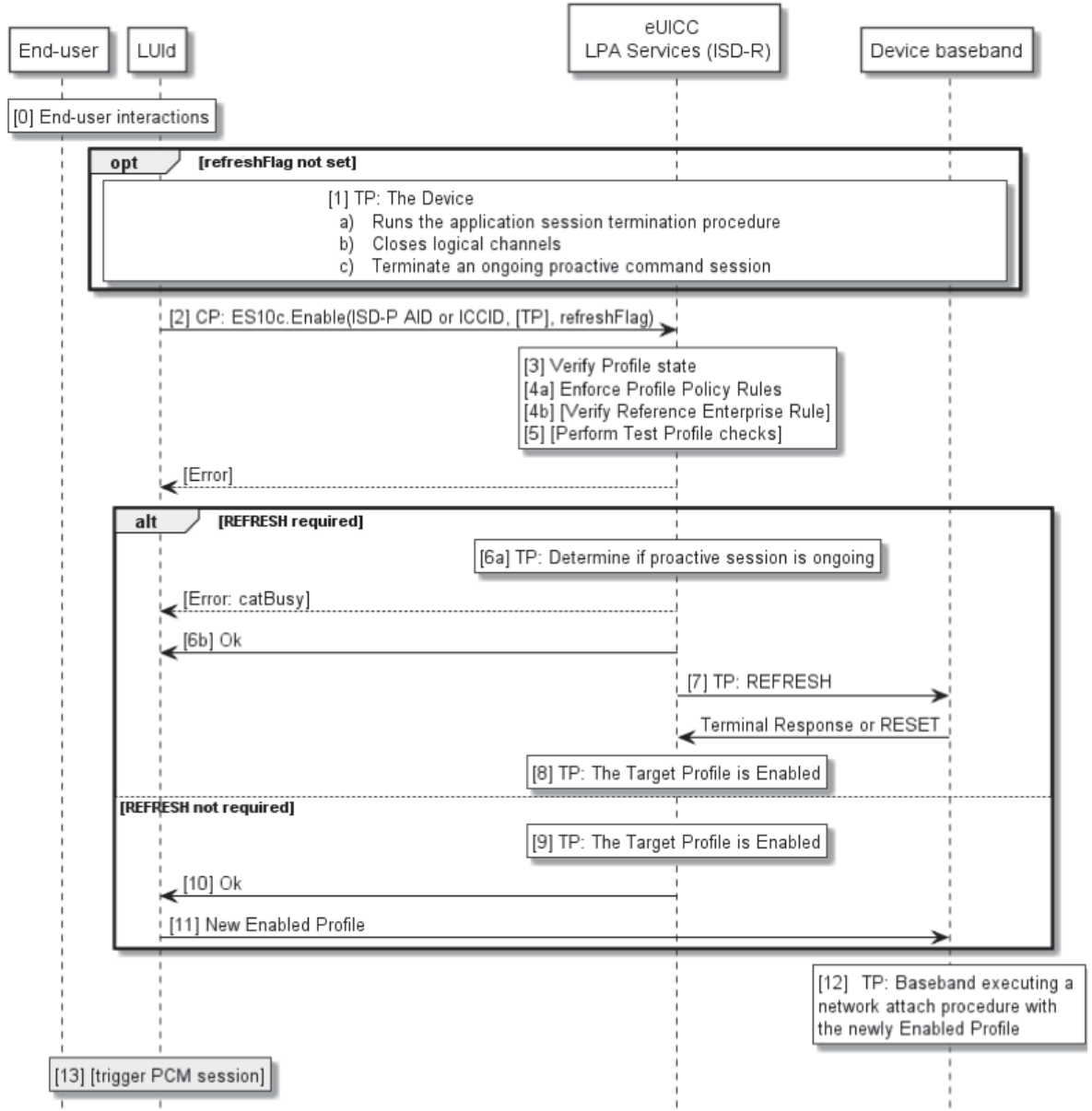


Figure 16: Enable Profile

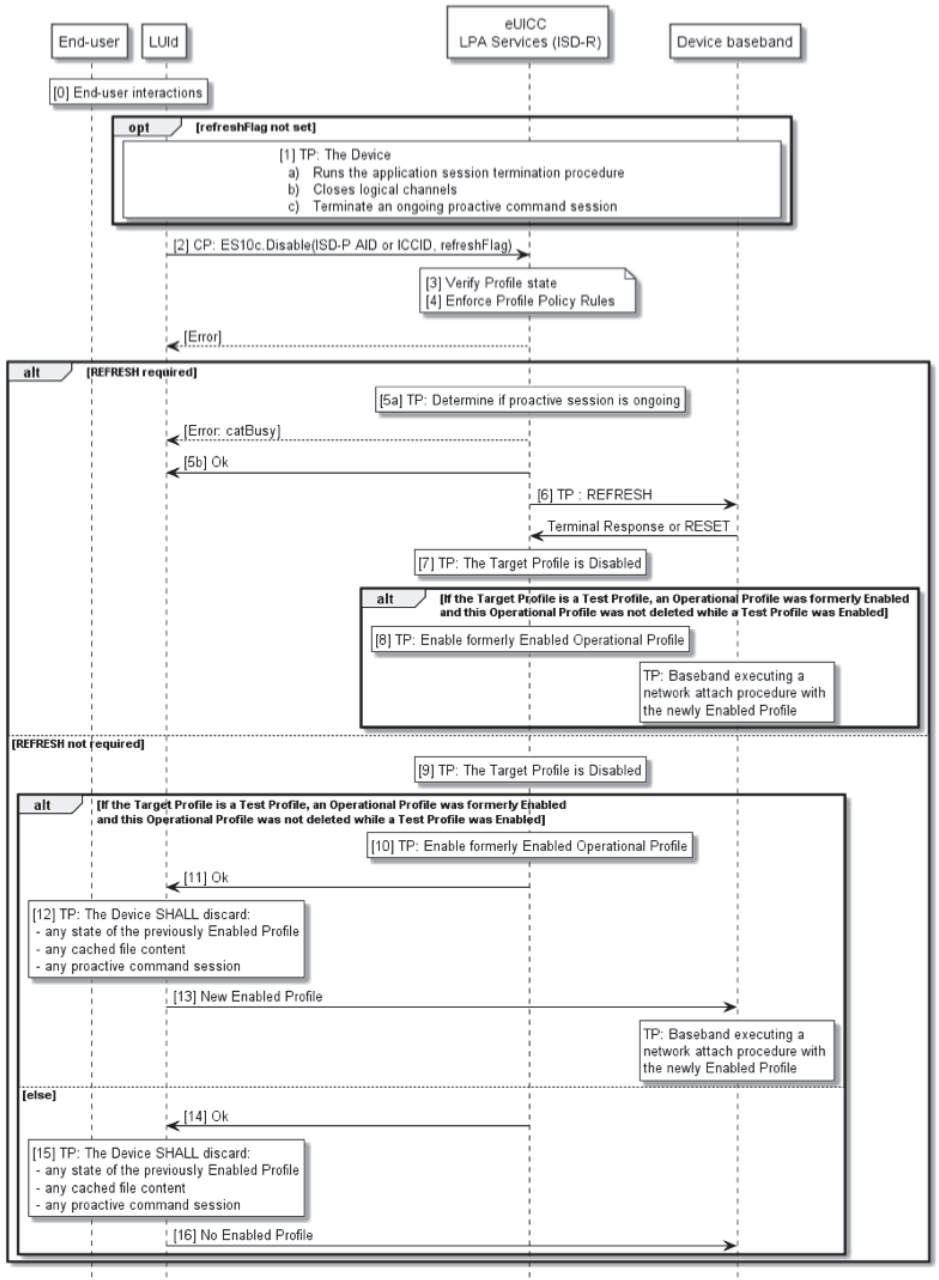


Figure 17: Disable Profile

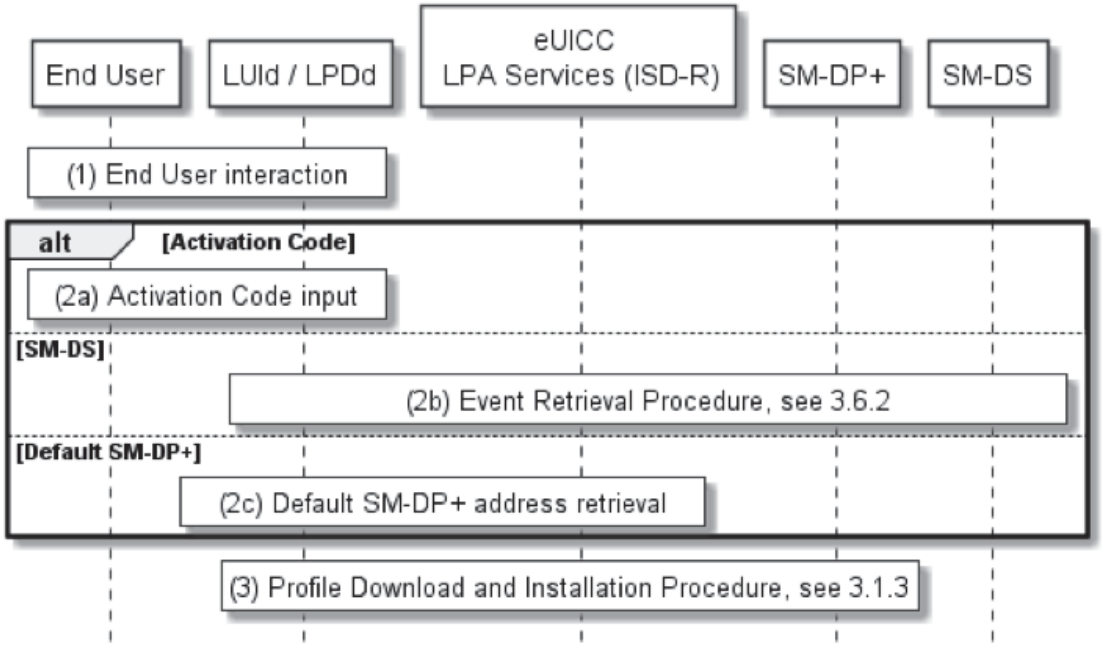


Figure 20: Add Profile

3.7 Remote Profile Management

The Operator initiates Remote Profile Management (RPM) procedure using the ES2+ interface.

RPM is executed by a Managing SM-DP+. A Profile MAY be configured to allow RPM by several Managing SM-DP+s. This specification assumes that a Managing SM-DP+ that prepares an RPM Package has full knowledge of the state of a Profile. How this state is synchronised among multiple Managing SM-DP+s, or procedures where a Managing SM-DP+ does not have full knowledge of the state of a Profile are out of the scope of this specification.

The LPA downloads an RPM Package using the ES9+ interface as described in section 3.7.2. An RPM Package MAY contain one or more RPM Commands.

Each RPM Command SHALL require Confirmation Request enforced by the LPA as described in section 3.7.2. The specific implementation of Confirmation Request by the LPA is out of scope of this specification.

Confirmation Request on multiple RPM Commands for consecutive operations MAY be combined to simplify the user experience and avoid repeated input steps for the End User. For instance, when executing two RPM Commands in an RPM Package, the Strong Confirmation for the first RPM Command and the Simple Confirmation for the second RPM Command MAY be combined. In the case of combined Confirmation Requests, it SHALL be clear to the End User what RPM Commands will be executed, and the highest Confirmation Level SHALL be obtained.

If End User accepts the execution of the RPM Package, the LPA transfers the RPM Package to the eUICC as described in section 3.7.3. The eUICC executes the RPM Command(s) contained in the RPM Package in the received order and generates the Load RPM Package Result specified in section 2.10.2.

Upon completing the execution of an RPM Package, the Operator receives the Load RPM Package Result. Based upon the outcome, the Operator can choose to initiate additional RPM operations. For instance, if a 'Contact PCMP' command resulted in a `noLprConfiguration` error, the Operator could request a new RPM Package containing both an 'Update Metadata' command with `pcmpAddress` and a 'Contact PCMP' command.

3.7.1 RPM Initiation

This procedure is used by Operator to issue an RPM Command(s).

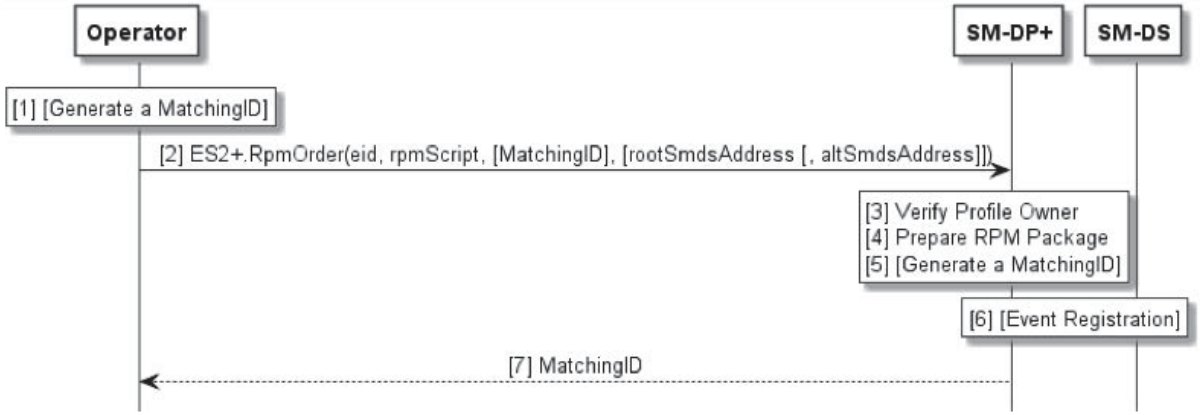


Figure 29a: RPM Initiation

Start Condition:

- The target eUICC has already installed a Profile from the Operator.
- The SM-DP+ is a Managing SM-DP+ of the target Profile.

3.7.2 RPM Download

This procedure is used by LPA to download an RPM Package and to get End User consent on RPM Execution.

The procedure applies for SEP and MEP. The following applies for Command Port:

	Command Port
MEP-A1/A2	0
MEP-B	>=0
SEP	Physical interface

All communication between the LPA and the eUICC in the RPM Download procedure SHALL use the Command Port.

3.7.3 RPM Execution

This procedure is used by LPA to transfer RPM Package to eUICC. The eUICC sequentially executes the RPM Command(s) contained in the RPM Package.

The procedure applies for SEP and MEP. The following applies for Command Port and Target Port:

	Command Port	Target Port
MEP-A1/A2	0	>0
MEP-B	As selected in the RPM Download procedure	>=0, identical to or different from Command Port
SEP	Physical interface	Physical interface

The Target Port is selected in the procedure depending on the presence of Disable or Enable commands.

3.8 Remote Management by the Operator

3.8.1 Metadata Update via ES6

This procedure is used by the Profile Owner to update Metadata of an enabled Profile.

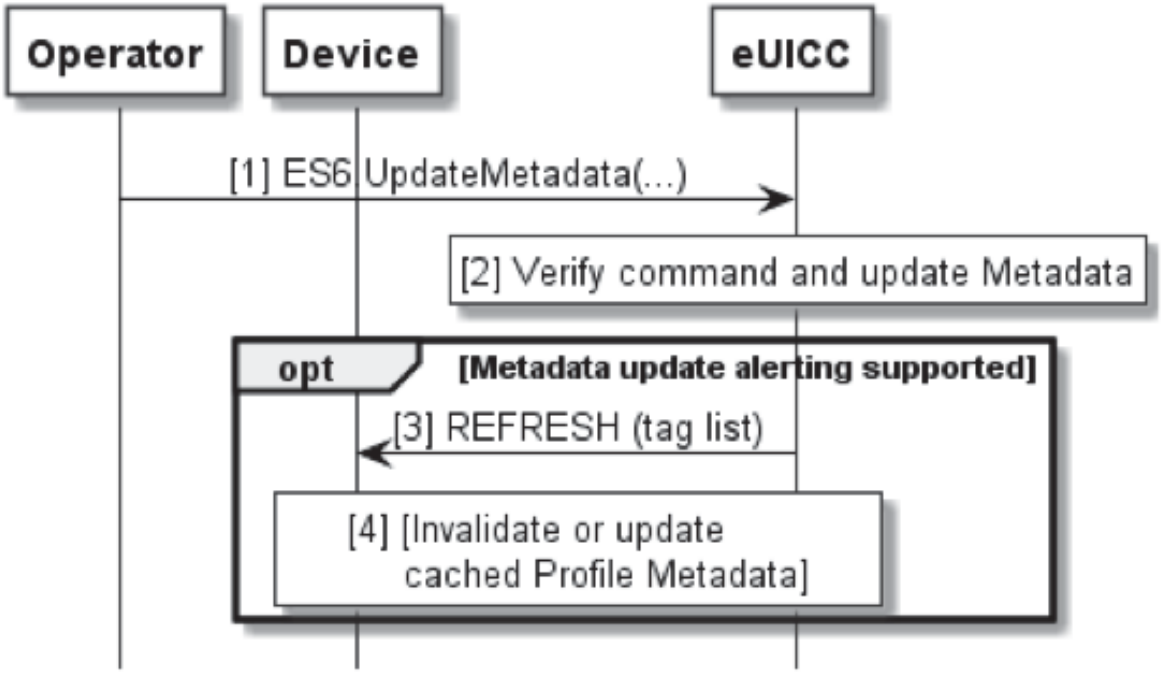


Figure 29j: Metadata Update

3.9 Profile Content Management

This procedure applies when a PCM session is triggered.

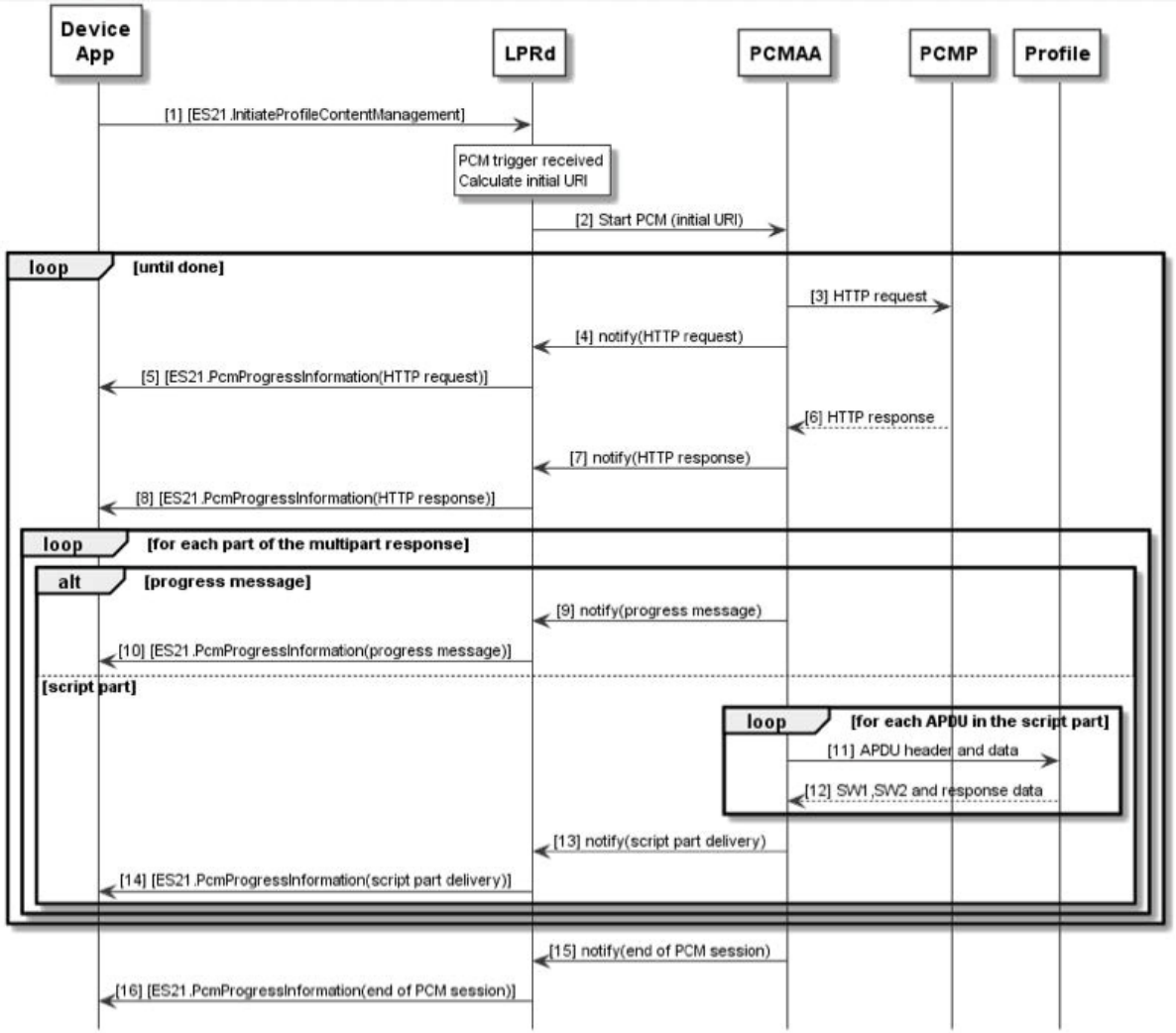


Figure 29I: Profile Content Management

	3.11 Device Change and Profile Recovery **3.11.1 Device Change** This procedure will allow the End User having a Profile in the old Device to add a Profile related to the same Subscription in the new Device. This procedure can further enable the downloaded Profile upon End User consent, which consequently MAY disable a currently Enabled Profile of the new Device (if any). Network connectivity is assumed.

3.1.6 Profile Lifecycle at SM-DP+

The previous sections provide detailed procedures associated with Remote Provisioning. Each Profile has state information on the SM-DP+ associated with it during the provisioning into an eUICC. The Profile lifecycle state can be one of the states listed in the following table.

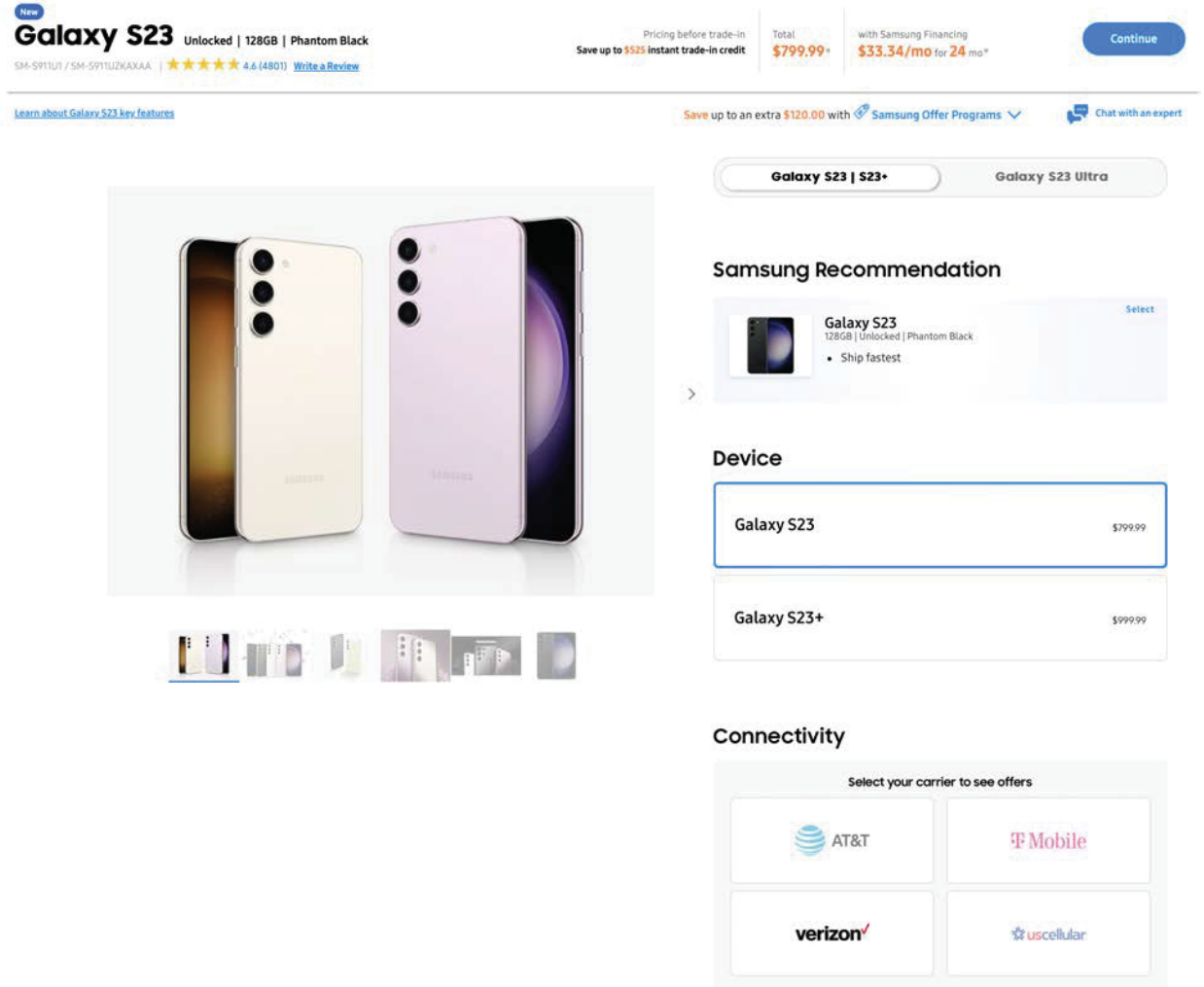
Additional states and additional or customised ES2+ functions MAY be agreed between the Operator and the SM-DP+.

State Name	Description
Available	The Profile is available in the inventory of the SM-DP+.
Allocated	The Profile is reserved for downloading without being linked to an EID.
Linked	The Profile is reserved for downloading and is linked to an EID.
Confirmed	The Profile is reserved for downloading (linked or not linked to an EID) with Matching ID and Confirmation Code if required.
Released	The Profile is ready for download and installation after Network Configuration by the Operator (e.g.: HLR Registration).
Downloaded	The Bound Profile was delivered to the LPA.
Installed	The Profile was successfully installed on the eUICC.
Error	The Profile has not been installed because of one of the following error cases: - Confirmation Code Retry Limit exceeded - Download Retry Limit exceeded - End User Rejection - Permanent error during download and installation
Unavailable	The Profile cannot be reused anymore by the SM-DP+.

Table 6b: Profile State in the SM-DP+

	2.4.4 ISD-P The ISD-P is the on-card representative of the SM-DP+ and is a secure container (Security Domain) for the hosting of a Profile. The ISD-P is used for the Profile download and installation in collaboration with the Profile Package Interpreter for the decoding/interpretation of the received Profile Package. An ISD-P hosts a unique Profile. No component outside the ISD-P SHALL have visibility or access to any Profile Component with the exception of the ISD-R, which SHALL have access to Profile Metadata. A Profile Component SHALL NOT have any visibility of, or access to, components outside its ISD-P. An ISD-P SHALL NOT have any visibility of, or access to, any other ISD-P. Deletion of a Profile SHALL remove the containing ISD-P and all Profile Components of the Profile.

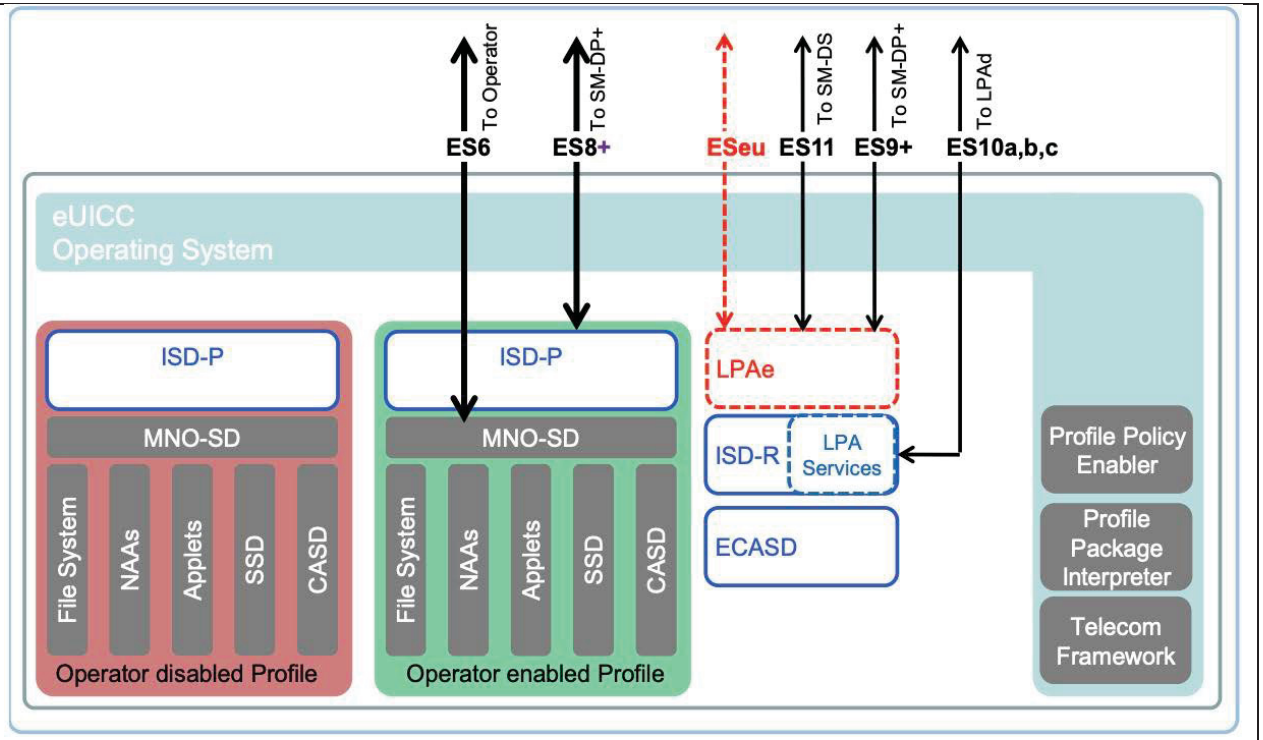
	2.9.3 Profile Policy Enabler The Profile Policy Enabler on the eUICC has two functions: • Verification that a Profile containing PPRs is authorised by the RAT. • Enforcement of the PPRs of a Profile. **2.9 Profile Policy Management** Profile Policy Management provides mechanisms by which Profile Owners can enforce the conditions of use under which services are provided. Profile Policy Management comprises three main elements: • Profile Policy Rules (PPR) • Rules Authorisation Table (RAT) • Profile Policy Enabler (PPE) More details are provided in the next sub sections. **2.9.1 Profile Policy Rules** The Profile Policy Rules (PPRs) are defined by the Profile Owners and set by the SM-DP+ in the Profile Metadata. They are also accessible by the LPA for verification or display to the End User. *See also* https://source.android.com/docs/core/connect/esim-euicc-api; https://source.android.com/docs/core/connect/esim-error-handling; https://source.android.com/docs/core/connect/esim-mep; https://source.android.com/docs/core/connect/esim-overview.
[1e] one or more processors configured to execute one or more machine-executable instructions that, when executed by the one or more processors, cause the one or more processors to:	Samsung Galaxy phones and tablets comprise "one or more processors configured to execute one or more machine-executable instructions that, when executed by the one or more processors, cause the one or more processors to." For example, the Galaxy S23 comprises at least a Snapdragon and/or Octa-Core processor. *See, e.g.,* https://www.samsung.com/us/smartphones/galaxy-s23/buy/galaxy-s23-128gb-unlocked-sm-s911uzkaxaa/



; https://www.samsung.com/us/smartphones/galaxy-s23/specs/:

	Galaxy S23 Ultra	Galaxy S23+	Galaxy S23
	Processor		
	Super fast processing	Super fast processing	Super fast processing
	Snapdragon® 8 Gen 2	Snapdragon® 8 Gen 2	Snapdragon® 8 Gen 2
	Octa-Core	Octa-Core	Octa-Core

https://www.gsma.com/esim/wp-content/uploads/2022/10/SGP.22-v3.0-1.pdf:

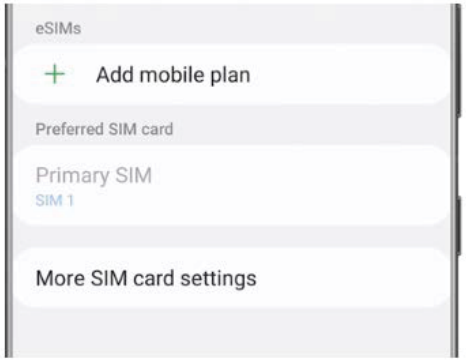
	 https://www.samsung.com/us/support/answer/ANS00079039/:

Using the eSIM

An eSIM is an embedded version of the physical SIM card on the phone. The eSIM provides connection to your carrier's network, however instead of inserting a card, you will activate it with your carrier account information. You can also use the eSIM alongside a physical SIM to add a second phone number or carrier to your phone.

Manage your SIM and eSIM

1. Open **Settings** and then tap **Connections**.
2. Tap **SIM card manager**.



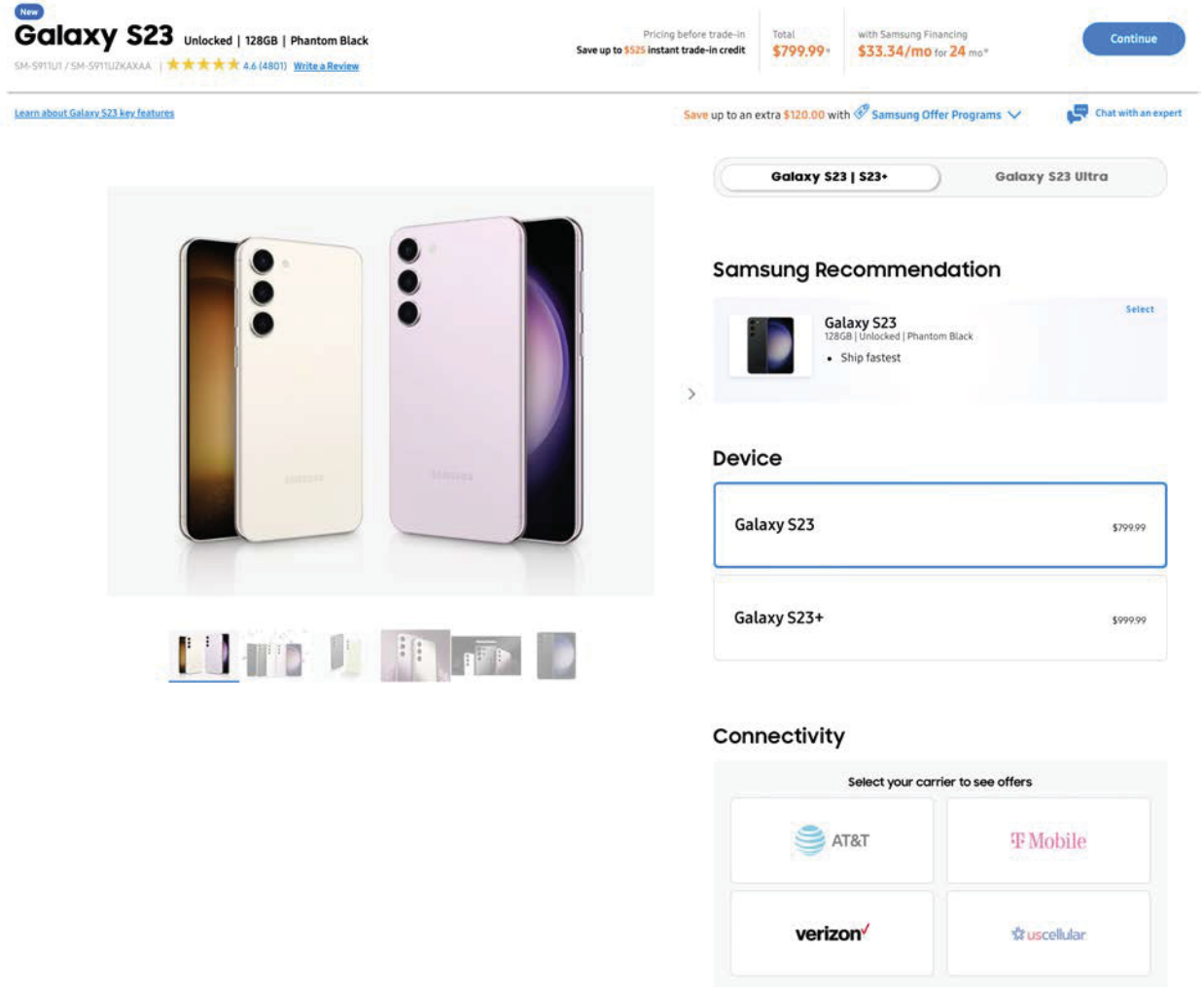
From here you can tap the **switch** next to your physical SIM, or activated eSIM to enable or disable their connections. You can also tap **Primary SIM** to change the default connection for making calls, sending texts, and using data.

To start using the eSIM, you will need to follow your carrier's instructions.

- **T-Mobile activation**
- **Verizon activation**
- **AT&T activation**

; https://www.samsung.com/ph/support/mobile-devices/how-to-activate-esim-on-a-galaxy-device/:

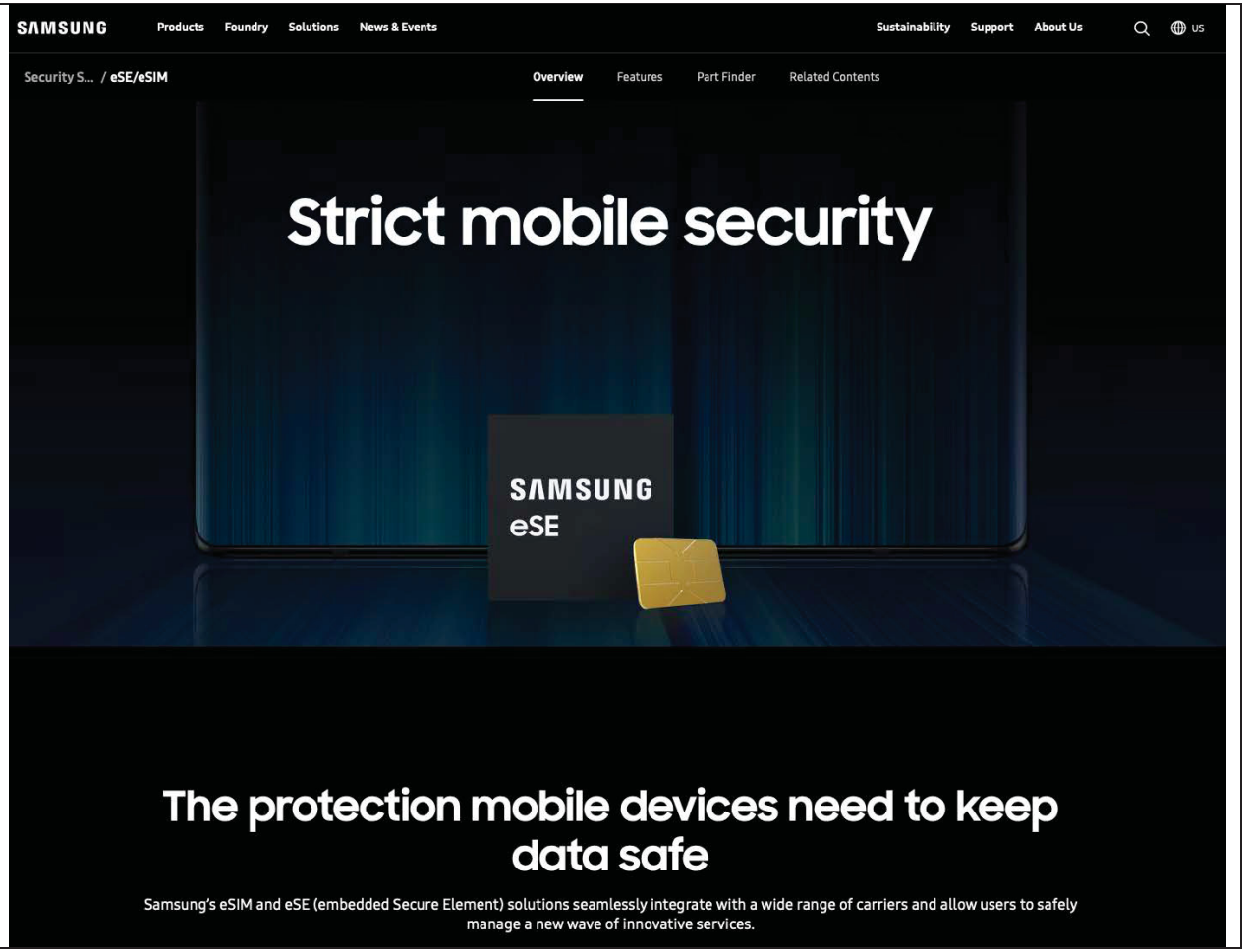
	How to activate eSIM on a Galaxy device Last Update date : Jul 24. 2023 **Your device includes an eSIM which functions as a SIM card. You can use the mobile network after activating the eSIM or installing a nano-SIM card. You can both activate the eSIM and install a nano-SIM card so you can have two phone numbers or service providers for a single device.** **In some areas, data transfer speeds may be slower if two SIM cards are inserted in the device than when one SIM card is inserted.** Before you try out the below recommendations as to your solution, be sure to check if your device's software is updated with the latest version. Please check how to update your mobile device's software in the following order. **Step 1.** Go to **Settings > Software update**. **Step 2.** Tap on **Download and install**. **Step 3**. Follow the on-screen instructions. **How to add your mobile plan on your smartphone with eSIM** To add your mobile network plan on an eSIM, you can scan a QR code that your carrier provided or install a pre-assigned plan automatically. Before adding your plan, make sure your Galaxy smartphone is connected to a wi-fi or mobile data network. **Note:** Device screenshots and menus may vary depending on the device model and software version. *See also* https://source.android.com/docs/core/connect/esim-euicc-api; https://source.android.com/docs/core/connect/esim-error-handling; https://source.android.com/docs/core/connect/esim-mep; https://source.android.com/docs/core/connect/esim-overview.
[1f] obtain, through the user interface, an indication of a user request to replace a particular credential of the one or more credentials with the target credential,	Samsung Galaxy phones and tablets "obtain, through the user interface, an indication of a user request to replace a particular credential of the one or more credentials with the target credential." *See, e.g.,* https://www.samsung.com/us/smartphones/galaxy-s23/buy/galaxy-s23-128gb-unlocked-sm-s911uzkaxaa/

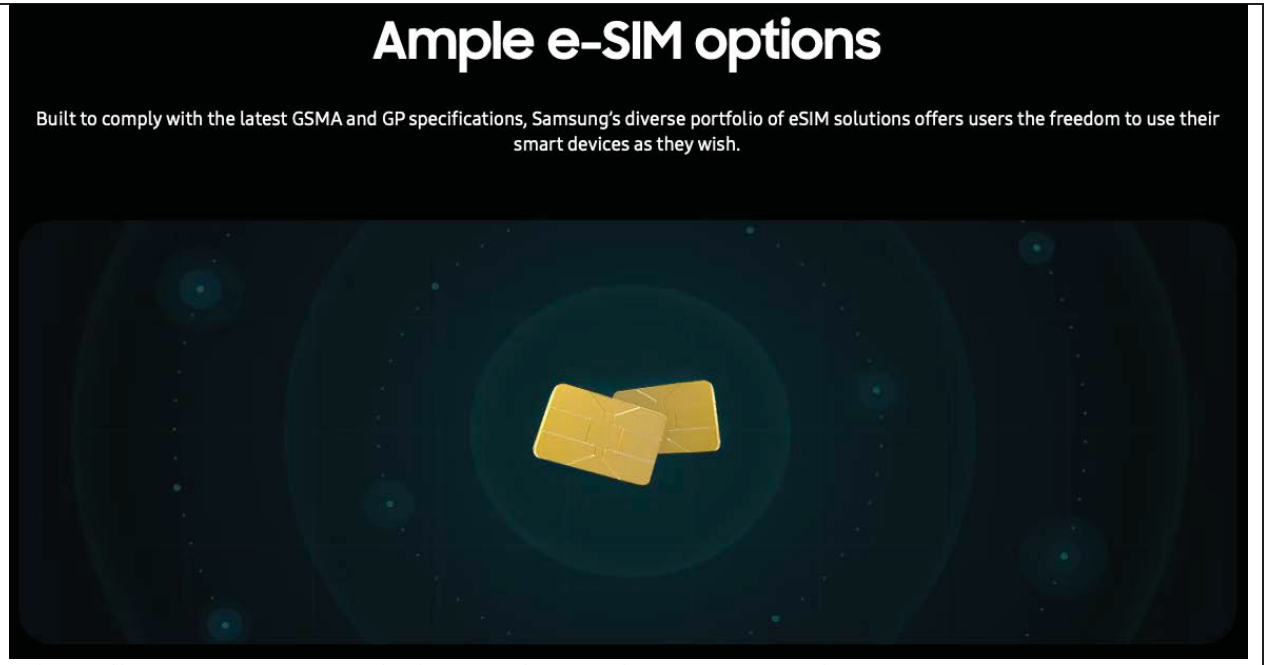


; https://www.samsung.com/us/smartphones/galaxy-s23/specs/:

	Galaxy S23 Ultra	Galaxy S23+	Galaxy S23
Storage			
	-	-	128GB
	256GB	256GB	256GB
	512GB	512GB	-
	1TB	-	-

; https://semiconductor.samsung.com/us/security-solution/ese-esim/:


SAMSUNG
Products
Foundry
Solutions
News & Events
Sustainability
Support
About Us
US
Security S... / eSE/eSIM
Overview
Features
Part Finder
Related Contents
Strict mobile security
SAMSUNG
eSE
The protection mobile devices need to keep data safe
Samsung's eSIM and eSE (embedded Secure Element) solutions seamlessly integrate with a wide range of carriers and allow users to safely manage a new wave of innovative services.

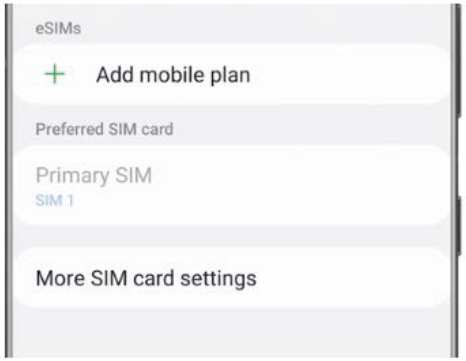
	 ; https://www.samsung.com/us/support/answer/ANS00079039/:

Using the eSIM

An eSIM is an embedded version of the physical SIM card on the phone. The eSIM provides connection to your carrier's network, however instead of inserting a card, you will activate it with your carrier account information. You can also use the eSIM alongside a physical SIM to add a second phone number or carrier to your phone.

Manage your SIM and eSIM

1. Open **Settings** and then tap **Connections**.
2. Tap **SIM card manager**.



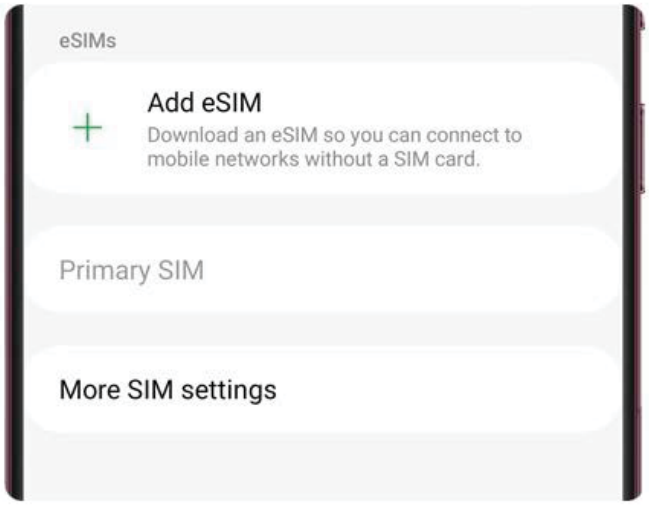
From here you can tap the **switch** next to your physical SIM, or activated eSIM to enable or disable their connections. You can also tap **Primary SIM** to change the default connection for making calls, sending texts, and using data.

To start using the eSIM, you will need to follow your carrier's instructions.

- **T-Mobile activation**
- **Verizon activation**
- **AT&T activation**

; https://www.samsung.com/ph/support/mobile-devices/how-to-activate-esim-on-a-galaxy-device/:

	# How to activate eSIM on a Galaxy device Last Update date : Jul 24. 2023 **Your device includes an eSIM which functions as a SIM card. You can use the mobile network after activating the eSIM or installing a nano-SIM card. You can both activate the eSIM and install a nano-SIM card so you can have two phone numbers or service providers for a single device.** **In some areas, data transfer speeds may be slower if two SIM cards are inserted in the device than when one SIM card is inserted.** Before you try out the below recommendations as to your solution, be sure to check if your device's software is updated with the latest version. Please check how to update your mobile device's software in the following order. **Step 1.** Go to **Settings > Software update**. **Step 2.** Tap on **Download and install**. **Step 3**. Follow the on-screen instructions. ## How to add your mobile plan on your smartphone with eSIM To add your mobile network plan on an eSIM, you can scan a QR code that your carrier provided or install a pre-assigned plan automatically. Before adding your plan, make sure your Galaxy smartphone is connected to a wi-fi or mobile data network. **Note:** Device screenshots and menus may vary depending on the device model and software version. ; https://www.samsung.com/us/support/answer/ANS10001619/ (referring to carrier's instructions for using eSIM):

	An eSIM is an embedded version of the physical SIM card on the device. The eSIM provides connection to your carrier's network, however instead of inserting a card, you will activate it with your carrier account information. You can also use the eSIM alongside a physical SIM to add a second phone number or carrier to your device. **1** Navigate to and open **Settings**, and then tap **Connections**. **2** Tap **SIM manager**. From here, you can tap the **switch** next to your physical SIM or activated eSIM to enable or disable their connections. You can also tap **Primary SIM** to change the default connection for making calls, sending texts, and using data.  ; https://www.samsung.com/us/support/search/?query=galaxy+activate+esim&referrerPageUrl=https%3A%2F%2Fwww.samsung.com%2Fus%2Fsupport%2F&tabOrder=index.html%2Cfaqs%2Canswers%2Ctroubleshooting_guides%2Csupport_videos%2Cresources%2Ccommunity_posts%2Clinks%2Cproducts&facetFilters=%7B%7D&filters=%7B%7D&verticalUrl=faqs.html:

SAMSUNG

Shop Mobile TV & Audio Appliances Computing Displays Accessories SmartThings Explore Support For Business

galaxy activate esim

All FAQs Answers Troubleshooting Guides Videos Resources Community Posts More

1 - 10 of 11

What is a hybrid eSIM card and how does it work?

What is an eSIM card and how does it differ from a physical SIM card?

An eSIM card, or embedded SIM card, is a digital SIM that is built directly into a device, eliminating the need for a physical SIM card. Instead of inserting a physical card, the device's eSIM connects to a cellular network remotely by downloading the necessary information from the network provider. This allows for greater flexibility, as users can switch between different carriers without physically changing the SIM card.

Important: Your network provider/mobile carrier (i.e. AT&T, Verizon, T-Mobile, etc.) is your best resource for carrier-specific information such as transferring your phone number from one sim card to another. Visit your providers online support content for more carrier-specific details:

- AT&T SIM card support content
- Verizon SIM card support content
- Xfinity/Comcast SIM card support content
- T-Mobile SIM card support content
- Charter Spectrum SIM card support content

Can I transfer my existing mobile number to an eSIM or hybrid eSIM card?

Can I use an eSIM or hybrid eSIM card in any device?

Can I activate a Windows AAOEM license on a virtual machine

What should I do if I encounter activation issues with a Windows AAOEM license?

How do I redeem a promotion for a subscription service?

What is a Windows AAOEM license?

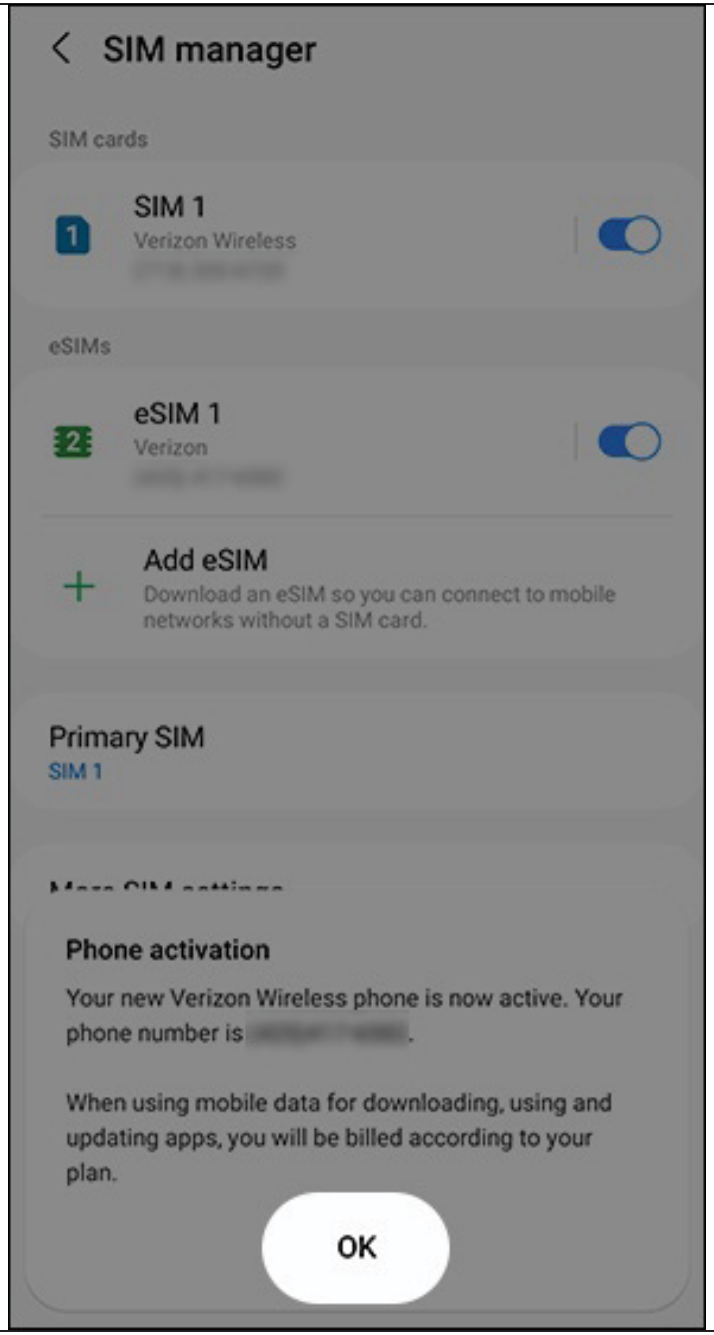
After inserting a new SIM card my phone is asking for a PIN or Unlock Code

Help with Google Factory Reset Protection (FRP)

; https://www.att.com/search/?q=sim%20card&catField=Support; https://www.verizon.com/onesearch/search?q=sim%20card&ES=support&src=wireless; https://www.t-mobile.com/search?q=sim%20card&category=support.

https://www.gsma.com/esim/wp-content/uploads/2022/10/SGP.22-v3.0-1.pdf.

	See also https://www.verizon.com/support/knowledge-base-240165/:


SIM manager
SIM cards
SIM 1
Verizon Wireless
eSIMs
eSIM 1
Verizon
Add eSIM
Download an eSIM so you can connect to mobile networks without a SIM card.
Primary SIM
SIM 1
Phone activation
Your new Verizon Wireless phone is now active. Your phone number is .
When using mobile data for downloading, using and updating apps, you will be billed according to your plan.
OK

; https://www.att.com/support/how-to/wireless/esim-get-started/:

Samsung smartphone

Just turn on your phone and follow the setup prompts. If you have wireless service bars or you can make a call, you're all set.

Don't have service? Look for a notification to add your eSIM or go to your phone **Settings.** Tap **Connections,** then **SIM manager** and **Add eSIM.**

Having trouble? Get more details for Samsung eSIMs.

; https://www.t-mobile.com/support/devices/device-troubleshooting/samsung-on-device-activation-troubleshooting

3.2 Local Profile Management

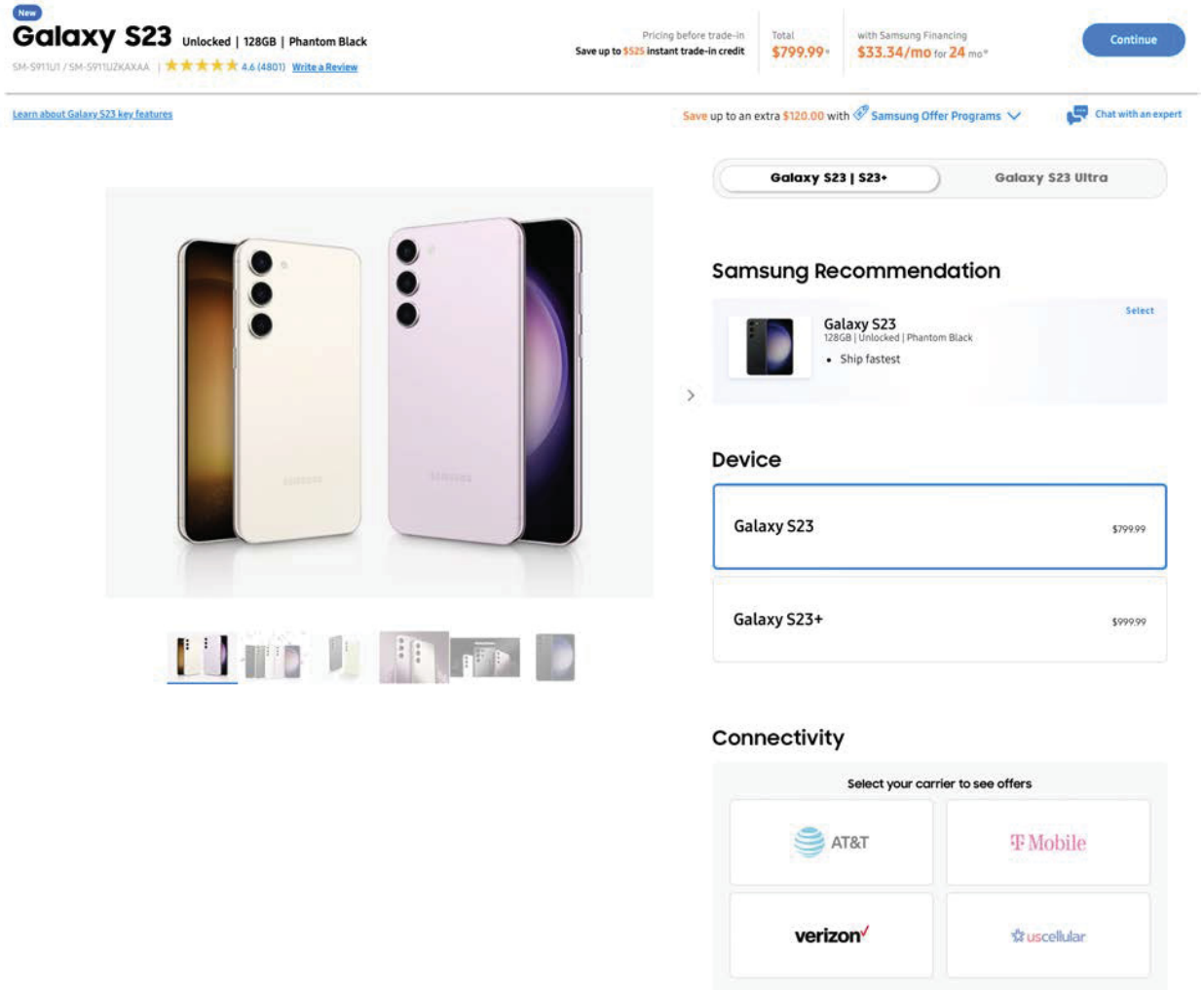
The End User initiates Local Profile Management procedures using the LUI. As specified in SGP.21 [4], User Intent is required for all procedures directed to Operational Profiles, except List Profiles. For each procedure the LPA SHALL enforce the Confirmation Level that is equal to or higher than the Confirmation Level defined in this specification. The specific implementation of Confirmation Requests by the LPA is out of scope of this specification.

In all cases, if the End User refuses or does not respond to a Confirmation Request, then the associated operation SHALL stop.

Confirmation Requests MAY be combined for consecutive operations to simplify the user experience and avoid repeated input steps for the End User. For instance, when performing a Profile download with an Activation Code, the Strong Confirmation for download and Simple Confirmation for enabling the Profile MAY be combined. In the case of combined Confirmation Requests, it SHALL be clear to the End User what operations will be performed, and the highest level of confirmation SHALL be obtained.

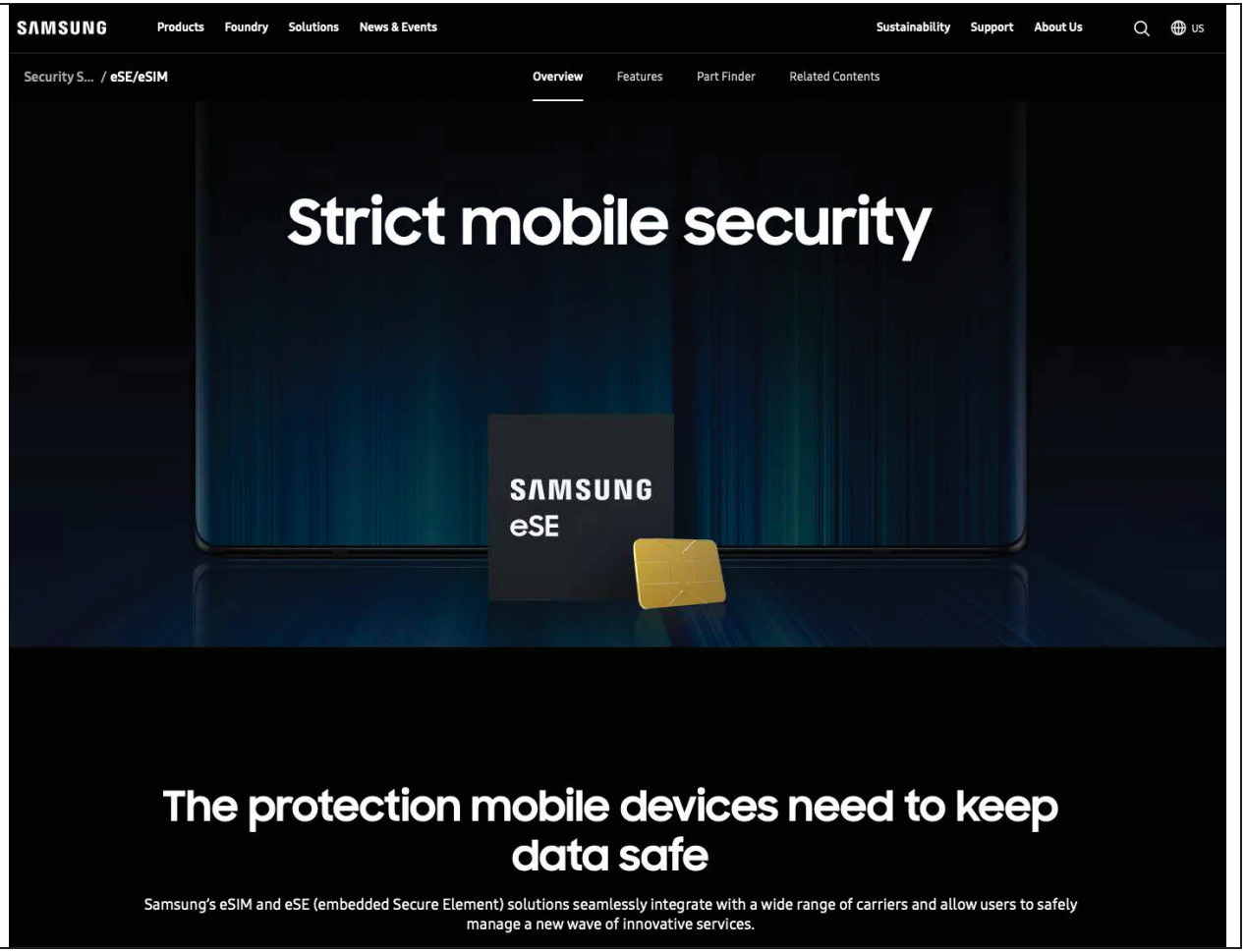
The LUI implementation of Add Profile (section 3.2.5) and Update all Profiles (in section 3.2.7) MAY be combined. For instance, as a composite Add/Update All operation, the LPAd MAY initiate Profile downloads and RPM downloads from the Default SM-DP+(s), Root SM-DS(s), and all Polling Addresses of the installed Profiles.

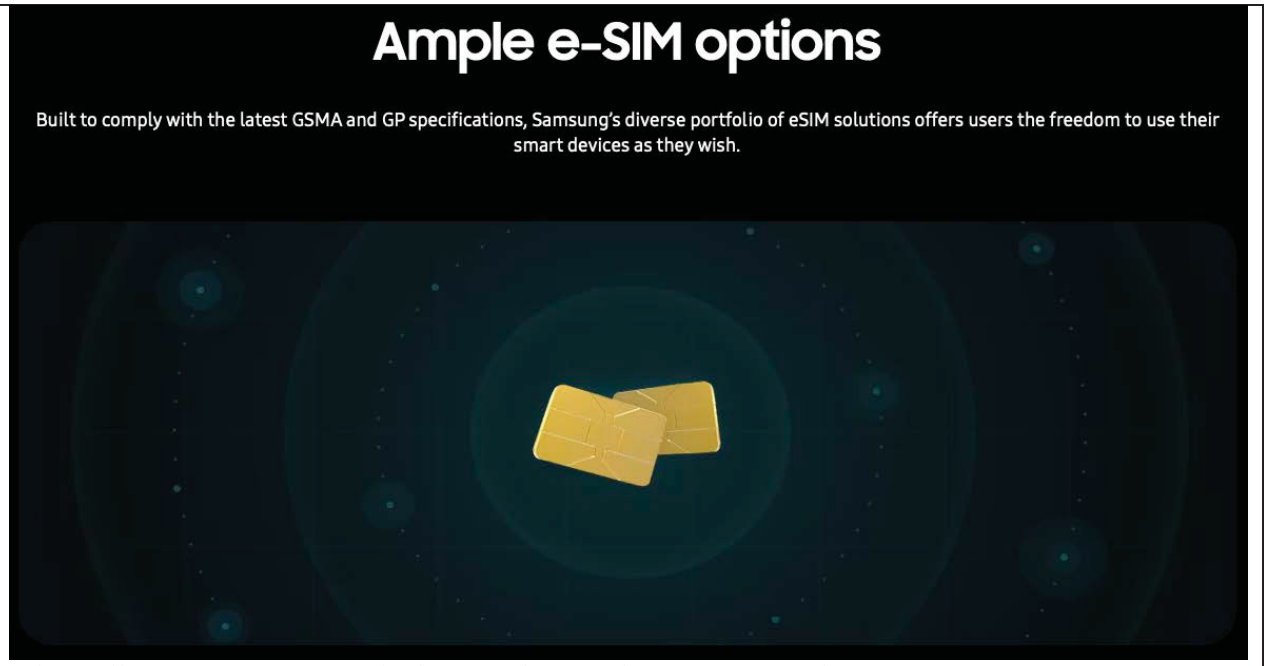
See also https://source.android.com/docs/core/connect/esim-euicc-api; https://source.android.com/docs/core/connect/esim-error-handling;

	https://source.android.com/docs/core/connect/esim-mep; https://source.android.com/docs/core/connect/esim-overview.
[1g] detect a network-provisioning state change, and	Samsung Galaxy phones and tablets "detect a network-provisioning state change." *See, e.g.,* https://www.samsung.com/us/smartphones/galaxy-s23/buy/galaxy-s23-128gb-unlocked-sm-s911uzkaxaa/  ; https://www.samsung.com/us/smartphones/galaxy-s23/specs/:

	Galaxy S23 Ultra	Galaxy S23+	Galaxy S23
Storage			
	-	-	128GB
	256GB	256GB	256GB
	512GB	512GB	-
	1TB	-	-

; https://semiconductor.samsung.com/us/security-solution/ese-esim/:


SAMSUNG
Products
Foundry
Solutions
News & Events
Sustainability
Support
About Us
US
Security S... / eSE/eSIM
Overview
Features
Part Finder
Related Contents
Strict mobile security
SAMSUNG
eSE
The protection mobile devices need to keep data safe
Samsung's eSIM and eSE (embedded Secure Element) solutions seamlessly integrate with a wide range of carriers and allow users to safely manage a new wave of innovative services.

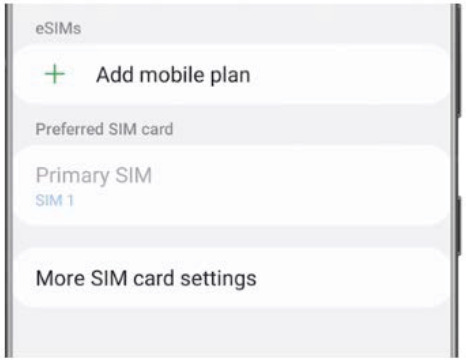
	 ; https://www.samsung.com/us/support/answer/ANS00079039/:

Using the eSIM

An eSIM is an embedded version of the physical SIM card on the phone. The eSIM provides connection to your carrier's network, however instead of inserting a card, you will activate it with your carrier account information. You can also use the eSIM alongside a physical SIM to add a second phone number or carrier to your phone.

Manage your SIM and eSIM

1. Open **Settings** and then tap **Connections**.
2. Tap **SIM card manager**.



From here you can tap the **switch** next to your physical SIM, or activated eSIM to enable or disable their connections. You can also tap **Primary SIM** to change the default connection for making calls, sending texts, and using data.

To start using the eSIM, you will need to follow your carrier's instructions.

- **T-Mobile activation**
- **Verizon activation**
- **AT&T activation**

; https://www.samsung.com/ph/support/mobile-devices/how-to-activate-esim-on-a-galaxy-device/:

	# How to activate eSIM on a Galaxy device Last Update date : Jul 24. 2023 **Your device includes an eSIM which functions as a SIM card. You can use the mobile network after activating the eSIM or installing a nano-SIM card. You can both activate the eSIM and install a nano-SIM card so you can have two phone numbers or service providers for a single device.** **In some areas, data transfer speeds may be slower if two SIM cards are inserted in the device than when one SIM card is inserted.** Before you try out the below recommendations as to your solution, be sure to check if your device's software is updated with the latest version. Please check how to update your mobile device's software in the following order. **Step 1.** Go to **Settings > Software update**. **Step 2.** Tap on **Download and install**. **Step 3**. Follow the on-screen instructions. ## How to add your mobile plan on your smartphone with eSIM To add your mobile network plan on an eSIM, you can scan a QR code that your carrier provided or install a pre-assigned plan automatically. Before adding your plan, make sure your Galaxy smartphone is connected to a wi-fi or mobile data network. **Note:** Device screenshots and menus may vary depending on the device model and software version. ; https://www.samsung.com/us/support/search/?query=galaxy+activate+esim&referrerPageUrl=https%3A%2F%2Fwww.samsung.com%2Fus%2Fsupport%2F&tabOrder=index.html%2Cfaqs%2Canswers%2Ctroubleshooting_guides%2Csupport_videos%2Cresources%2Ccommunity_posts%2Clinks%2Cproducts&facetFilters=%7B%7D&filters=%7B%7D&verticalUrl=faqs.html:

SAMSUNG Shop Mobile TV & Audio Appliances Computing Displays Accessories SmartThings Explore Support For Business

galaxy activate esim

All FAQs Answers Troubleshooting Guides Videos Resources Community Posts More

1 - 10 of 11

What is a hybrid eSIM card and how does it work?

What is an eSIM card and how does it differ from a physical SIM card?

An eSIM card, or embedded SIM card, is a digital SIM that is built directly into a device, eliminating the need for a physical SIM card. Instead of inserting a physical card, the device's eSIM connects to a cellular network remotely by downloading the necessary information from the network provider. This allows for greater flexibility, as users can switch between different carriers without physically changing the SIM card.

Important: Your network provider/mobile carrier (i.e. AT&T, Verizon, T-Mobile, etc.) is your best resource for carrier-specific information such as transferring your phone number from one sim card to another. Visit your providers online support content for more carrier-specific details:

- AT&T SIM card support content
- Verizon SIM card support content
- Xfinity/Comcast SIM card support content
- T-Mobile SIM card support content
- Charter Spectrum SIM card support content

Can I transfer my existing mobile number to an eSIM or hybrid eSIM card?

Can I use an eSIM or hybrid eSIM card in any device?

Can I activate a Windows AAOEM license on a virtual machine

What should I do if I encounter activation issues with a Windows AAOEM license?

How do I redeem a promotion for a subscription service?

What is a Windows AAOEM license?

After inserting a new SIM card my phone is asking for a PIN or Unlock Code

Help with Google Factory Reset Protection (FRP)

; https://www.att.com/search/?q=sim%20card&catField=Support; https://www.verizon.com/onesearch/search?q=sim%20card&ES=support&src=wireless; https://www.t-mobile.com/search?q=sim%20card&category=support.

https://www.gsma.com/esim/wp-content/uploads/2022/10/SGP.22-v3.0-1.pdf:

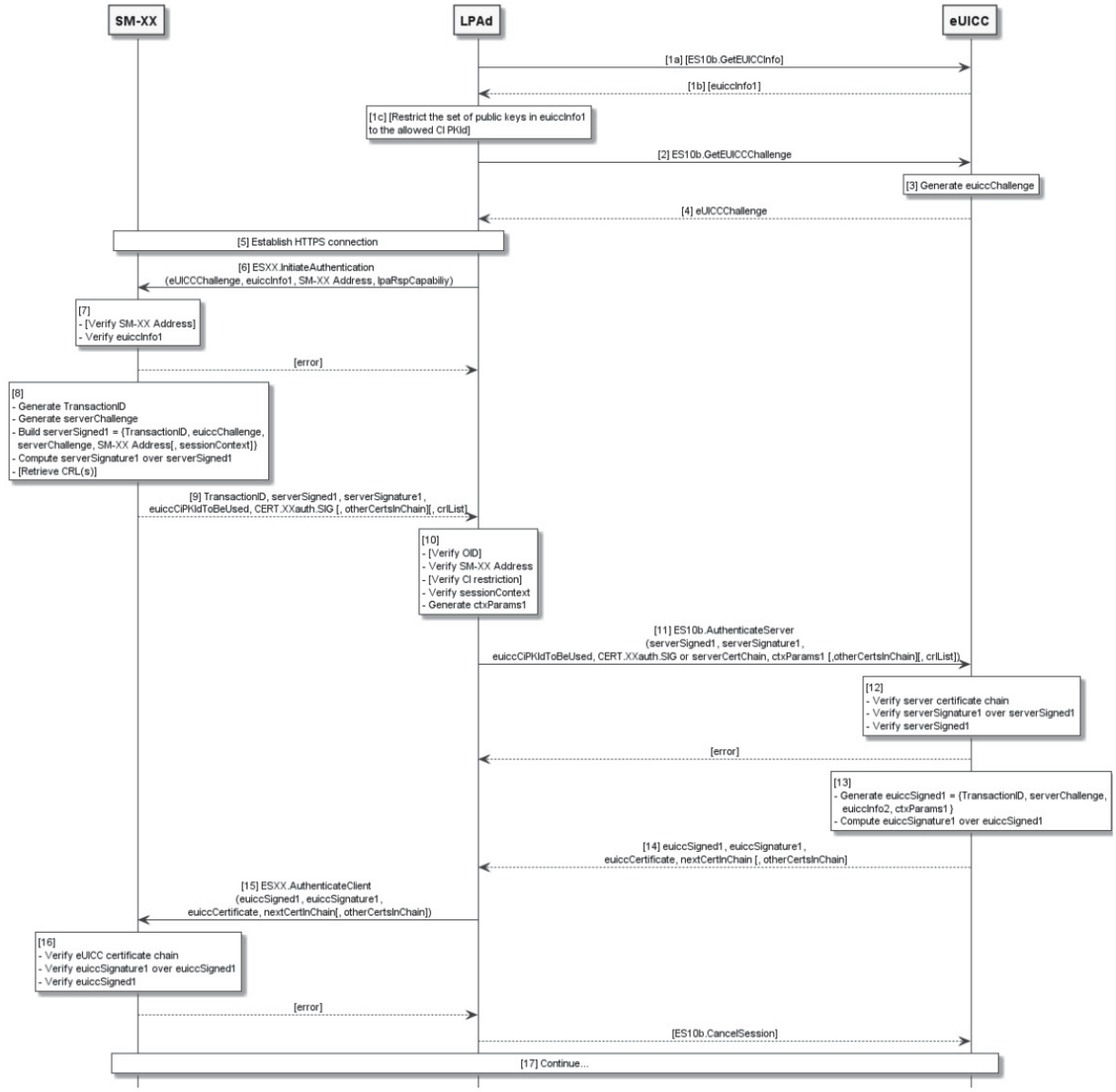


Figure 8a: Common Mutual Authentication Procedure

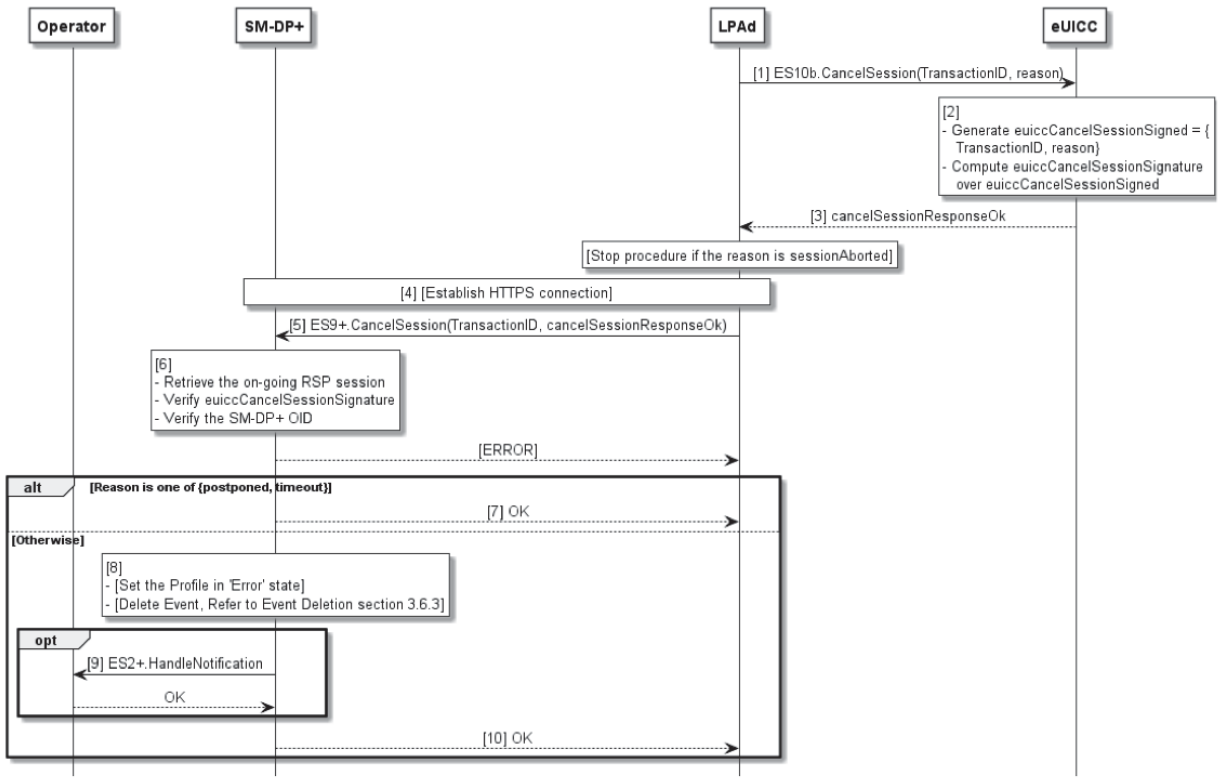


Figure 8b: Common Cancel Session Procedure

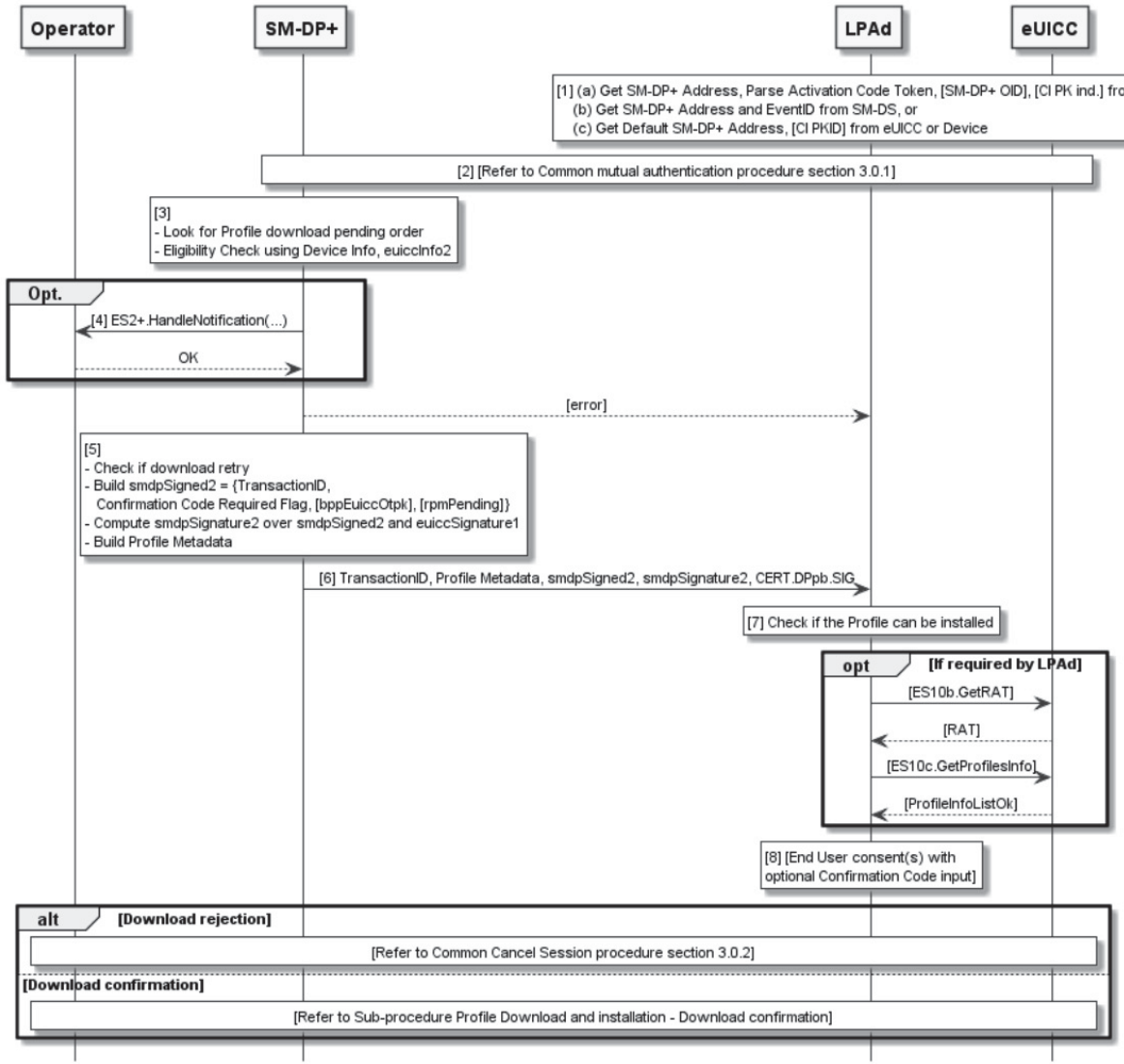


Figure 11: Profile Download and Installation

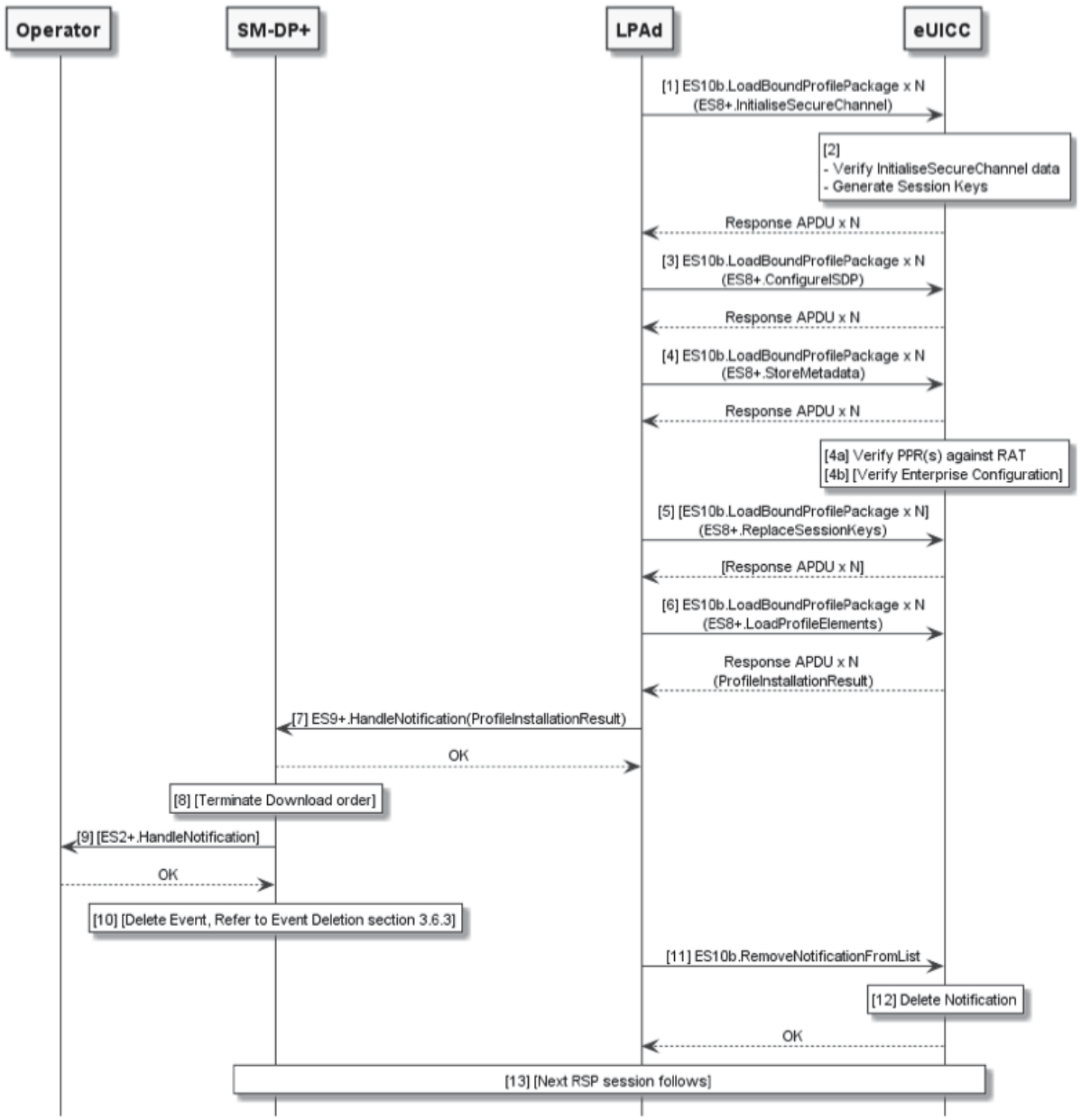


Figure 14: Sub-procedure Profile Installation

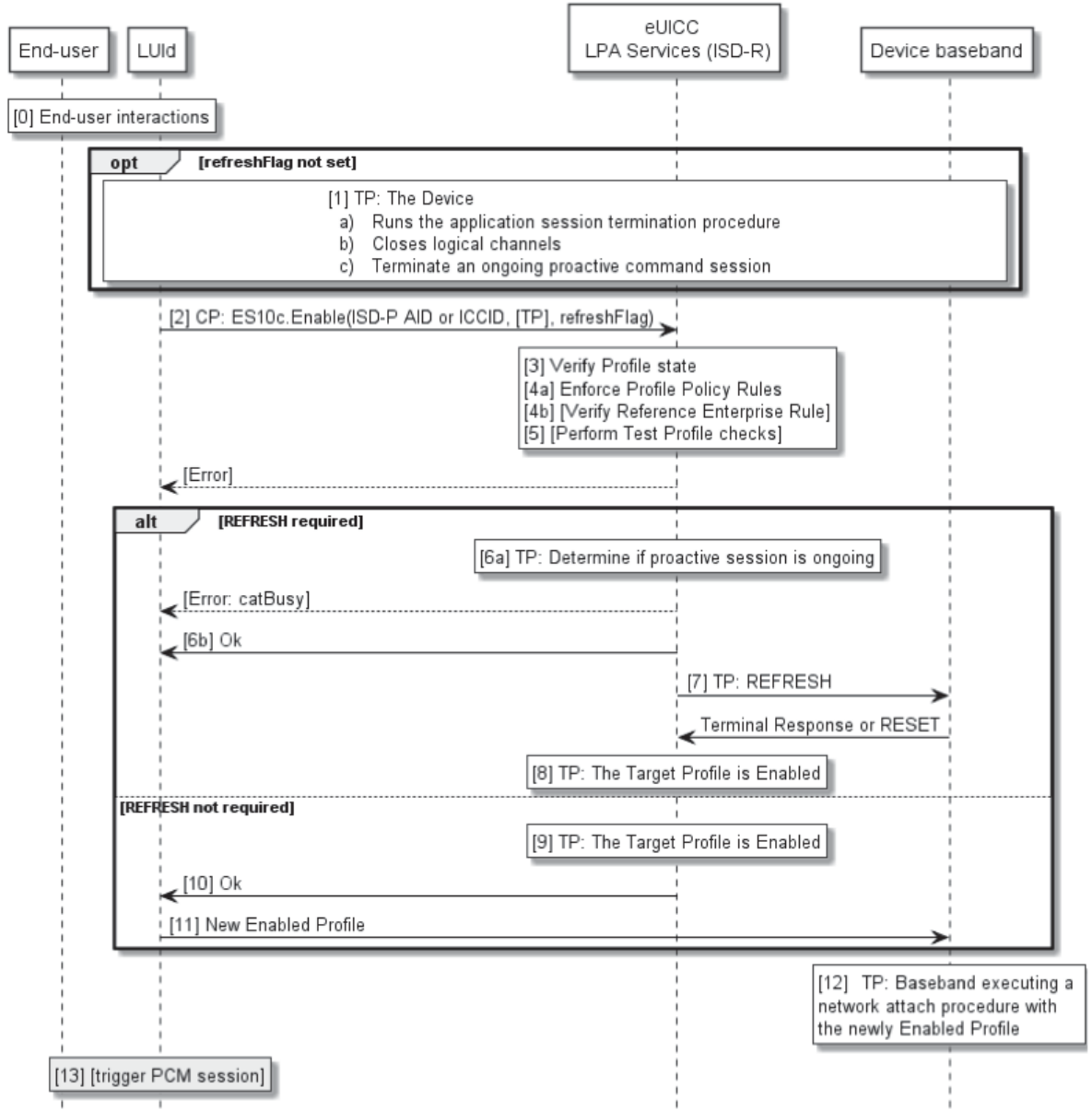


Figure 16: Enable Profile

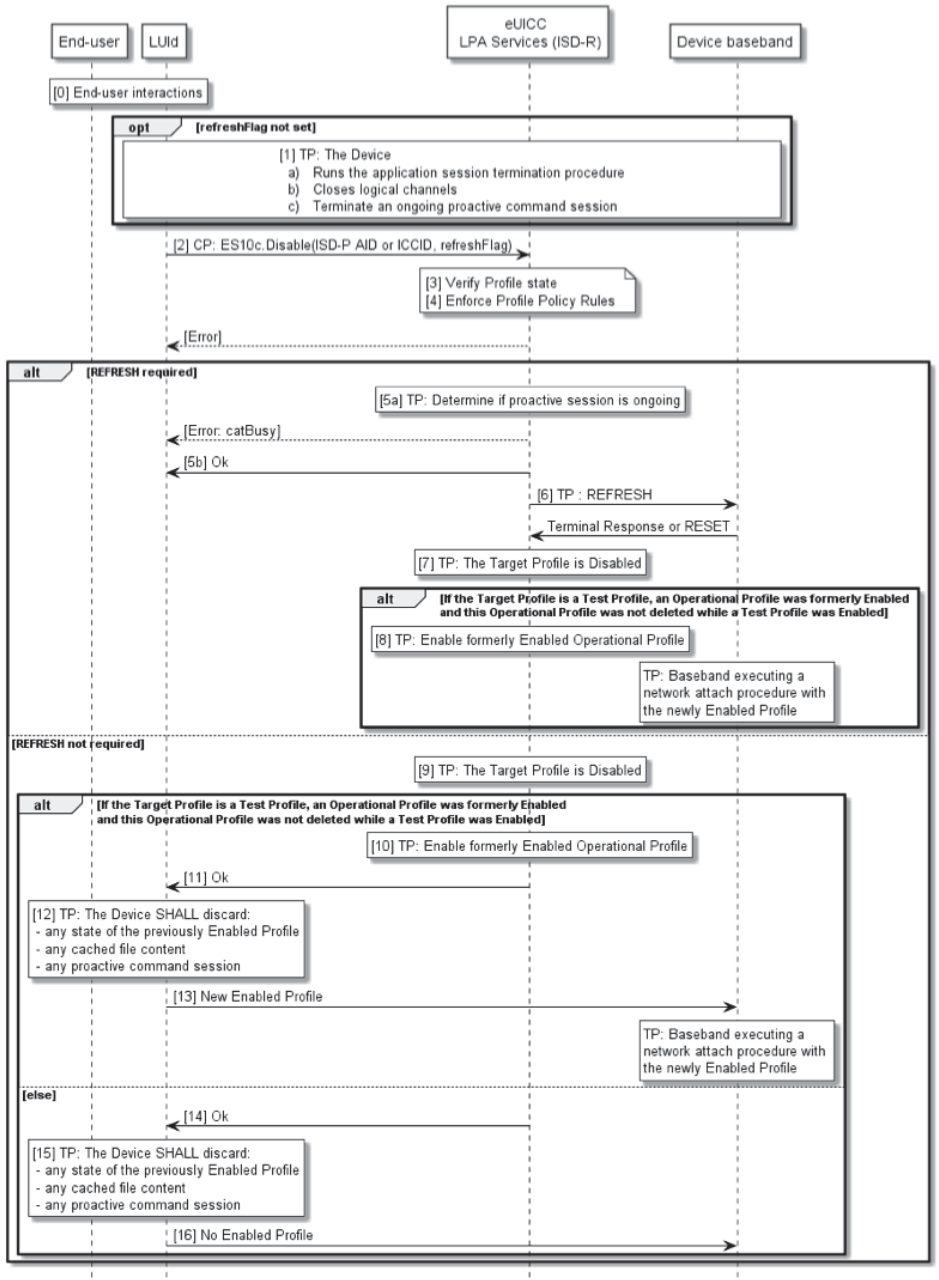


Figure 17: Disable Profile

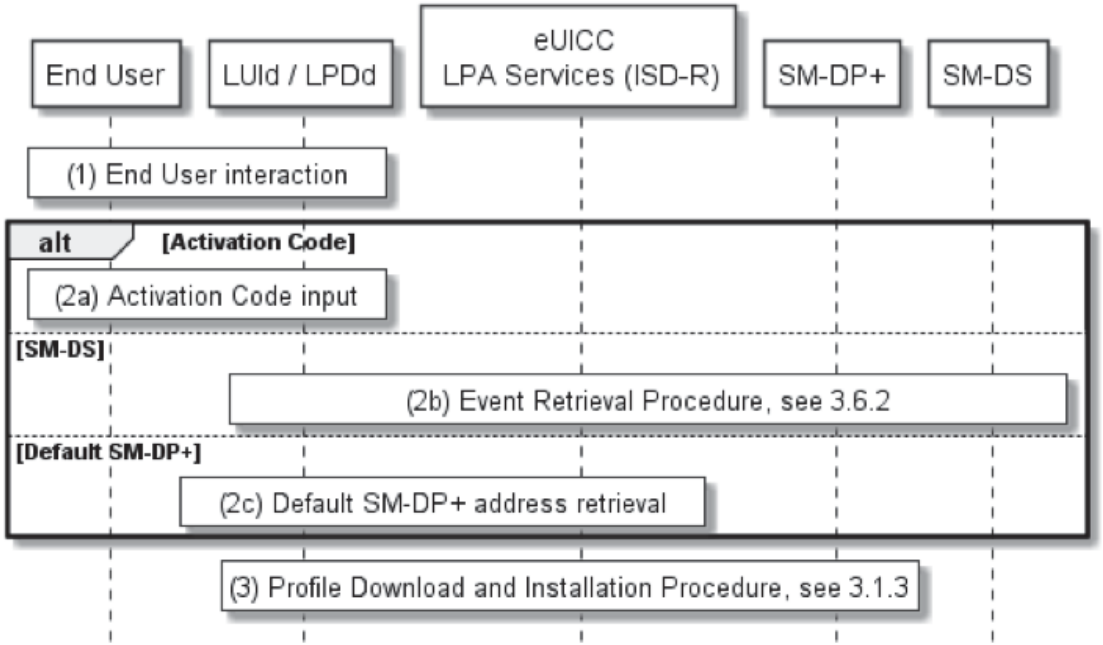


Figure 20: Add Profile

3.7 Remote Profile Management

The Operator initiates Remote Profile Management (RPM) procedure using the ES2+ interface.

RPM is executed by a Managing SM-DP+. A Profile MAY be configured to allow RPM by several Managing SM-DP+s. This specification assumes that a Managing SM-DP+ that prepares an RPM Package has full knowledge of the state of a Profile. How this state is synchronised among multiple Managing SM-DP+s, or procedures where a Managing SM-DP+ does not have full knowledge of the state of a Profile are out of the scope of this specification.

The LPA downloads an RPM Package using the ES9+ interface as described in section 3.7.2. An RPM Package MAY contain one or more RPM Commands.

Each RPM Command SHALL require Confirmation Request enforced by the LPA as described in section 3.7.2. The specific implementation of Confirmation Request by the LPA is out of scope of this specification.

Confirmation Request on multiple RPM Commands for consecutive operations MAY be combined to simplify the user experience and avoid repeated input steps for the End User. For instance, when executing two RPM Commands in an RPM Package, the Strong Confirmation for the first RPM Command and the Simple Confirmation for the second RPM Command MAY be combined. In the case of combined Confirmation Requests, it SHALL be clear to the End User what RPM Commands will be executed, and the highest Confirmation Level SHALL be obtained.

If End User accepts the execution of the RPM Package, the LPA transfers the RPM Package to the eUICC as described in section 3.7.3. The eUICC executes the RPM Command(s) contained in the RPM Package in the received order and generates the Load RPM Package Result specified in section 2.10.2.

Upon completing the execution of an RPM Package, the Operator receives the Load RPM Package Result. Based upon the outcome, the Operator can choose to initiate additional RPM operations. For instance, if a 'Contact PCMP' command resulted in a `noLprConfiguration` error, the Operator could request a new RPM Package containing both an 'Update Metadata' command with `pcmpAddress` and a 'Contact PCMP' command.

3.7.1 RPM Initiation

This procedure is used by Operator to issue an RPM Command(s).

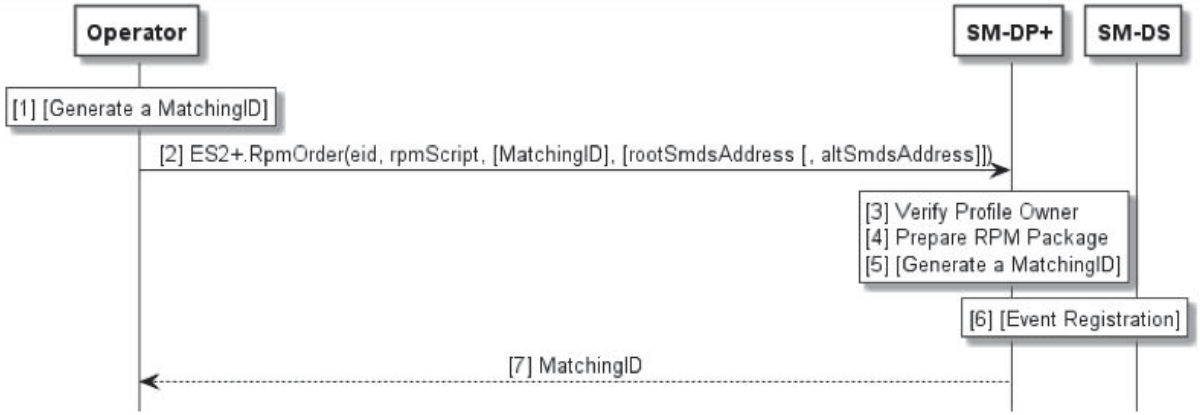


Figure 29a: RPM Initiation

Start Condition:

- The target eUICC has already installed a Profile from the Operator.
- The SM-DP+ is a Managing SM-DP+ of the target Profile.

3.7.2 RPM Download

This procedure is used by LPA to download an RPM Package and to get End User consent on RPM Execution.

The procedure applies for SEP and MEP. The following applies for Command Port:

	Command Port
MEP-A1/A2	0
MEP-B	>=0
SEP	Physical interface

All communication between the LPA and the eUICC in the RPM Download procedure SHALL use the Command Port.

3.7.3 RPM Execution

This procedure is used by LPA to transfer RPM Package to eUICC. The eUICC sequentially executes the RPM Command(s) contained in the RPM Package.

The procedure applies for SEP and MEP. The following applies for Command Port and Target Port:

	Command Port	Target Port
MEP-A1/A2	0	>0
MEP-B	As selected in the RPM Download procedure	>=0, identical to or different from Command Port
SEP	Physical interface	Physical interface

The Target Port is selected in the procedure depending on the presence of Disable or Enable commands.

3.8 Remote Management by the Operator

3.8.1 Metadata Update via ES6

This procedure is used by the Profile Owner to update Metadata of an enabled Profile.

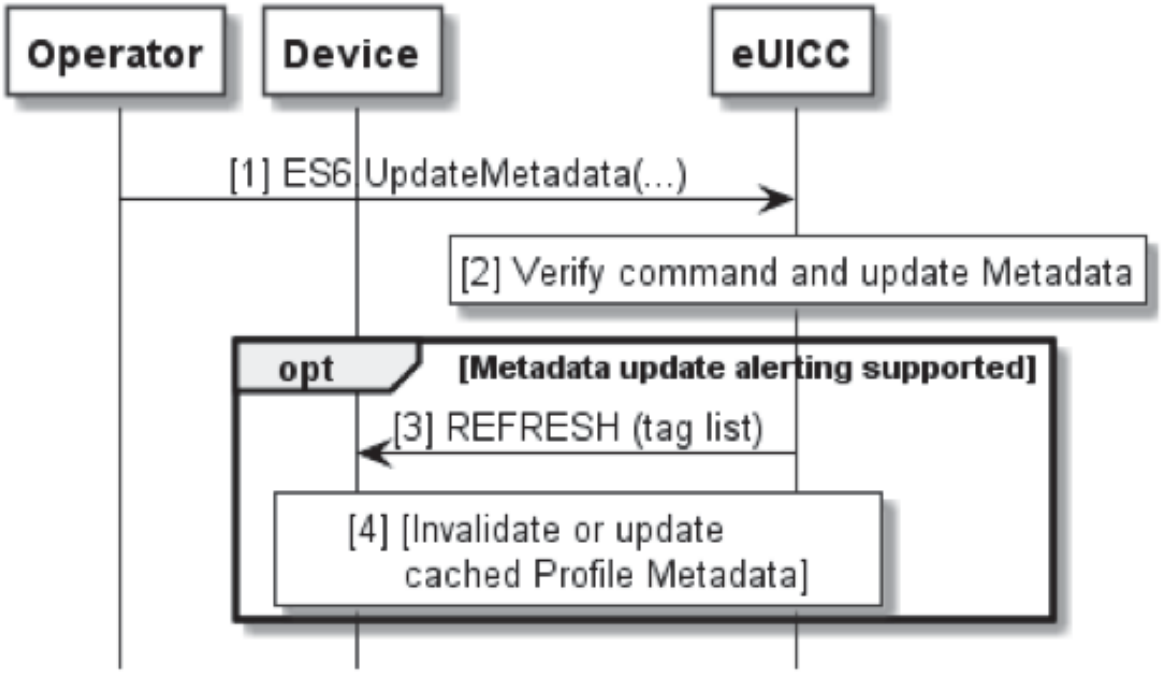


Figure 29j: Metadata Update

3.9 Profile Content Management

This procedure applies when a PCM session is triggered.

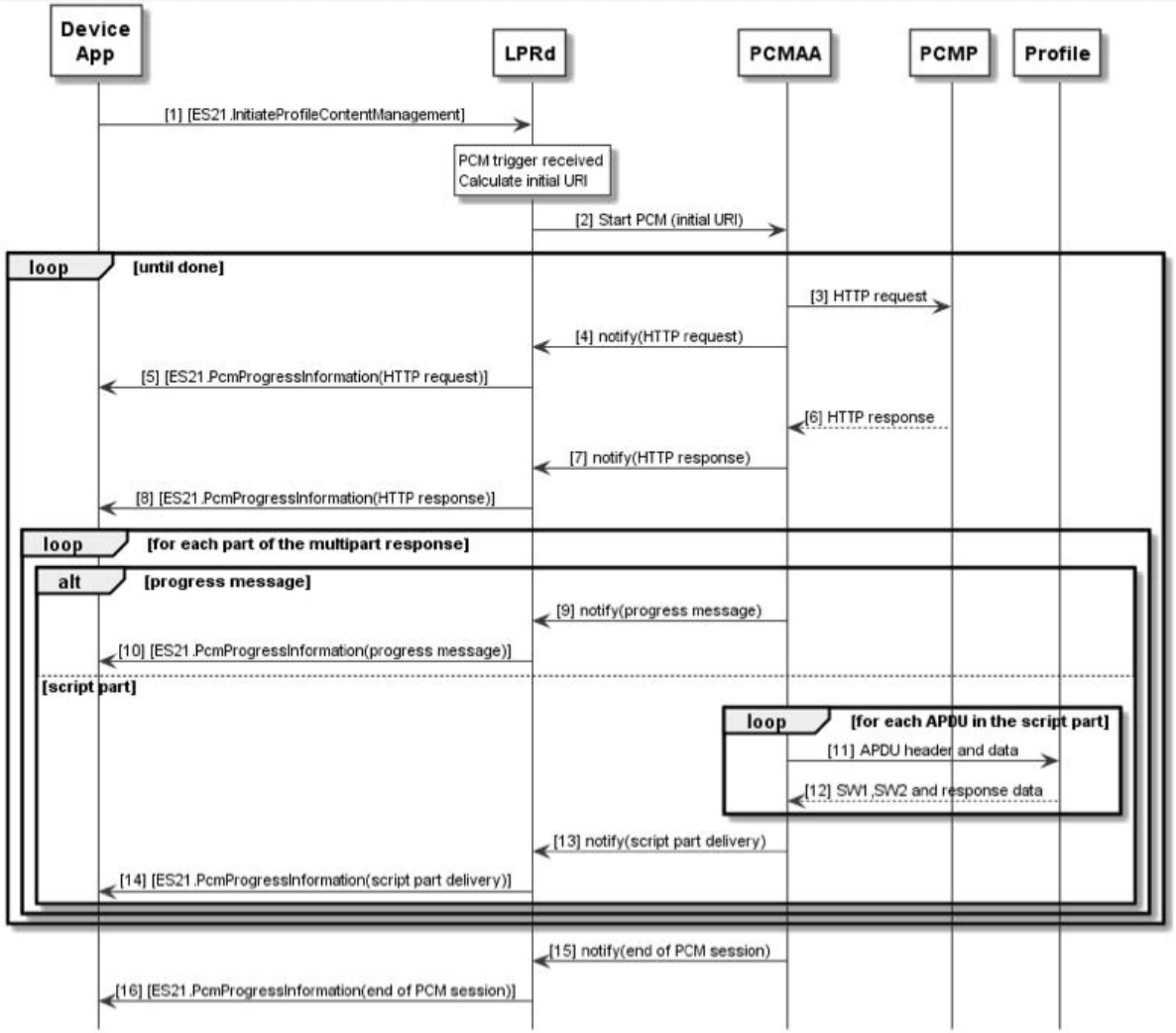


Figure 29I: Profile Content Management

	3.11 Device Change and Profile Recovery **3.11.1 Device Change** This procedure will allow the End User having a Profile in the old Device to add a Profile related to the same Subscription in the new Device. This procedure can further enable the downloaded Profile upon End User consent, which consequently MAY disable a currently Enabled Profile of the new Device (if any). Network connectivity is assumed.

3.1.6 Profile Lifecycle at SM-DP+

The previous sections provide detailed procedures associated with Remote Provisioning. Each Profile has state information on the SM-DP+ associated with it during the provisioning into an eUICC. The Profile lifecycle state can be one of the states listed in the following table.

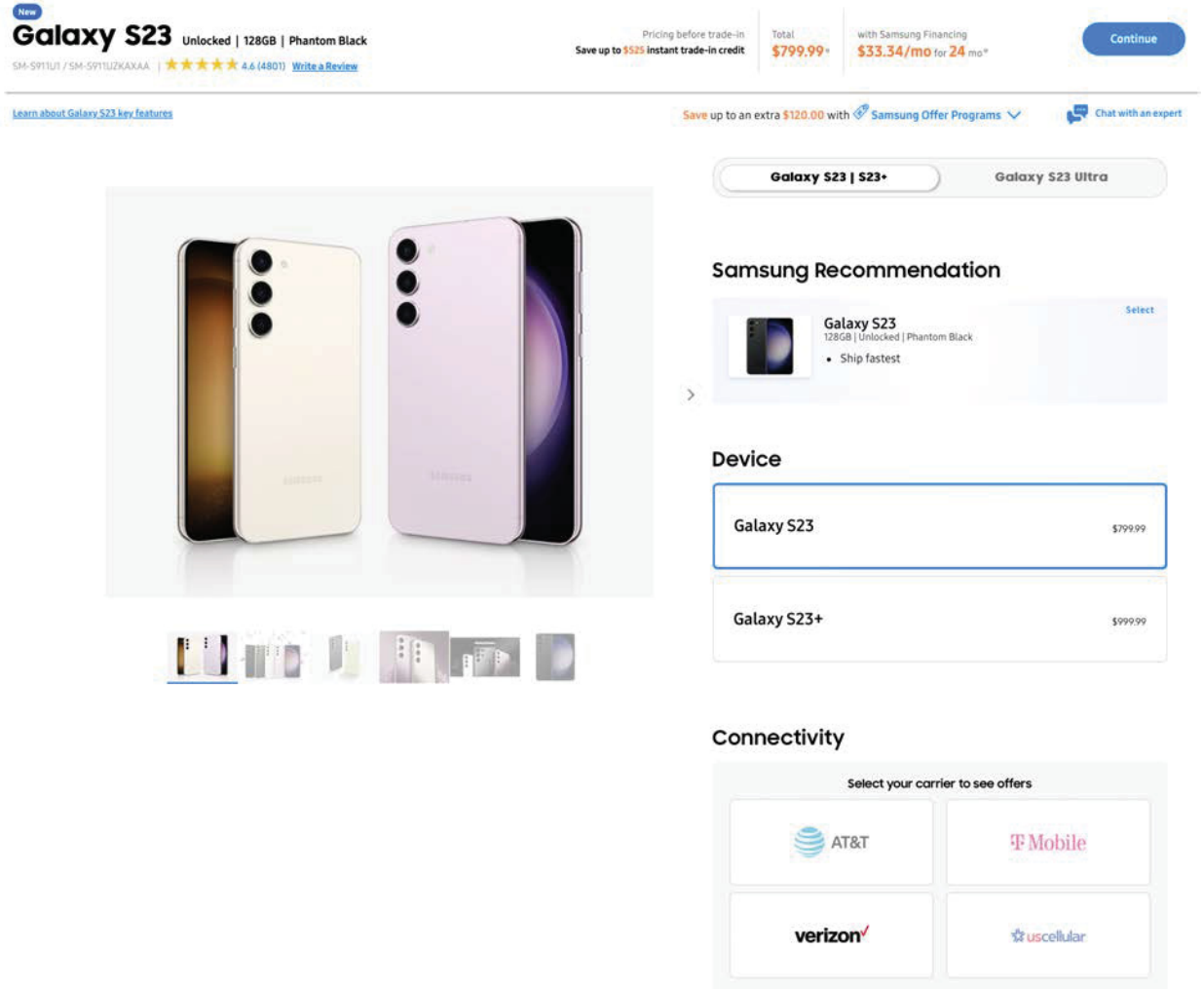
Additional states and additional or customised ES2+ functions MAY be agreed between the Operator and the SM-DP+.

State Name	Description
Available	The Profile is available in the inventory of the SM-DP+.
Allocated	The Profile is reserved for downloading without being linked to an EID.
Linked	The Profile is reserved for downloading and is linked to an EID.
Confirmed	The Profile is reserved for downloading (linked or not linked to an EID) with Matching ID and Confirmation Code if required.
Released	The Profile is ready for download and installation after Network Configuration by the Operator (e.g.: HLR Registration).
Downloaded	The Bound Profile was delivered to the LPA.
Installed	The Profile was successfully installed on the eUICC.
Error	The Profile has not been installed because of one of the following error cases: - Confirmation Code Retry Limit exceeded - Download Retry Limit exceeded - End User Rejection - Permanent error during download and installation
Unavailable	The Profile cannot be reused anymore by the SM-DP+.

Table 6b: Profile State in the SM-DP+

See also https://source.android.com/docs/core/connect/esim-euicc-api; https://source.android.com/docs/core/connect/esim-error-handling;

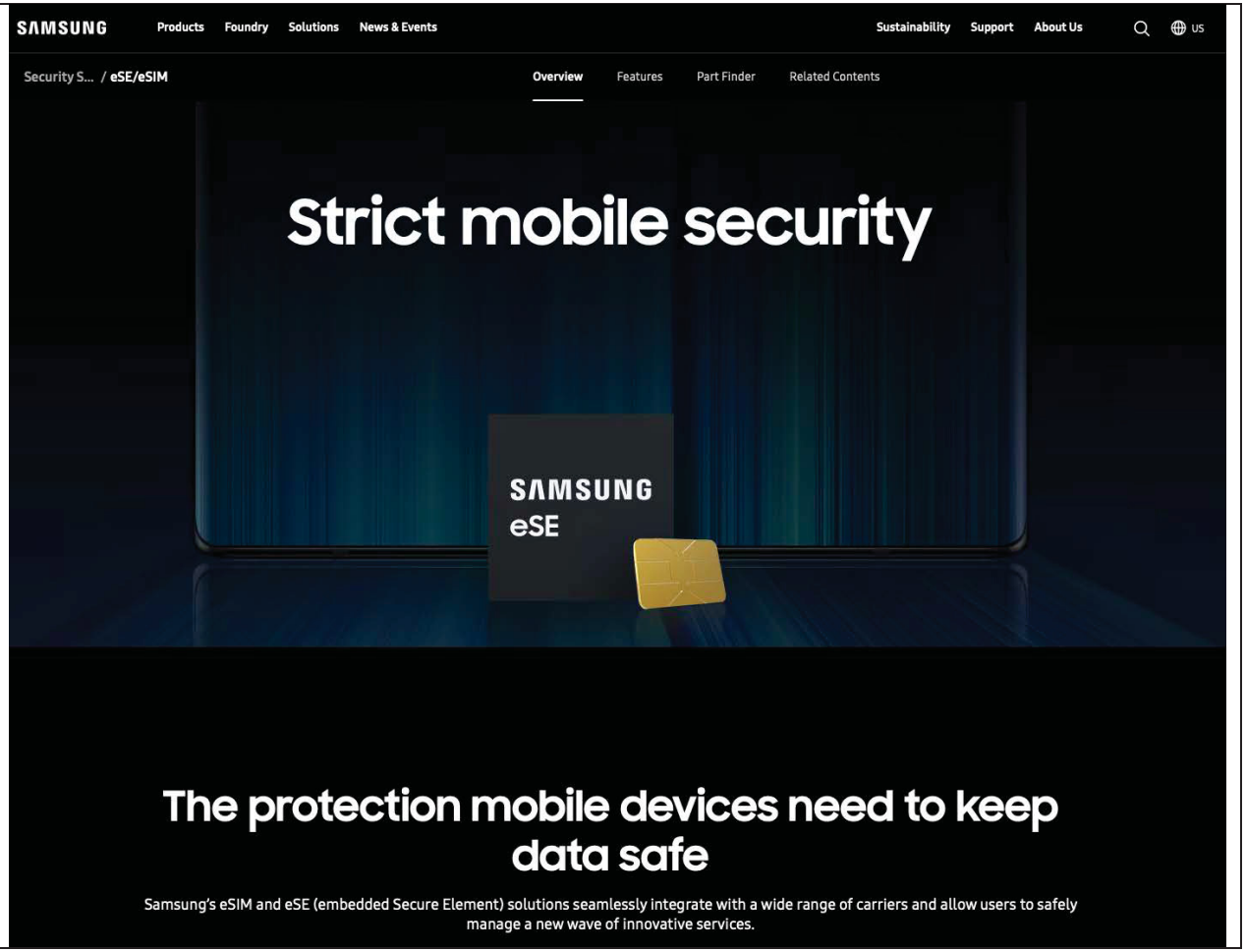
	https://source.android.com/docs/core/connect/esim-mep; https://source.android.com/docs/core/connect/esim-overview.
[1h] based on the detected network-provisioning state change, automatically determine that the particular credential does not match the target credential, initiate a programming session with a network element communicatively coupled to the wireless device over the wireless access network, obtain an updated credential from the network element, and assist in storing, in memory, the updated credential as the particular credential.	Samsung Galaxy phones and tablets "based on the detected network-provisioning state change, automatically determine that the particular credential does not match the target credential, initiate a programming session with a network element communicatively coupled to the wireless device over the wireless access network, obtain an updated credential from the network element, and assist in storing, in memory, the updated credential as the particular credential." *See, e.g.,* https://www.samsung.com/us/smartphones/galaxy-s23/buy/galaxy-s23-128gb-unlocked-sm-s911uzkaxaa/

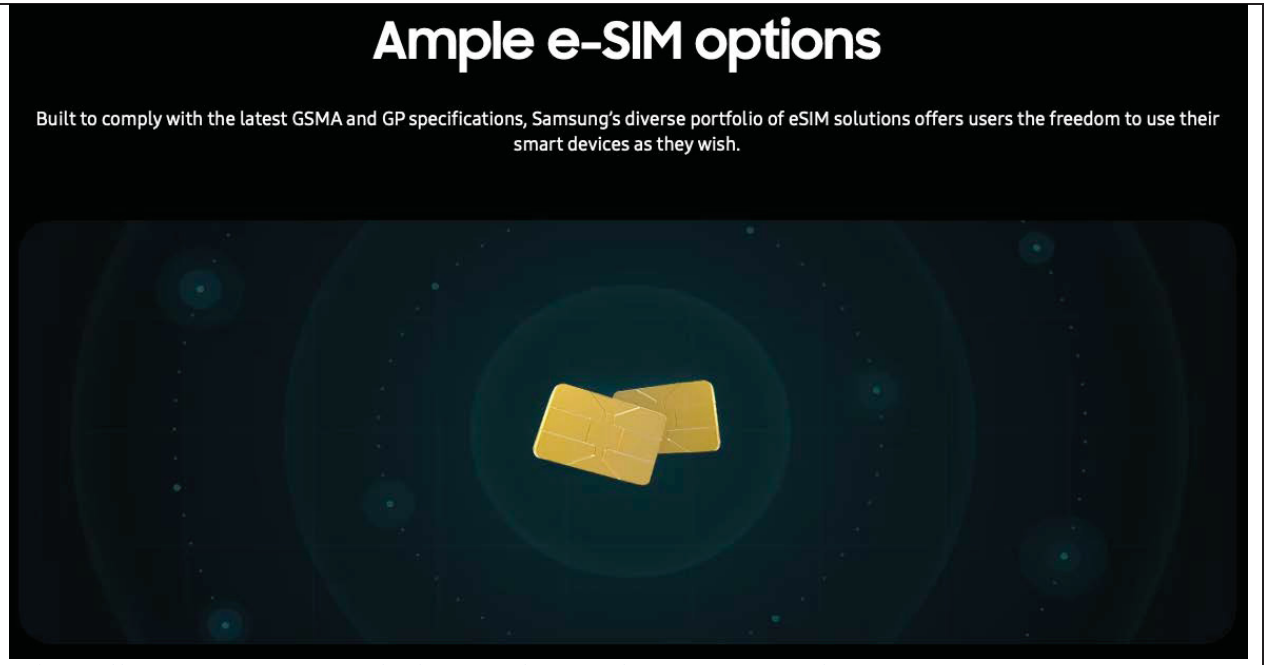


; https://www.samsung.com/us/smartphones/galaxy-s23/specs/:

	Galaxy S23 Ultra	Galaxy S23+	Galaxy S23
Storage			
	-	-	128GB
	256GB	256GB	256GB
	512GB	512GB	-
	1TB	-	-

; https://semiconductor.samsung.com/us/security-solution/ese-esim/:


SAMSUNG
Products
Foundry
Solutions
News & Events
Sustainability
Support
About Us
US
Security S... / eSE/eSIM
Overview
Features
Part Finder
Related Contents
Strict mobile security
SAMSUNG
eSE
The protection mobile devices need to keep data safe
Samsung's eSIM and eSE (embedded Secure Element) solutions seamlessly integrate with a wide range of carriers and allow users to safely manage a new wave of innovative services.

	 ; https://www.samsung.com/us/support/answer/ANS00079039/:

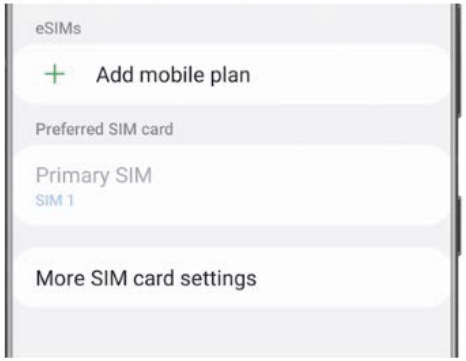
103

Using the eSIM

An eSIM is an embedded version of the physical SIM card on the phone. The eSIM provides connection to your carrier's network, however instead of inserting a card, you will activate it with your carrier account information. You can also use the eSIM alongside a physical SIM to add a second phone number or carrier to your phone.

Manage your SIM and eSIM

1. Open **Settings** and then tap **Connections**.
2. Tap **SIM card manager**.



From here you can tap the **switch** next to your physical SIM, or activated eSIM to enable or disable their connections. You can also tap **Primary SIM** to change the default connection for making calls, sending texts, and using data.

To start using the eSIM, you will need to follow your carrier's instructions.

- **T-Mobile activation**
- **Verizon activation**
- **AT&T activation**

; https://www.samsung.com/ph/support/mobile-devices/how-to-activate-esim-on-a-galaxy-device/:

	# How to activate eSIM on a Galaxy device Last Update date : Jul 24. 2023 **Your device includes an eSIM which functions as a SIM card. You can use the mobile network after activating the eSIM or installing a nano-SIM card. You can both activate the eSIM and install a nano-SIM card so you can have two phone numbers or service providers for a single device.** **In some areas, data transfer speeds may be slower if two SIM cards are inserted in the device than when one SIM card is inserted.** Before you try out the below recommendations as to your solution, be sure to check if your device's software is updated with the latest version. Please check how to update your mobile device's software in the following order. **Step 1.** Go to **Settings > Software update**. **Step 2.** Tap on **Download and install**. **Step 3**. Follow the on-screen instructions. ## How to add your mobile plan on your smartphone with eSIM To add your mobile network plan on an eSIM, you can scan a QR code that your carrier provided or install a pre-assigned plan automatically. Before adding your plan, make sure your Galaxy smartphone is connected to a wi-fi or mobile data network. **Note:** Device screenshots and menus may vary depending on the device model and software version. ; https://www.samsung.com/us/support/search/?query=galaxy+activate+esim&referrerPageUrl=https%3A%2F%2Fwww.samsung.com%2Fus%2Fsupport%2F&tabOrder=index.html%2Cfaqs%2Canswers%2Ctroubleshooting_guides%2Csupport_videos%2Cresources%2Ccommunity_posts%2Clinks%2Cproducts&facetFilters=%7B%7D&filters=%7B%7D&verticalUrl=faqs.html:

SAMSUNG Shop Mobile TV & Audio Appliances Computing Displays Accessories SmartThings Explore Support For Business

galaxy activate esim

All FAQs Answers Troubleshooting Guides Videos Resources Community Posts More

1 - 10 of 11

What is a hybrid eSIM card and how does it work?

What is an eSIM card and how does it differ from a physical SIM card?

An eSIM card, or embedded SIM card, is a digital SIM that is built directly into a device, eliminating the need for a physical SIM card. Instead of inserting a physical card, the device's eSIM connects to a cellular network remotely by downloading the necessary information from the network provider. This allows for greater flexibility, as users can switch between different carriers without physically changing the SIM card.

Important: Your network provider/mobile carrier (i.e. AT&T, Verizon, T-Mobile, etc.) is your best resource for carrier-specific information such as transferring your phone number from one sim card to another. Visit your providers online support content for more carrier-specific details:

- AT&T SIM card support content
- Verizon SIM card support content
- Xfinity/Comcast SIM card support content
- T-Mobile SIM card support content
- Charter Spectrum SIM card support content

Can I transfer my existing mobile number to an eSIM or hybrid eSIM card?

Can I use an eSIM or hybrid eSIM card in any device?

Can I activate a Windows AAOEM license on a virtual machine

What should I do if I encounter activation issues with a Windows AAOEM license?

How do I redeem a promotion for a subscription service?

What is a Windows AAOEM license?

After inserting a new SIM card my phone is asking for a PIN or Unlock Code

Help with Google Factory Reset Protection (FRP)

; https://www.att.com/search/?q=sim%20card&catField=Support; https://www.verizon.com/onesearch/search?q=sim%20card&ES=support&src=wireless; https://www.t-mobile.com/search?q=sim%20card&category=support.

https://www.gsma.com/esim/wp-content/uploads/2022/10/SGP.22-v3.0-1.pdf:

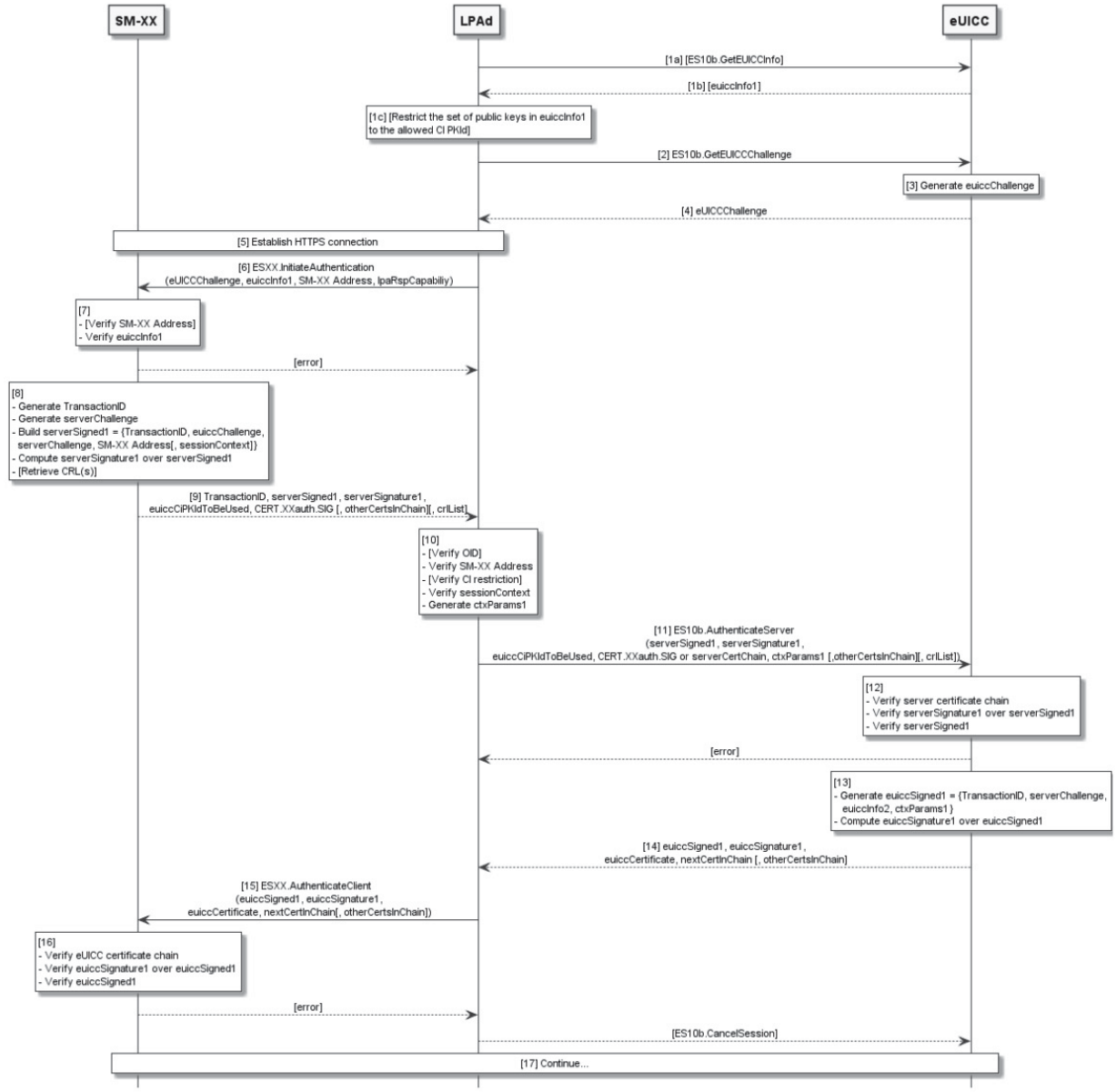


Figure 8a: Common Mutual Authentication Procedure

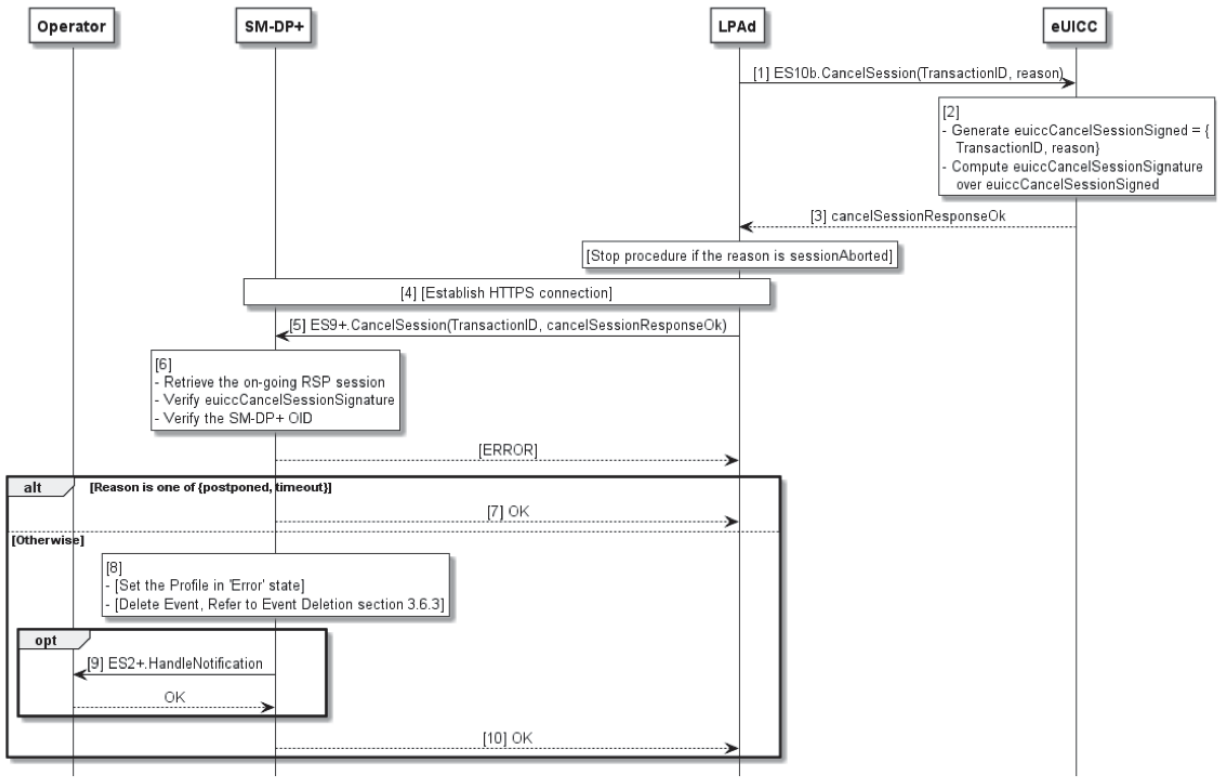


Figure 8b: Common Cancel Session Procedure

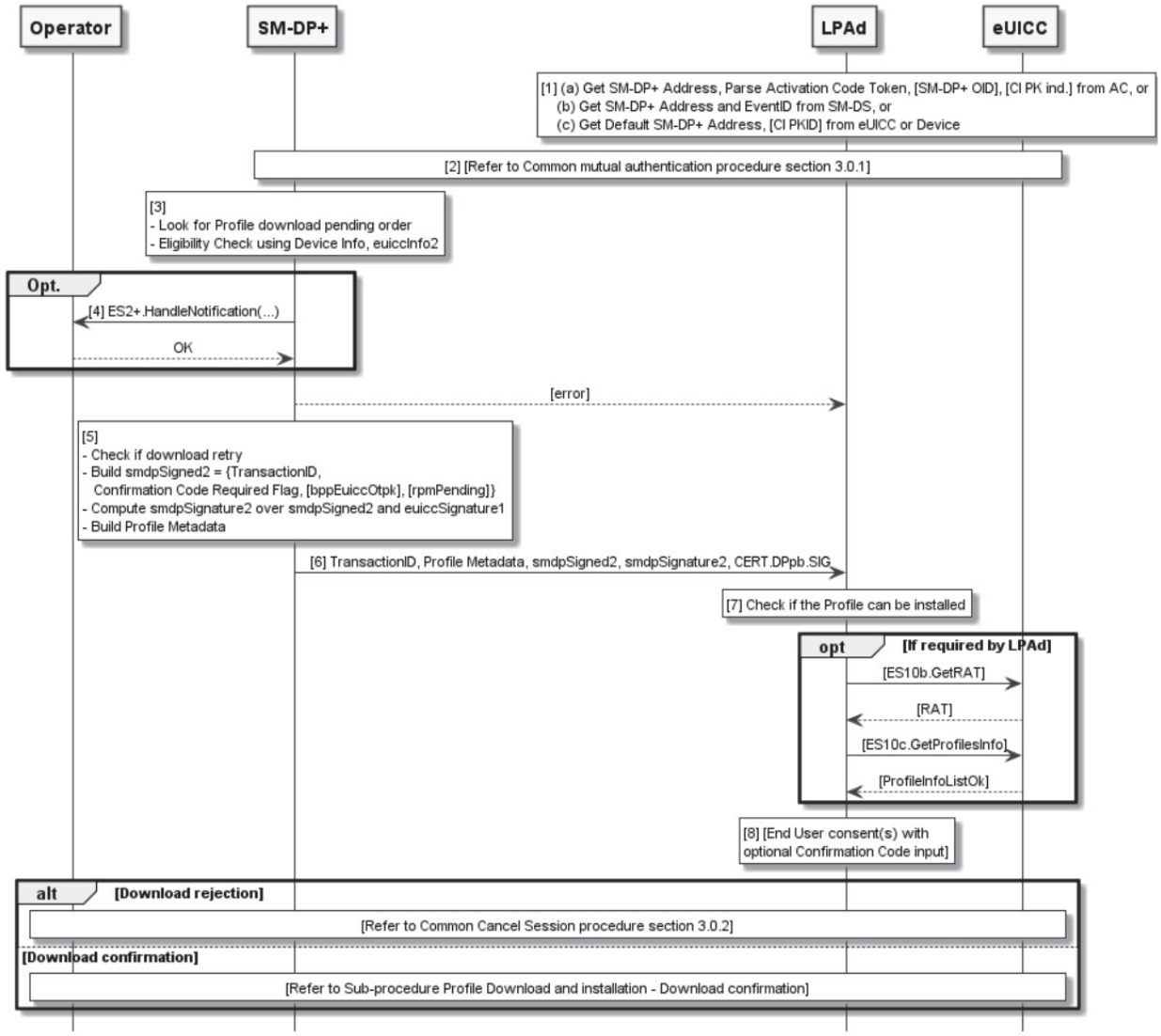


Figure 11: Profile Download and Installation

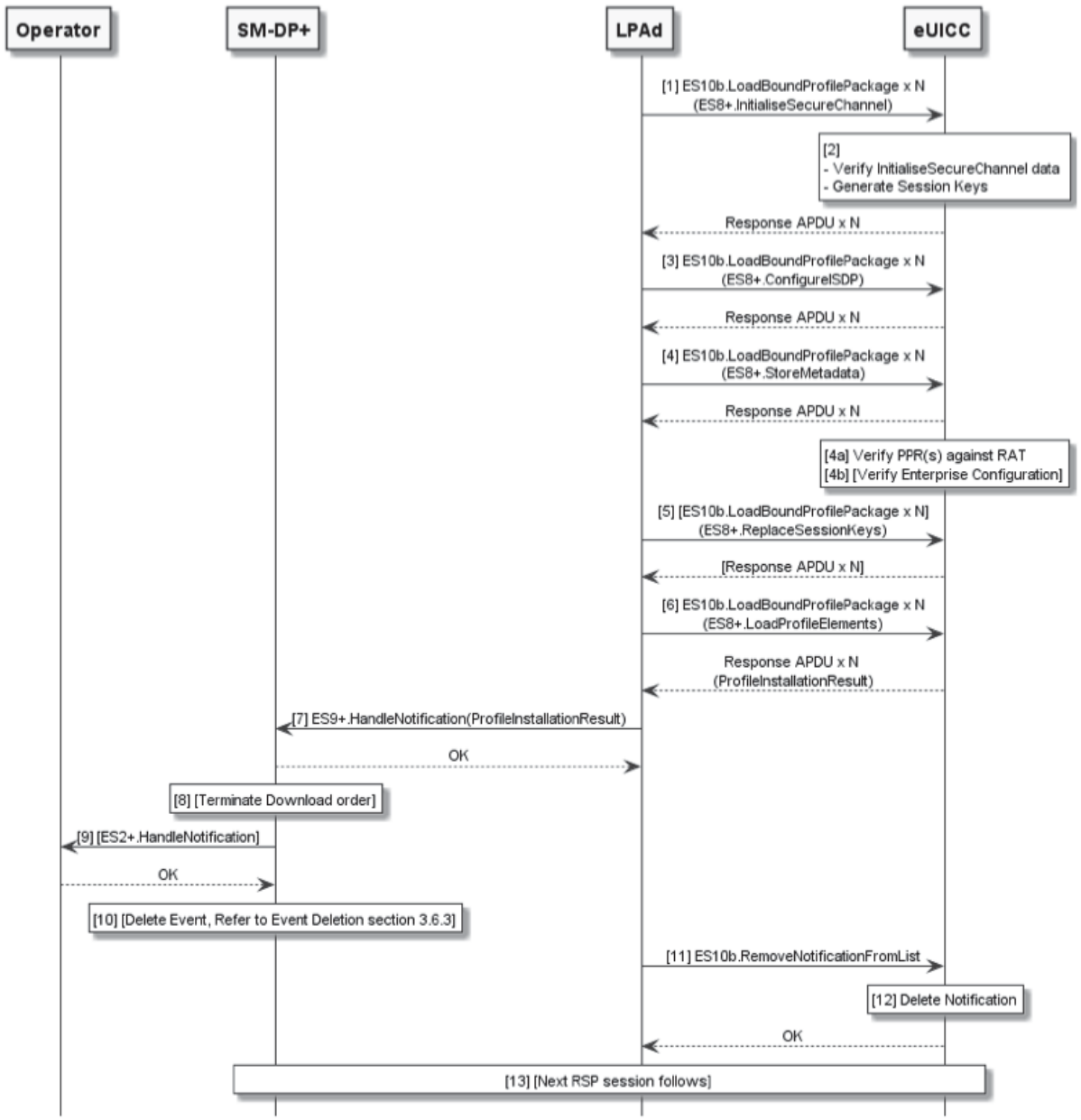


Figure 14: Sub-procedure Profile Installation

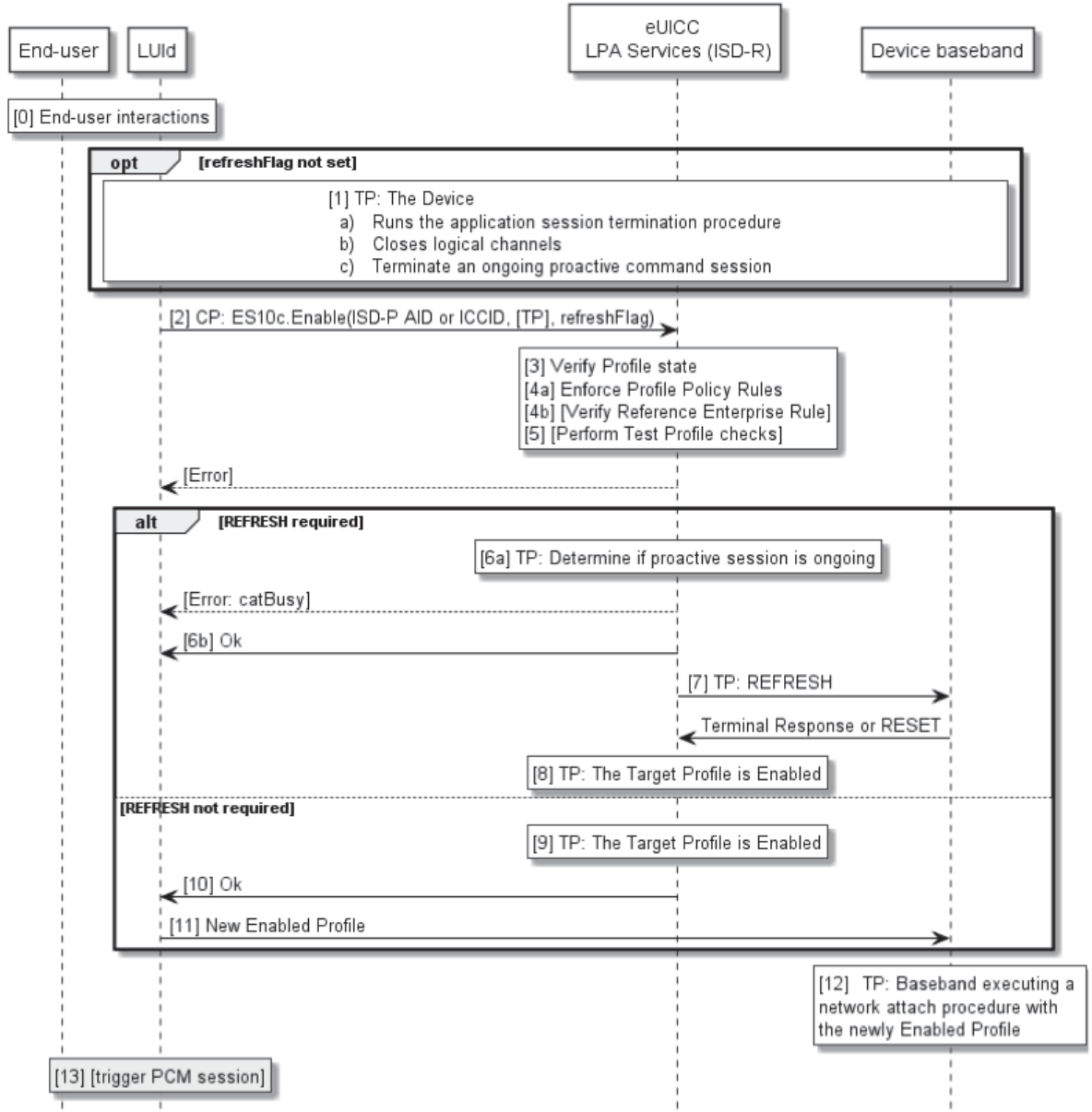


Figure 16: Enable Profile

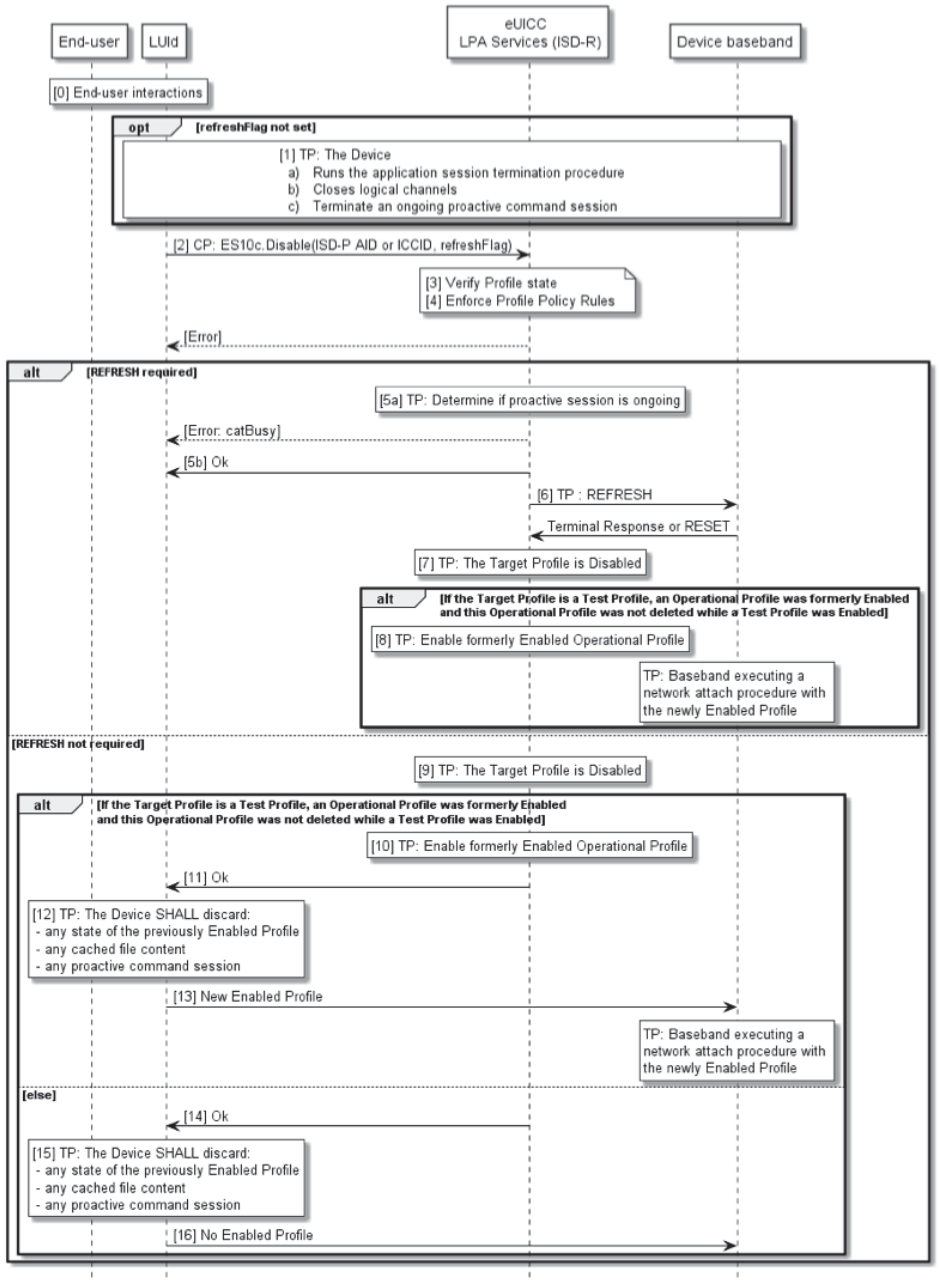


Figure 17: Disable Profile

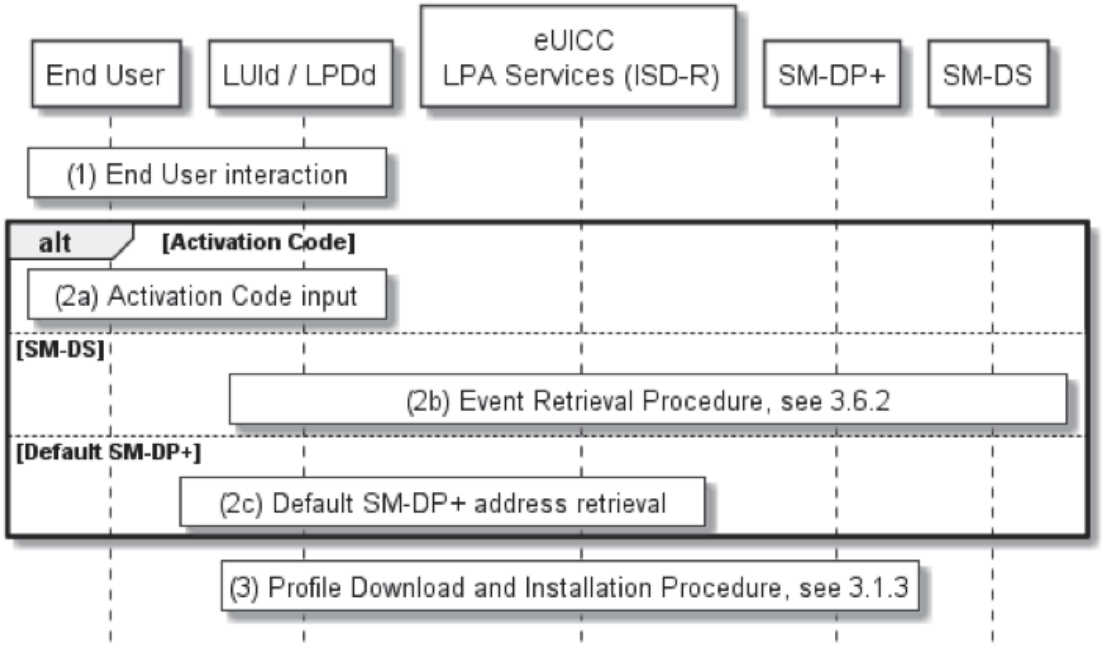


Figure 20: Add Profile

3.7 Remote Profile Management

The Operator initiates Remote Profile Management (RPM) procedure using the ES2+ interface.

RPM is executed by a Managing SM-DP+. A Profile MAY be configured to allow RPM by several Managing SM-DP+s. This specification assumes that a Managing SM-DP+ that prepares an RPM Package has full knowledge of the state of a Profile. How this state is synchronised among multiple Managing SM-DP+s, or procedures where a Managing SM-DP+ does not have full knowledge of the state of a Profile are out of the scope of this specification.

The LPA downloads an RPM Package using the ES9+ interface as described in section 3.7.2. An RPM Package MAY contain one or more RPM Commands.

Each RPM Command SHALL require Confirmation Request enforced by the LPA as described in section 3.7.2. The specific implementation of Confirmation Request by the LPA is out of scope of this specification.

Confirmation Request on multiple RPM Commands for consecutive operations MAY be combined to simplify the user experience and avoid repeated input steps for the End User. For instance, when executing two RPM Commands in an RPM Package, the Strong Confirmation for the first RPM Command and the Simple Confirmation for the second RPM Command MAY be combined. In the case of combined Confirmation Requests, it SHALL be clear to the End User what RPM Commands will be executed, and the highest Confirmation Level SHALL be obtained.

If End User accepts the execution of the RPM Package, the LPA transfers the RPM Package to the eUICC as described in section 3.7.3. The eUICC executes the RPM Command(s) contained in the RPM Package in the received order and generates the Load RPM Package Result specified in section 2.10.2.

Upon completing the execution of an RPM Package, the Operator receives the Load RPM Package Result. Based upon the outcome, the Operator can choose to initiate additional RPM operations. For instance, if a 'Contact PCMP' command resulted in a `noLprConfiguration` error, the Operator could request a new RPM Package containing both an 'Update Metadata' command with `pcmpAddress` and a 'Contact PCMP' command.

3.7.1 RPM Initiation

This procedure is used by Operator to issue an RPM Command(s).

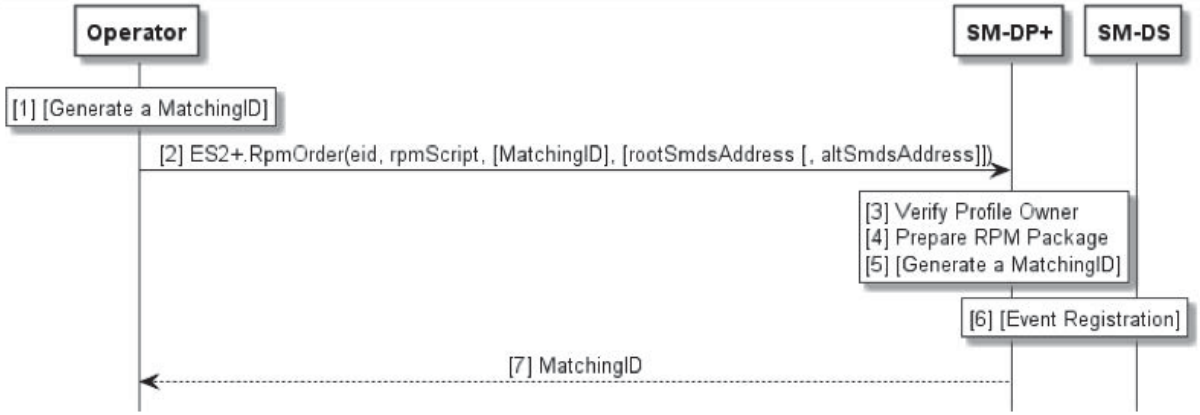


Figure 29a: RPM Initiation

Start Condition:

- The target eUICC has already installed a Profile from the Operator.
- The SM-DP+ is a Managing SM-DP+ of the target Profile.

3.7.2 RPM Download

This procedure is used by LPA to download an RPM Package and to get End User consent on RPM Execution.

The procedure applies for SEP and MEP. The following applies for Command Port:

	Command Port
MEP-A1/A2	0
MEP-B	>=0
SEP	Physical interface

All communication between the LPA and the eUICC in the RPM Download procedure SHALL use the Command Port.

3.7.3 RPM Execution

This procedure is used by LPA to transfer RPM Package to eUICC. The eUICC sequentially executes the RPM Command(s) contained in the RPM Package.

The procedure applies for SEP and MEP. The following applies for Command Port and Target Port:

	Command Port	Target Port
MEP-A1/A2	0	>0
MEP-B	As selected in the RPM Download procedure	>=0, identical to or different from Command Port
SEP	Physical interface	Physical interface

The Target Port is selected in the procedure depending on the presence of Disable or Enable commands.

3.8 Remote Management by the Operator

3.8.1 Metadata Update via ES6

This procedure is used by the Profile Owner to update Metadata of an enabled Profile.

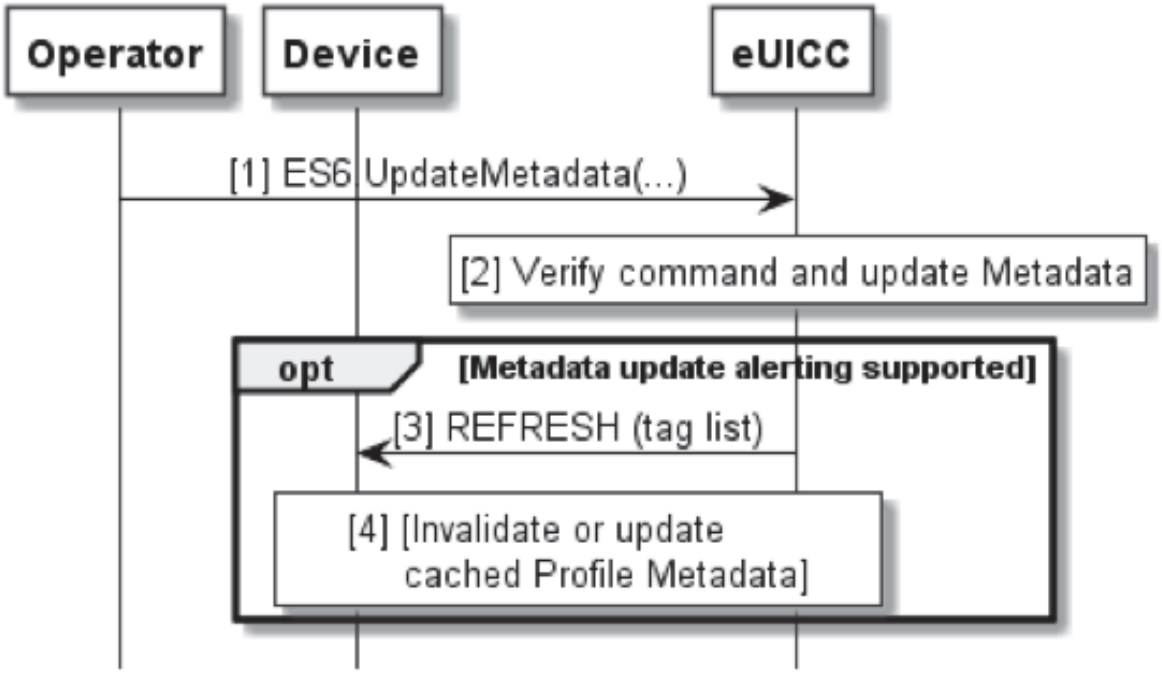


Figure 29j: Metadata Update

3.9 Profile Content Management

This procedure applies when a PCM session is triggered.

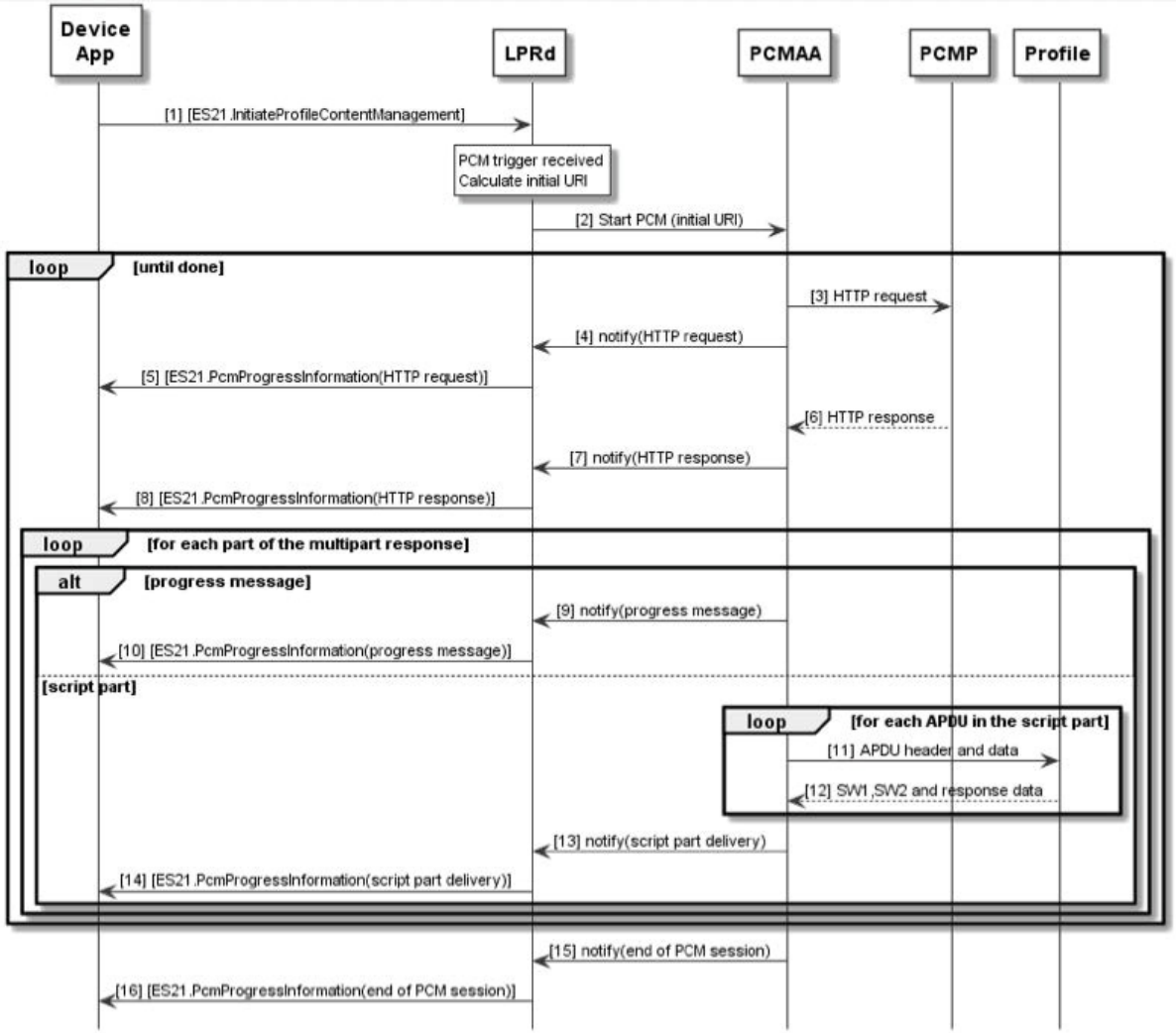


Figure 29I: Profile Content Management

	3.11 Device Change and Profile Recovery **3.11.1 Device Change** This procedure will allow the End User having a Profile in the old Device to add a Profile related to the same Subscription in the new Device. This procedure can further enable the downloaded Profile upon End User consent, which consequently MAY disable a currently Enabled Profile of the new Device (if any). Network connectivity is assumed.

3.1.6 Profile Lifecycle at SM-DP+

The previous sections provide detailed procedures associated with Remote Provisioning. Each Profile has state information on the SM-DP+ associated with it during the provisioning into an eUICC. The Profile lifecycle state can be one of the states listed in the following table.

Additional states and additional or customised ES2+ functions MAY be agreed between the Operator and the SM-DP+.

State Name	Description
Available	The Profile is available in the inventory of the SM-DP+.
Allocated	The Profile is reserved for downloading without being linked to an EID.
Linked	The Profile is reserved for downloading and is linked to an EID.
Confirmed	The Profile is reserved for downloading (linked or not linked to an EID) with Matching ID and Confirmation Code if required.
Released	The Profile is ready for download and installation after Network Configuration by the Operator (e.g.: HLR Registration).
Downloaded	The Bound Profile was delivered to the LPA.
Installed	The Profile was successfully installed on the eUICC.
Error	The Profile has not been installed because of one of the following error cases: - Confirmation Code Retry Limit exceeded - Download Retry Limit exceeded - End User Rejection - Permanent error during download and installation
Unavailable	The Profile cannot be reused anymore by the SM-DP+.

Table 6b: Profile State in the SM-DP+

See also https://source.android.com/docs/core/connect/esim-euicc-api; https://source.android.com/docs/core/connect/esim-error-handling; https://source.android.com/docs/core/connect/esim-mep; https://source.android.com/docs/core/connect/esim-overview.

Claim 2

Issued Claim(s)	Public Documentation
2. The wireless device recited in claim 1, wherein, when executed by the one or more processors, the one or more machine-executable instructions further cause the one or more processors to:	The Accused Devices comprise the "wireless device recited in claim 1, wherein, when executed by the one or more processors, the one or more machine-executable instructions further cause the one or more processors to." *See*, for example, the disclosures identified for claim 1.
determine that the updated credential does not match the target credential, and based on the determination that the updated credential does not match the target credential, take an action.	The Accused Devices "determine that the updated credential does not match the target credential, and based on the determination that the updated credential does not match the target credential, take an action." *See*, for example, the disclosures identified for claim 1. For further example, the Accused Devices take an action (e.g., downloading, installing updating, enabling, disabling, or deleting) when credentials do not match. *See, e.g.,* https://www.gsma.com/esim/wp-content/uploads/2022/10/SGP.22-v3.0-1.pdf:

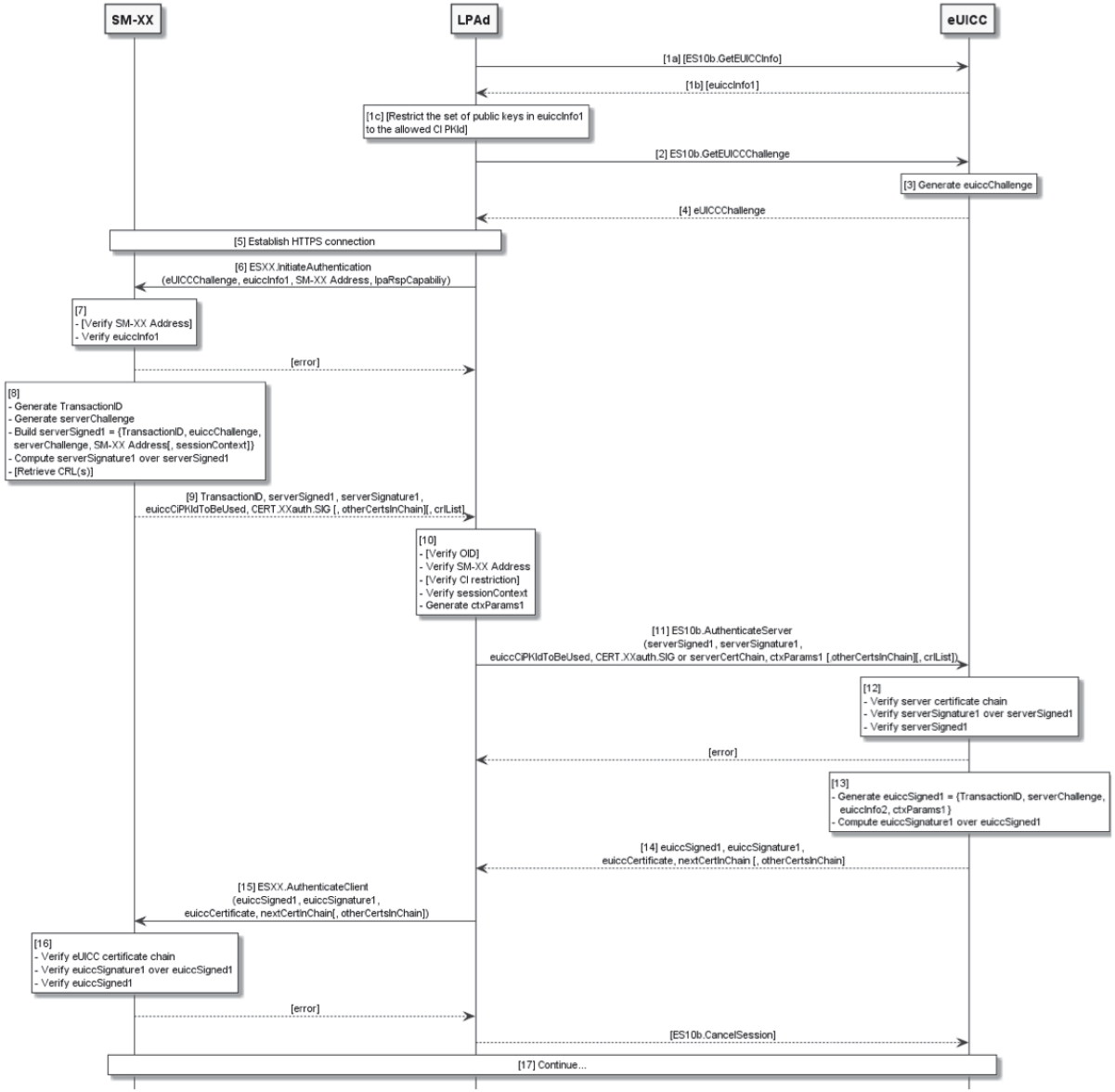


Figure 8a: Common Mutual Authentication Procedure

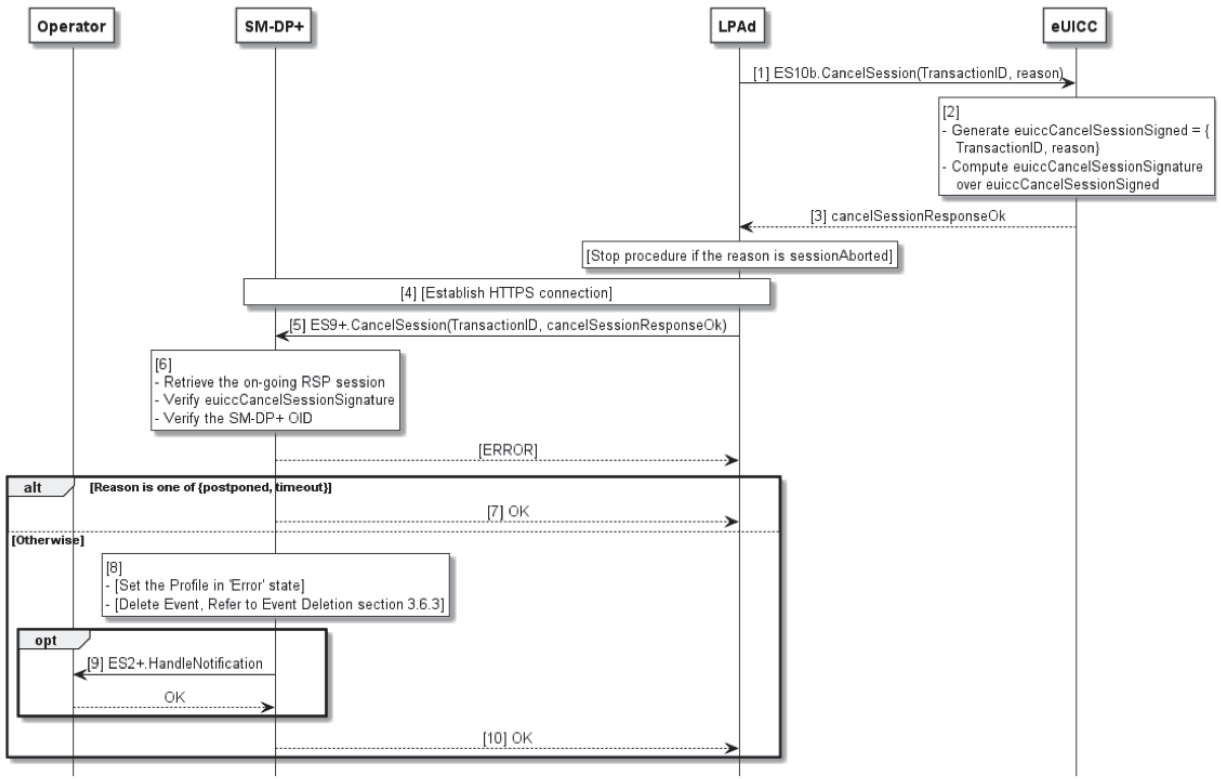


Figure 8b: Common Cancel Session Procedure

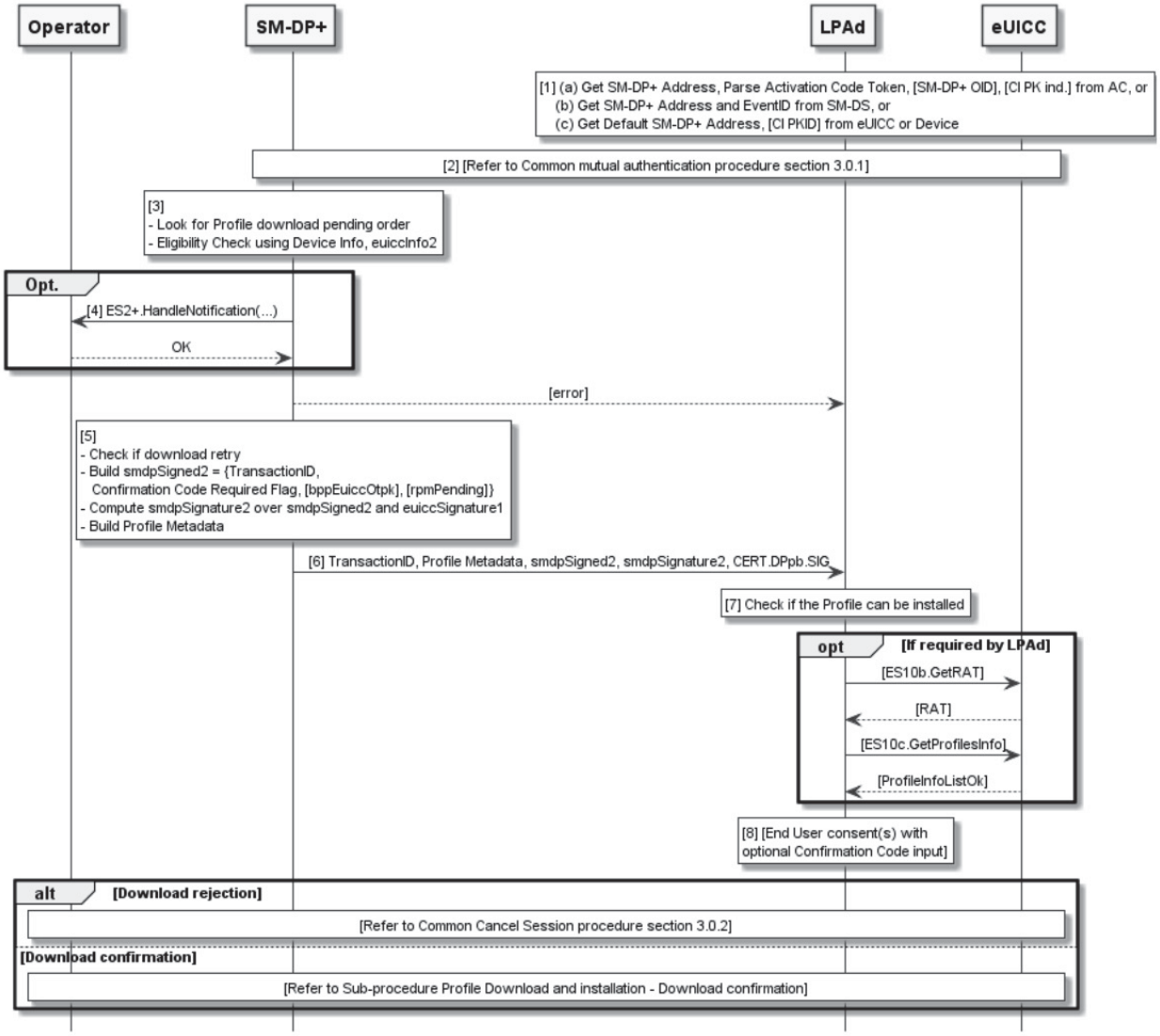


Figure 11: Profile Download and Installation

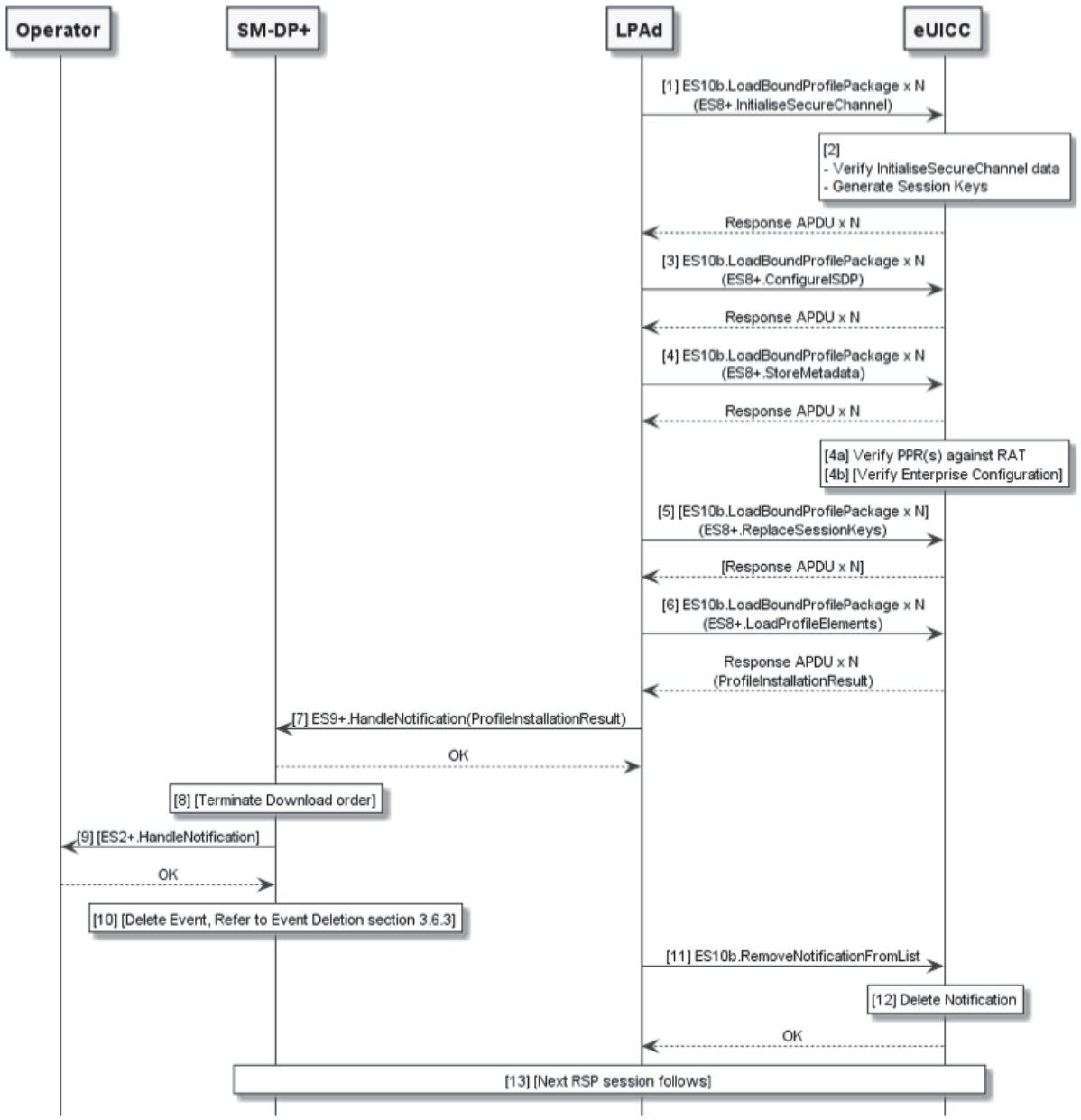


Figure 14: Sub-procedure Profile Installation

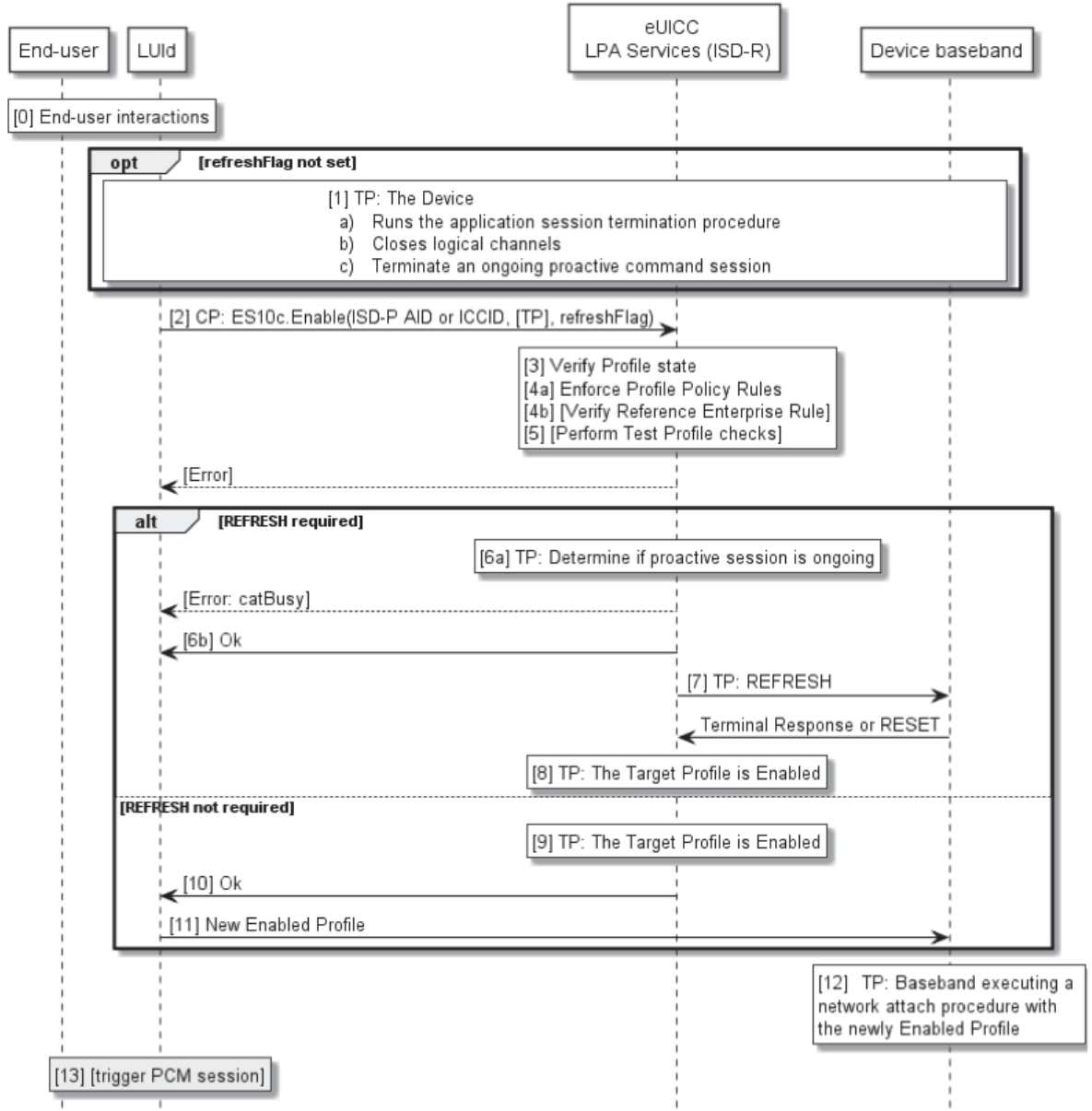


Figure 16: Enable Profile

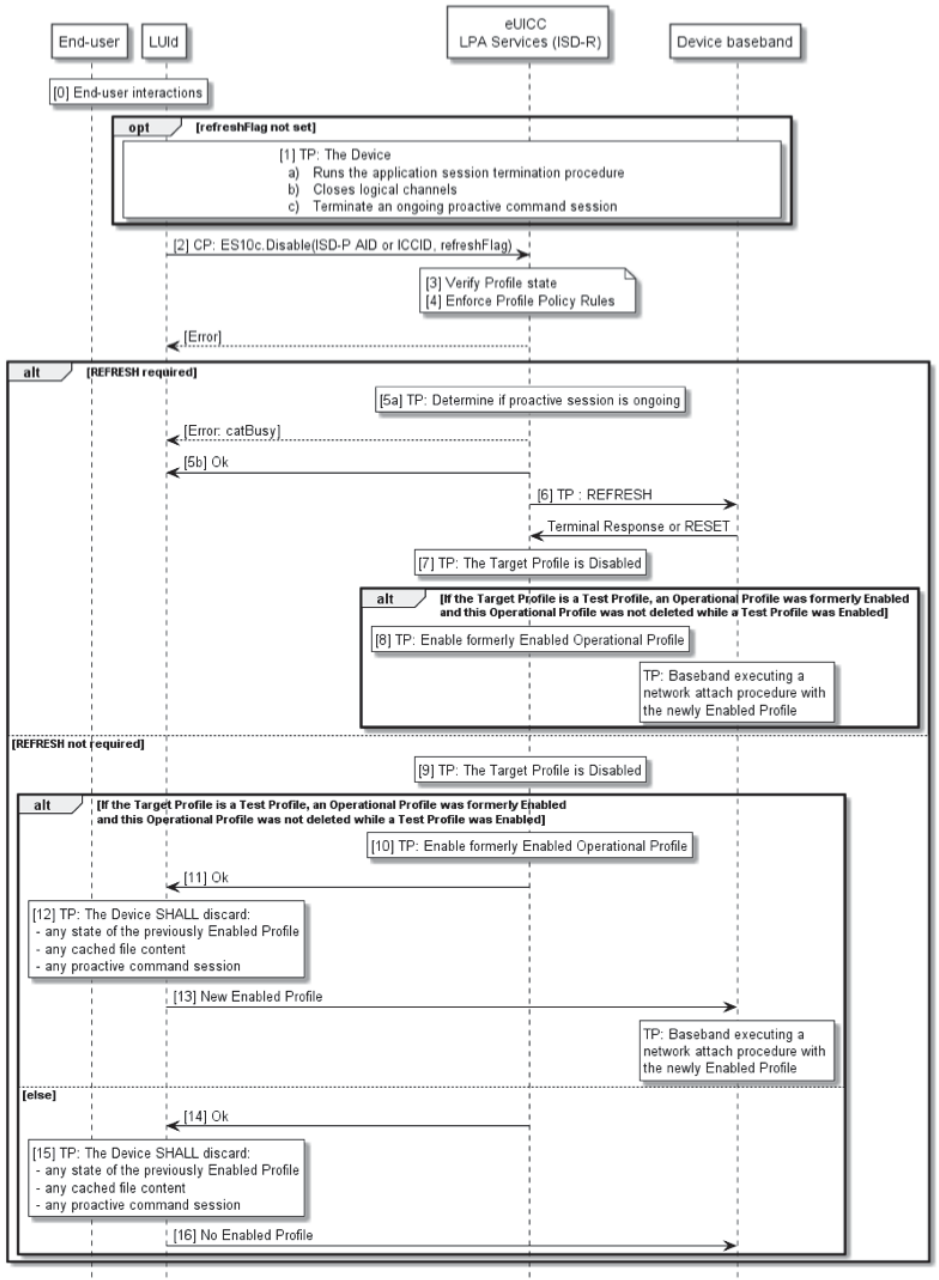


Figure 17: Disable Profile

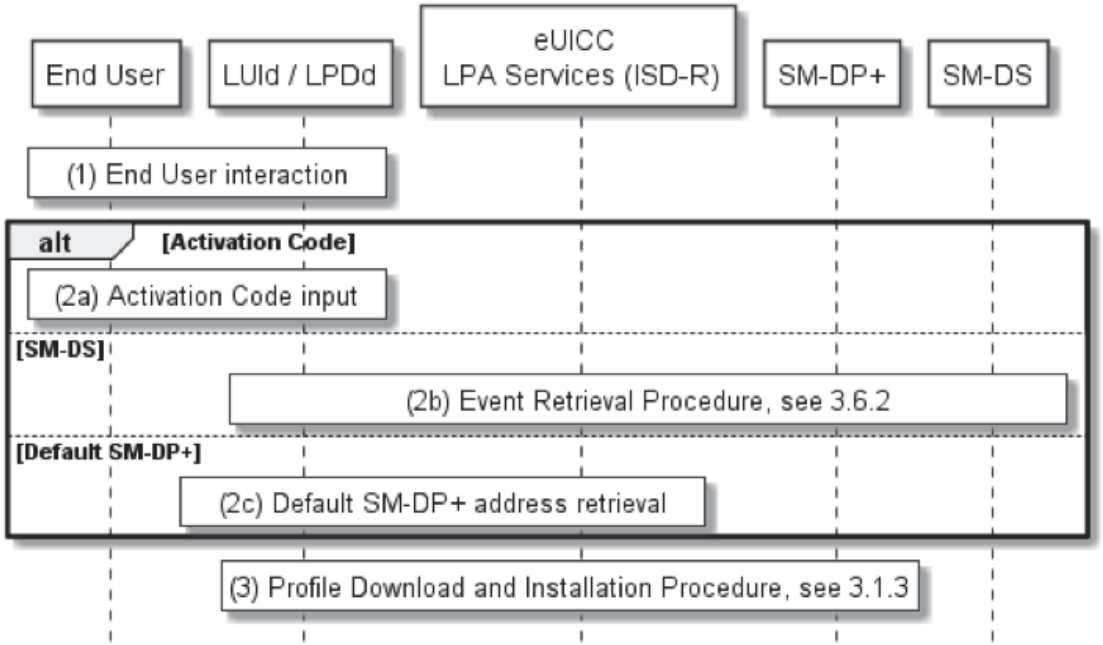


Figure 20: Add Profile

3.7 Remote Profile Management

The Operator initiates Remote Profile Management (RPM) procedure using the ES2+ interface.

RPM is executed by a Managing SM-DP+. A Profile MAY be configured to allow RPM by several Managing SM-DP+s. This specification assumes that a Managing SM-DP+ that prepares an RPM Package has full knowledge of the state of a Profile. How this state is synchronised among multiple Managing SM-DP+s, or procedures where a Managing SM-DP+ does not have full knowledge of the state of a Profile are out of the scope of this specification.

The LPA downloads an RPM Package using the ES9+ interface as described in section 3.7.2. An RPM Package MAY contain one or more RPM Commands.

Each RPM Command SHALL require Confirmation Request enforced by the LPA as described in section 3.7.2. The specific implementation of Confirmation Request by the LPA is out of scope of this specification.

Confirmation Request on multiple RPM Commands for consecutive operations MAY be combined to simplify the user experience and avoid repeated input steps for the End User. For instance, when executing two RPM Commands in an RPM Package, the Strong Confirmation for the first RPM Command and the Simple Confirmation for the second RPM Command MAY be combined. In the case of combined Confirmation Requests, it SHALL be clear to the End User what RPM Commands will be executed, and the highest Confirmation Level SHALL be obtained.

If End User accepts the execution of the RPM Package, the LPA transfers the RPM Package to the eUICC as described in section 3.7.3. The eUICC executes the RPM Command(s) contained in the RPM Package in the received order and generates the Load RPM Package Result specified in section 2.10.2.

Upon completing the execution of an RPM Package, the Operator receives the Load RPM Package Result. Based upon the outcome, the Operator can choose to initiate additional RPM operations. For instance, if a 'Contact PCMP' command resulted in a `noLprConfiguration` error, the Operator could request a new RPM Package containing both an 'Update Metadata' command with `pcmpAddress` and a 'Contact PCMP' command.

3.7.1 RPM Initiation

This procedure is used by Operator to issue an RPM Command(s).

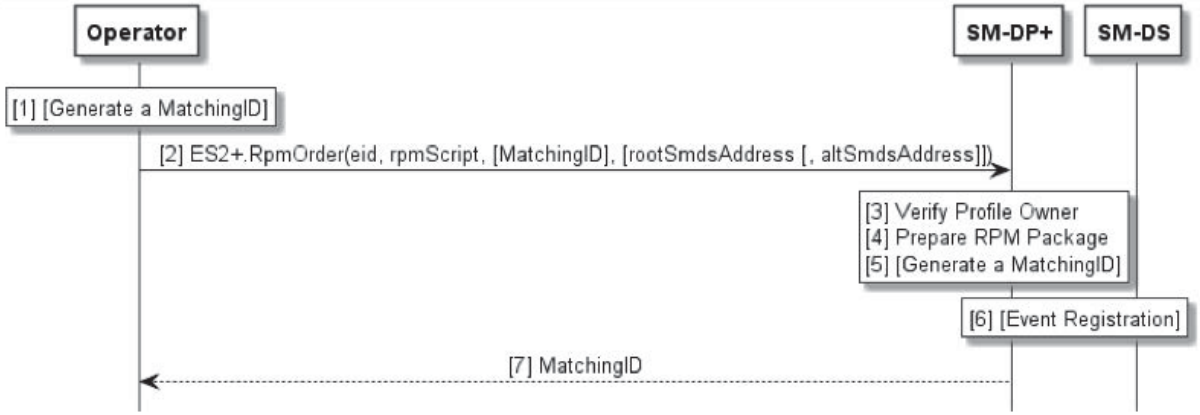


Figure 29a: RPM Initiation

Start Condition:

- The target eUICC has already installed a Profile from the Operator.
- The SM-DP+ is a Managing SM-DP+ of the target Profile.

3.7.2 RPM Download

This procedure is used by LPA to download an RPM Package and to get End User consent on RPM Execution.

The procedure applies for SEP and MEP. The following applies for Command Port:

	Command Port
MEP-A1/A2	0
MEP-B	>=0
SEP	Physical interface

All communication between the LPA and the eUICC in the RPM Download procedure SHALL use the Command Port.

3.7.3 RPM Execution

This procedure is used by LPA to transfer RPM Package to eUICC. The eUICC sequentially executes the RPM Command(s) contained in the RPM Package.

The procedure applies for SEP and MEP. The following applies for Command Port and Target Port:

	Command Port	Target Port
MEP-A1/A2	0	>0
MEP-B	As selected in the RPM Download procedure	>=0, identical to or different from Command Port
SEP	Physical interface	Physical interface

The Target Port is selected in the procedure depending on the presence of Disable or Enable commands.

3.8 Remote Management by the Operator

3.8.1 Metadata Update via ES6

This procedure is used by the Profile Owner to update Metadata of an enabled Profile.

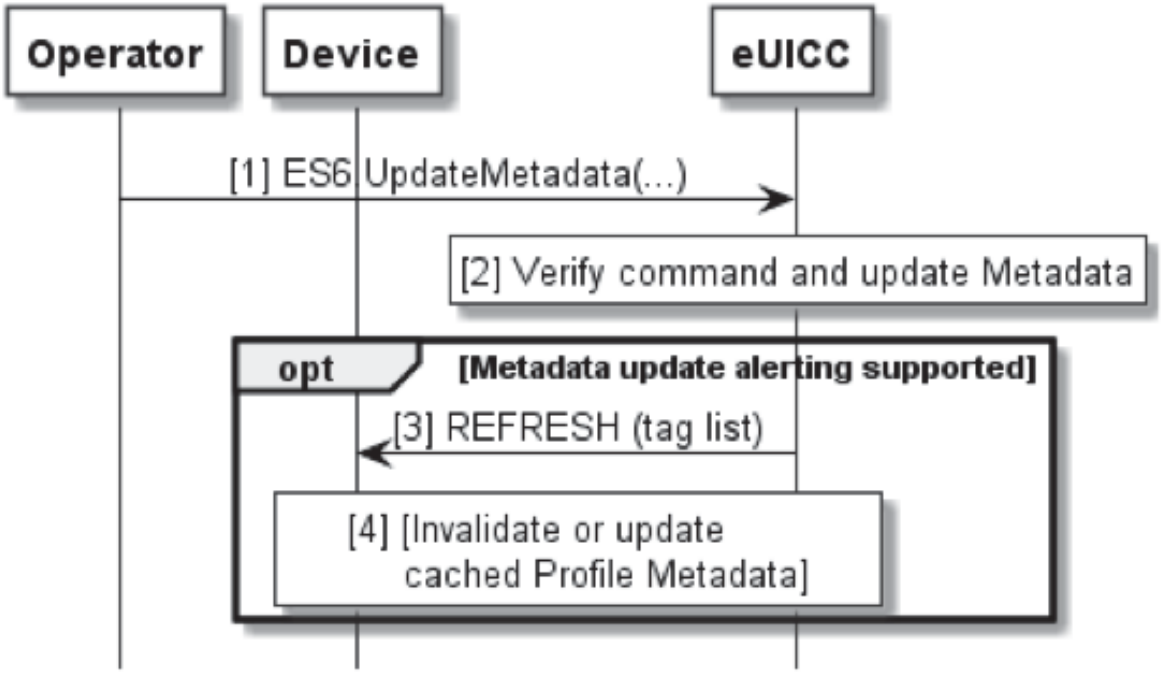


Figure 29j: Metadata Update

3.9 Profile Content Management

This procedure applies when a PCM session is triggered.

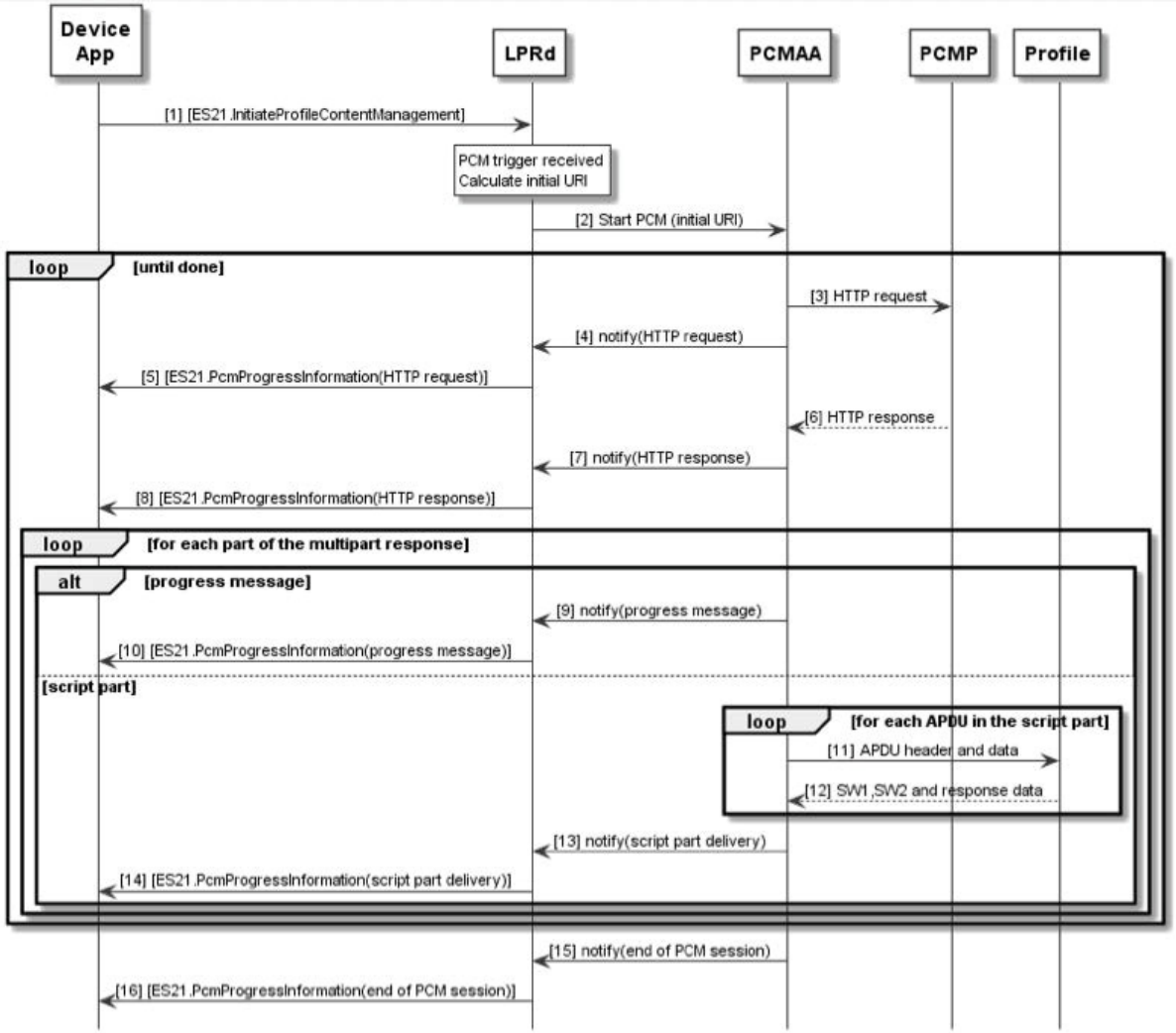


Figure 29I: Profile Content Management

	3.11 Device Change and Profile Recovery **3.11.1 Device Change** This procedure will allow the End User having a Profile in the old Device to add a Profile related to the same Subscription in the new Device. This procedure can further enable the downloaded Profile upon End User consent, which consequently MAY disable a currently Enabled Profile of the new Device (if any). Network connectivity is assumed.

Claim 3

Issued Claim(s)	Public Documentation
3. The wireless device recited in claim 2, wherein the action is to communicate with the network element.	The Accused Devices comprise the "wireless device recited in claim 2, wherein the action is to communicate with the network element." *See*, for example, the disclosures identified for claim 2 wherein a "Device" communicates with a variety of "network elements," such as "Operator[s]," "entities," and/or "server[s]" via "interfaces." *See, e.g.,* https://www.gsma.com/esim/wp-content/uploads/2022/10/SGP.22-v3.0-1.pdf:

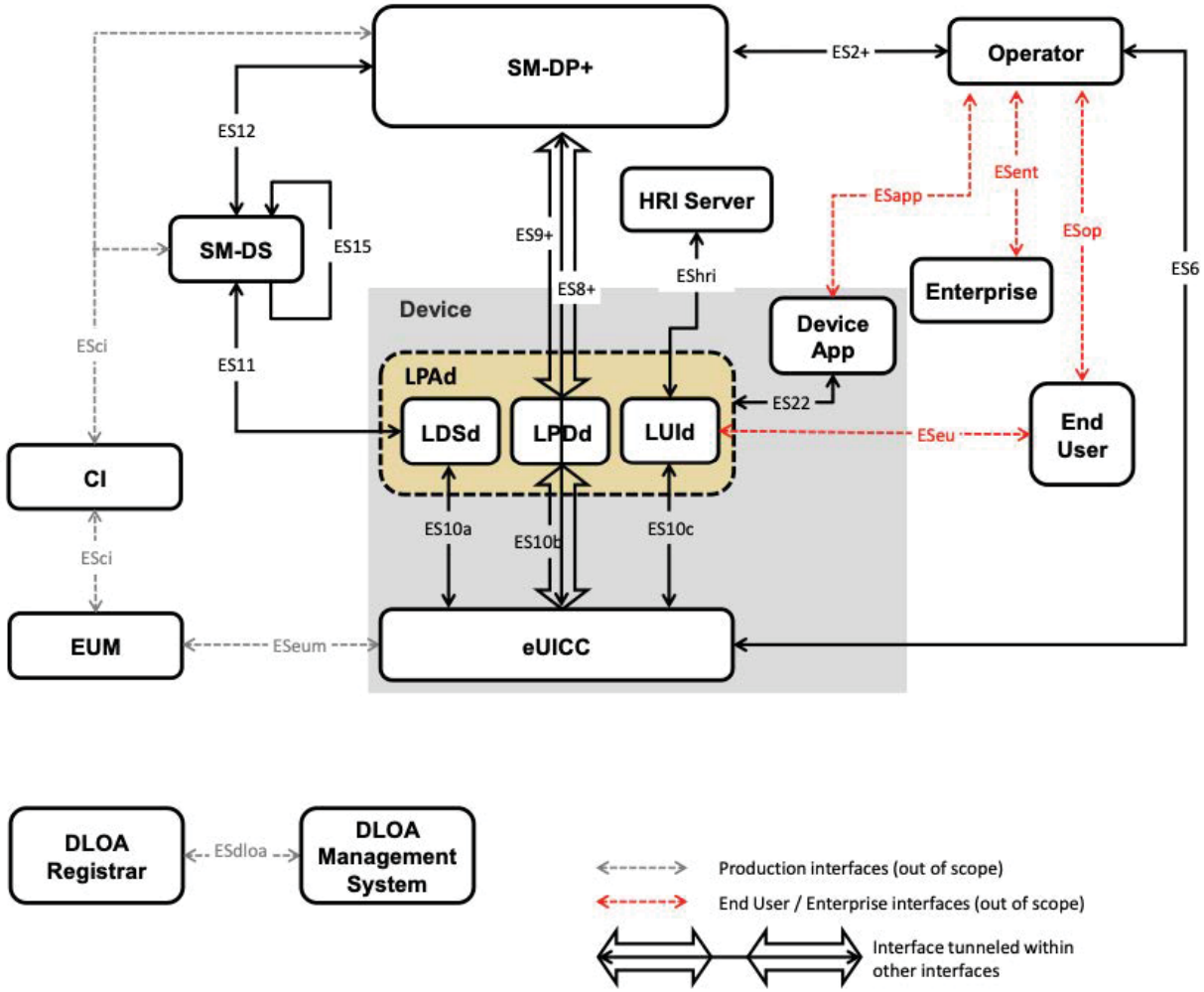


Figure 1: Remote SIM Provisioning System, LPA in the Device

Figure 1 shows the entities required for Profile Download and RPM. Figure 1a shows the additional entities required for Profile Content Management using an LPA Proxy (LPRd) and a PCM Admin Agent. The PCM Admin Agent MAY be external to the LPAd.

A Device supporting both the LPAd and the LPAe SHALL implement an appropriate mechanism that sets the LPA to be used.

The above figure provides the complete description of the consumer Remote SIM Provisioning and Management system, when LPA is in the Device (LPAd).

The Remote SIM Provisioning and Management system also allows to have the LPA in the eUICC (LPAe). This architecture is shown in the following figure.

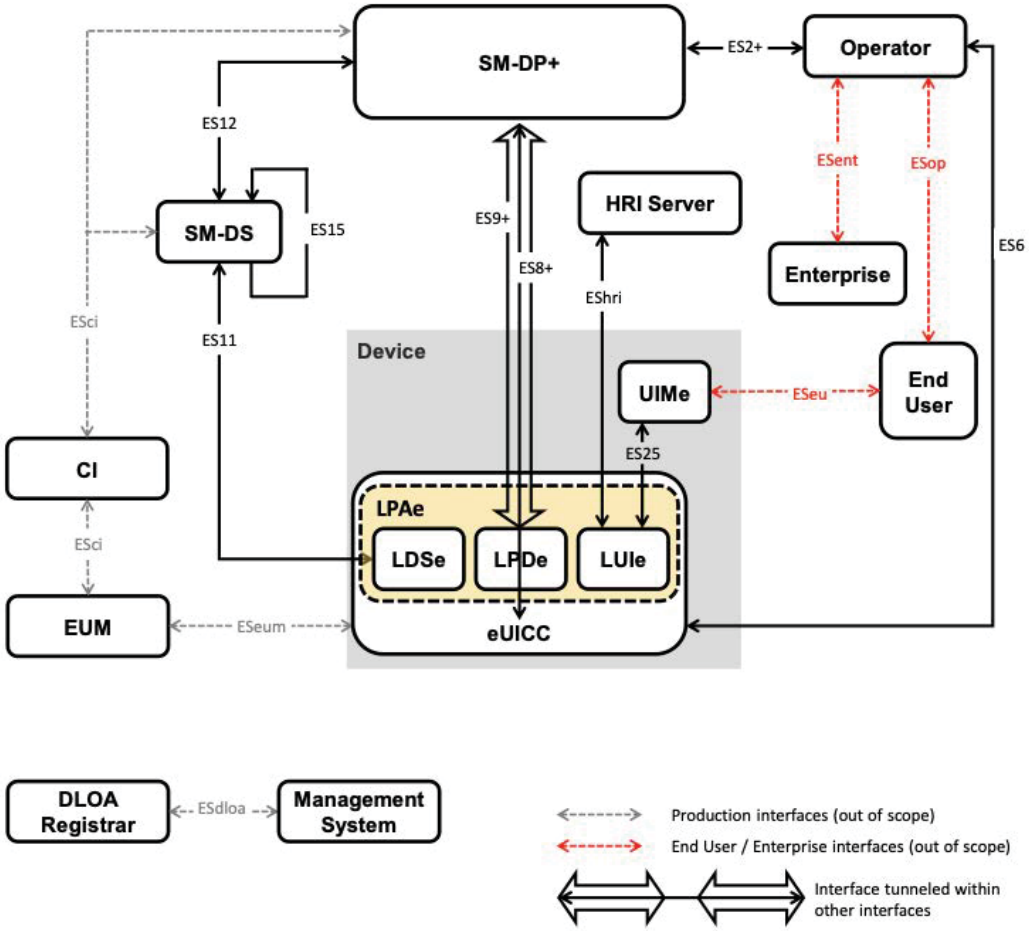


Figure 2: Remote SIM Provisioning System, LPA in the eUICC

2.3 Interfaces

The following table provides information about the interfaces within the architecture.

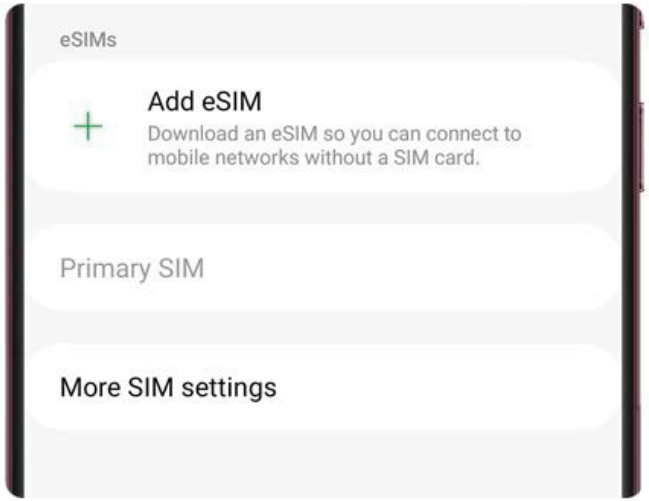
Interface	Between		Description
ES2+	Operator	SM-DP+	Used by the Operator to order Profiles for specific eUICCs as well as other administrative functions.
ES6	Operator	eUICC	Used by the Operator for the management of Operator services via OTA services.
ES8+	SM-DP+	eUICC	Provides a secure end-to-end channel between the SM-DP+ and the eUICC for the administration of the ISD-P and the associated Profile during download and installation. It provides Perfect Forward Secrecy.
ES9+	SM-DP+	LPD	Used to provide a secure transport between the SM-DP+ and the LPA (LPD) for Profile Download, RPM, etc.
ES10a	LDSd	eUICC	Used between the LDSd and the LPA Services to handle a Profile discovery.
ES10b	LPDd	eUICC	Used between the LPDd and the LPA services to transfer a Bound Profile Package to the eUICC. This interface plays no role in the decryption of Profile Packages.
ES10c	LUId	eUICC	Used between the LUId and the LPA services for Local Profile Management by the End User.
ES11	LDS	SM-DS	Used by the LDS to retrieve Event Records for the respective eUICC.
ES12	SM-DP+	SM-DS	Used by the SM-DP+ to register Event Records with the SM-DS and to delete its Event Records.
ES15	SM-DS	SM-DS	Used in the case of deployments of cascaded SM-DSs to connect those SM-DSs.
ES20	PCMP	PCMAA	Used to send APDU scripts enhanced by additional information.
ES21	Device Application	LPRd	Used to trigger the PCMAA and to send PCM notifications to the Device Application.
ES22	Device Application	LPAd	Used by a Device Application to interwork with the LPA (out of scope of this specification).
ES25	UIMe	LUIe	Used between the UIMe and the LUIe to transfer End User related interaction.
ESaa	PCMAA	enabled Profile	Used to select an application of the Enabled Profile and to exchange APDUs subsequently. Identical to the interface between the Admin Agent and the Secure Element

Interface	Between		Description
			defined in GP SERAM [74] and not further described in this specification.
ESapp	Operator	Device Application	Interface between the Operator and the Device Application (out of scope of this specification). NOTE: an example of a protocol that can be used on ESapp can be found in [i1].
EShri	LUI	HRI Server	Used to retrieve High Resolution Icons.
ESop	Operator	End User	Business interface between Operator and End user (out of scope of this specification).
ESent	Operator	Enterprise	Interface between the Operator and the Enterprise (out of scope of this specification).
ESeu	End User	LUI	Interface to initiate local profile management functions (out of scope of this specification).
ESeum	eUICC	EUM	Administrative interface between the eUICC vendor (EUM) and the eUICC (out of scope of this specification).
ESci	CI	SM-DP+ SM-DS EUM	This interface is used by the SM-DP+, SM-DS and EUM to request a certificate and retrieve certificate revocation status. Any other relying party MAY retrieve certificate revocation status. The interface for Certificate Signing Request is defined in SGP.14 [45] section 5.1. The interface for CRL retrieval is defined in the present document, section 4.5.2.1.2 "Extension CRL Distribution Points".
ESdloa	DLOA Registrar	Management System	This interface is defined in GlobalPlatform DLOA [57] section 5.
ESdsps	SM-DS	push server	Interface between SM-DS and push server (out of scope of this specification).
ESps	push server	push client	Interface between push server and push client (out of scope of this specification).
ESpc	push client	LPAd	Interface between push client and LPAd (out of scope of this specification).

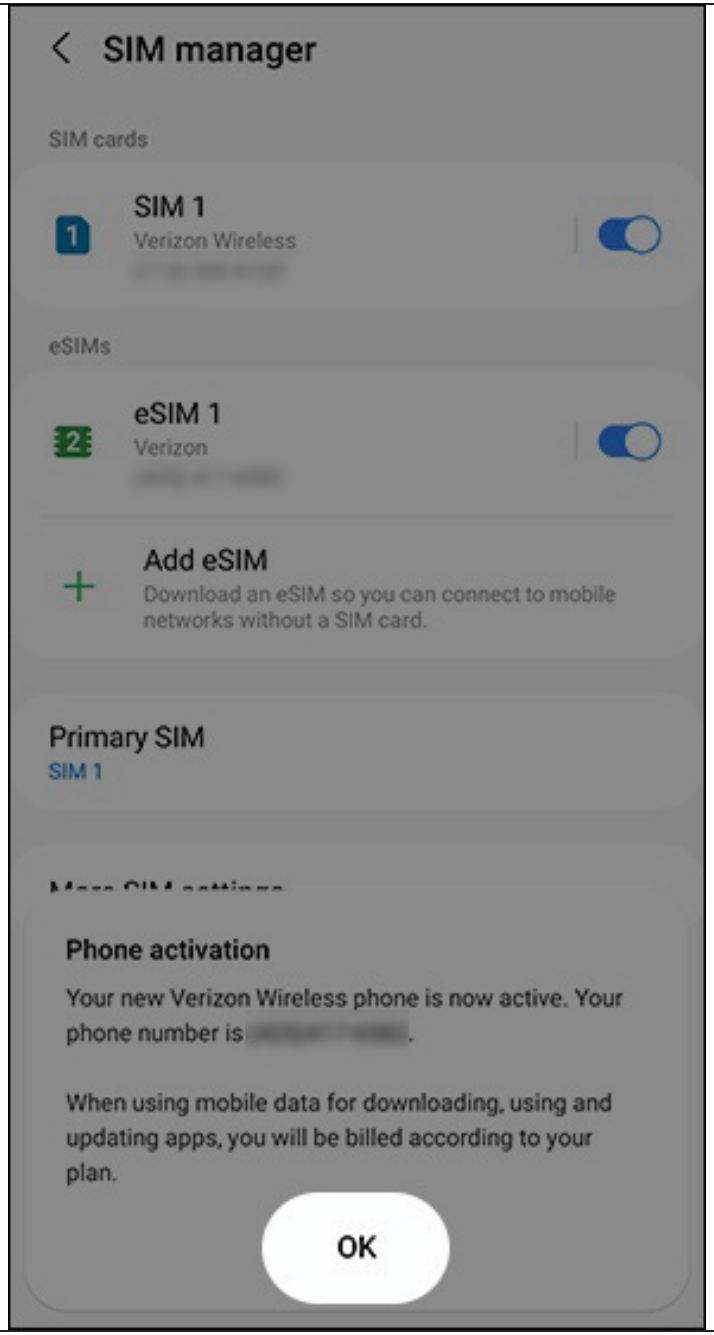
Table 1: Interfaces

Claim 4

Issued Claim(s)	Public Documentation
4. The wireless device recited in claim 2, wherein the action is to cause a notification to be presented through the user interface, wherein the notification reports an error.	The Accused Devices comprise the "wireless device recited in claim 2, wherein the action is to cause a notification to be presented through the user interface, wherein the notification reports an error." *See*, for example, the disclosures identified for claim 2. For further example, the Accused Devices comprise a user interface where notifications can be presented. *See, e.g.,* https://www.samsung.com/us/support/answer/ANS10001619/ (referring to

	carrier's instructions for using eSIM): An eSIM is an embedded version of the physical SIM card on the device. The eSIM provides connection to your carrier's network, however instead of inserting a card, you will activate it with your carrier account information. You can also use the eSIM alongside a physical SIM to add a second phone number or carrier to your device. **1** Navigate to and open **Settings**, and then tap **Connections**. **2** Tap **SIM manager**. From here, you can tap the **switch** next to your physical SIM or activated eSIM to enable or disable their connections. You can also tap **Primary SIM** to change the default connection for making calls, sending texts, and using data. 

	; https://www.samsung.com/my/support/mobile-devices/using-your-galaxy-smartphones-with-esim/; *see also* https://www.verizon.com/support/knowledge-base-240165/:


SIM manager
SIM cards
SIM 1
Verizon Wireless
eSIMs
eSIM 1
Verizon
Add eSIM
Download an eSIM so you can connect to mobile networks without a SIM card.
Primary SIM
SIM 1
Phone activation
Your new Verizon Wireless phone is now active. Your phone number is .
When using mobile data for downloading, using and updating apps, you will be billed according to your plan.
OK

	; https://www.att.com/support/how-to/wireless/esim-get-started/: **Samsung smartphone** Just turn on your phone and follow the setup prompts. If you have wireless service bars or you can make a call, you're all set. Don't have service? Look for a notification to add your eSIM or go to your phone **Settings.** Tap **Connections,** then **SIM manager** and **Add eSIM.** Having trouble? Get more details for Samsung eSIMs. ; https://www.t-mobile.com/support/devices/device-troubleshooting/samsung-on-device-activation-troubleshooting

Phone with Dual SIM

Get help if you can't activate your eSIM. For help with these steps, pick your device on the **Device tutorials** page and use the search bar.

1. If the device wasn't purchased from T-Mobile, make sure that it's unlocked.
2. Make sure you're connected to a Wi-Fi network and the internet works.
3. Update the device software to the latest version.
4. Restart your device and try again.
5. Select the specific errors that you're getting and follow any steps.

Error 506: No internet connection

- The device is unable to connect to the internet over Wi-Fi.
- Make sure you're connected to Wi-Fi and can access the internet, then try again.

Error 507: Permission needed

- This means you're not authorized to make changes on the account.
- Have the primary account holder log in using their T-Mobile ID when activating.

Error 511: Assistance required to transfer eSIM

Self-serve path to transfer eSIM is unavailable. **Contact us** to set up the eSIM on your device.

Error 518: Your account has a security restriction

A security restriction is preventing the eSIM activation. Make sure you've turned off **SIM Protection**, then **contact us** for help.

Error 519: This number has SIM Protection on

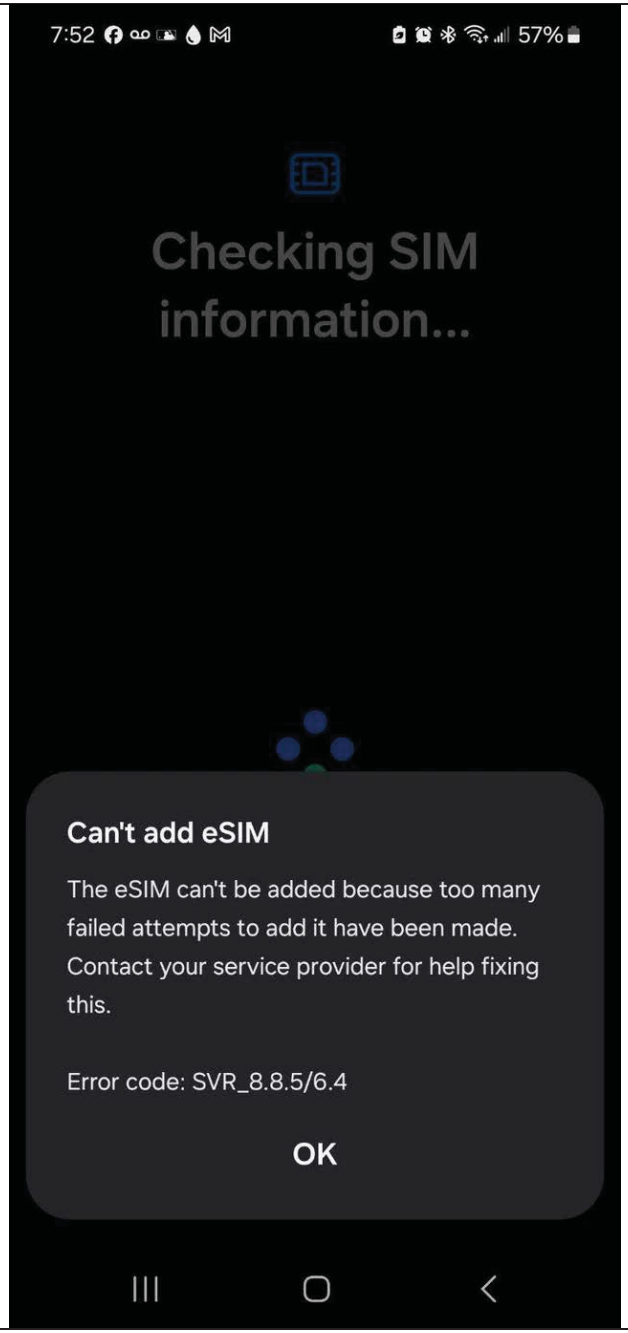
SIM Protection is preventing eSIM activation. Log into your T-Mobile account to remove the feature and try again.

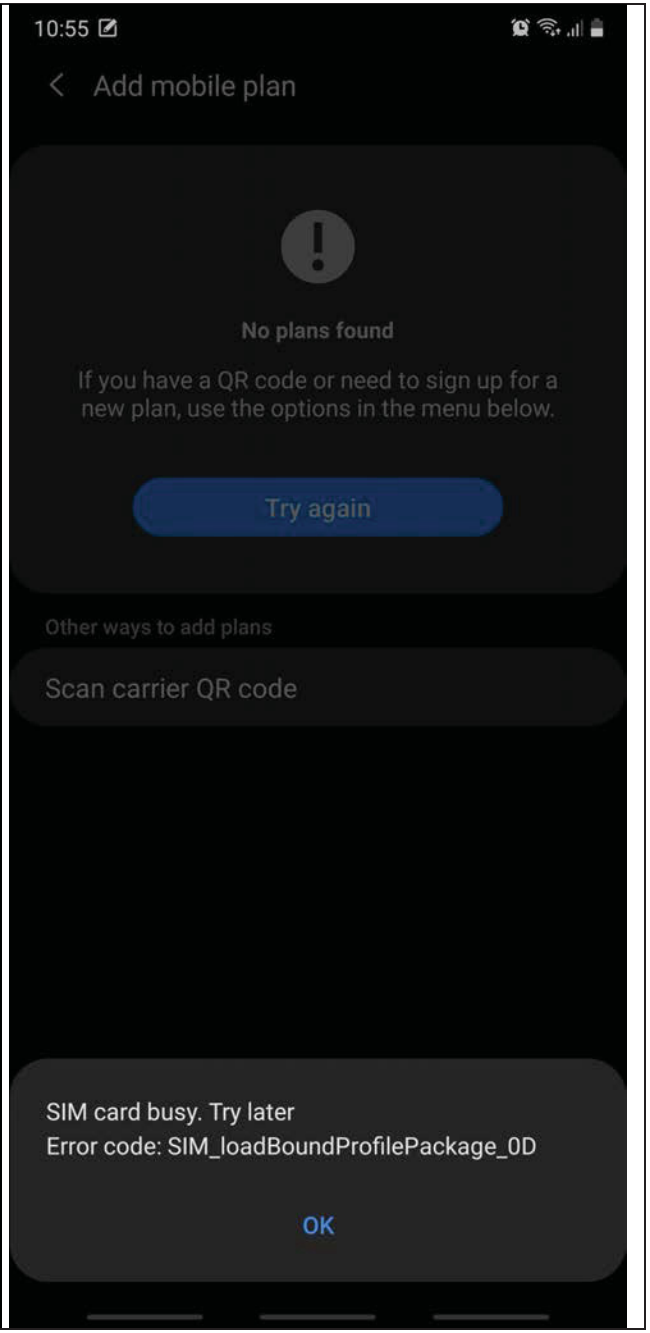
The number you entered isn't on your account

- The number you entered isn't associated to the T-Mobile ID you used to log in.
- Log in with the T-Mobile ID associated with the number you want to activate.

; https://www.t-mobile.com/support/tutorials/device/samsung/galaxy-s23-plus/topic/esim/activating-esim/36; https://source.android.com/docs/core/connect/esim-euicc-api; https://source.android.com/docs/core/connect/esim-error-handling; https://source.android.com/docs/core/connect/esim-mep; https://source.android.com/docs/core/connect/esim-overview:

	Resolvable errors There are some cases where the system is unable to complete the eSIM operation but the error can be resolved by the user. For example, `downloadSubscription` may fail if the profile metadata indicates that a *carrier confirmation code* is required. Or `switchToSubscription` may fail if the carrier app has carrier privileges over the destination profile (that is, carrier owns the profile) but doesn't have carrier privileges over the currently enabled profile, and hence user consent is required. For these cases, the caller's callback is called with `EuiccManager#EMBEDDED_SUBSCRIPTION_RESULT_RESOLVABLE_ERROR`. The callback `Intent` contains internal extras such that when the caller passes it to `EuiccManager#startResolutionActivity`, resolution can be requested through the LUI. Using the confirmation code for example again, `EuiccManager#startResolutionActivity` triggers an LUI screen that allows the user to enter a confirmation code; after the code is entered, the download operation is resumed. This approach provides the carrier app with full control over when the UI is shown, but gives the LPA/LUI an extensible method for adding new handling of user-recoverable issues in the future without needing client apps to change. *See also* exemplary screenshot:


7:52
57%
Checking SIM information...
Can't add eSIM
The eSIM can't be added because too many failed attempts to add it have been made. Contact your service provider for help fixing this.
Error code: SVR_8.8.5/6.4
OK


10:55
Add mobile plan
No plans found
If you have a QR code or need to sign up for a new plan, use the options in the menu below.
Try again
Other ways to add plans
Scan carrier QR code
SIM card busy. Try later
Error code: SIM_loadBoundProfilePackage_0D
OK

Claim 5

Issued Claim(s)	Public Documentation
5. The wireless device recited in claim 2, wherein the action is to cause a notification to be presented through the user interface, wherein the notification reports that a procedure is in progress or has not been completed.	The Accused Devices comprise the "wireless device recited in claim 2, wherein the action is to cause a notification to be presented through the user interface, wherein the notification reports that a procedure is in progress or has not been completed." *See*, for example, the disclosures identified for claims 2 and 4.

Claim 6

Issued Claim(s)	Public Documentation
6. The wireless device recited in claim 2, wherein the action is to at least assist in restricting communications by the wireless device over the wireless access network.	The Accused Devices comprise the "wireless device recited in claim 2, wherein the action is to at least assist in restricting communications by the wireless device over the wireless access network." *See*, for example, the disclosures identified for claim 2.

Claim 7

Issued Claim(s)	Public Documentation
7. The wireless device recited in claim 1, wherein, when executed by the one or more processors, the one or more machine-executable instructions further cause the one or more processors to:	The Accused Devices comprise the "wireless device recited in claim 1, wherein, when executed by the one or more processors, the one or more machine-executable instructions further cause the one or more processors to." *See*, for example, the disclosures identified for claim 1.
determine that the updated credential matches the target credential, and based on the determination that the updated	The Accused Devices "determine that the updated credential matches the target credential, and based on the determination that the updated credential matches the target credential, take an action."

credential matches the target credential, take an action.	*See*, for example, the disclosures identified for claim 1. For further example, the Accused Devices take an action (e.g., downloading, installing updating, enabling, disabling, or deleting) when credentials match. *See, e.g.,* https://www.gsma.com/esim/wp-content/uploads/2022/10/SGP.22-v3.0-1.pdf:

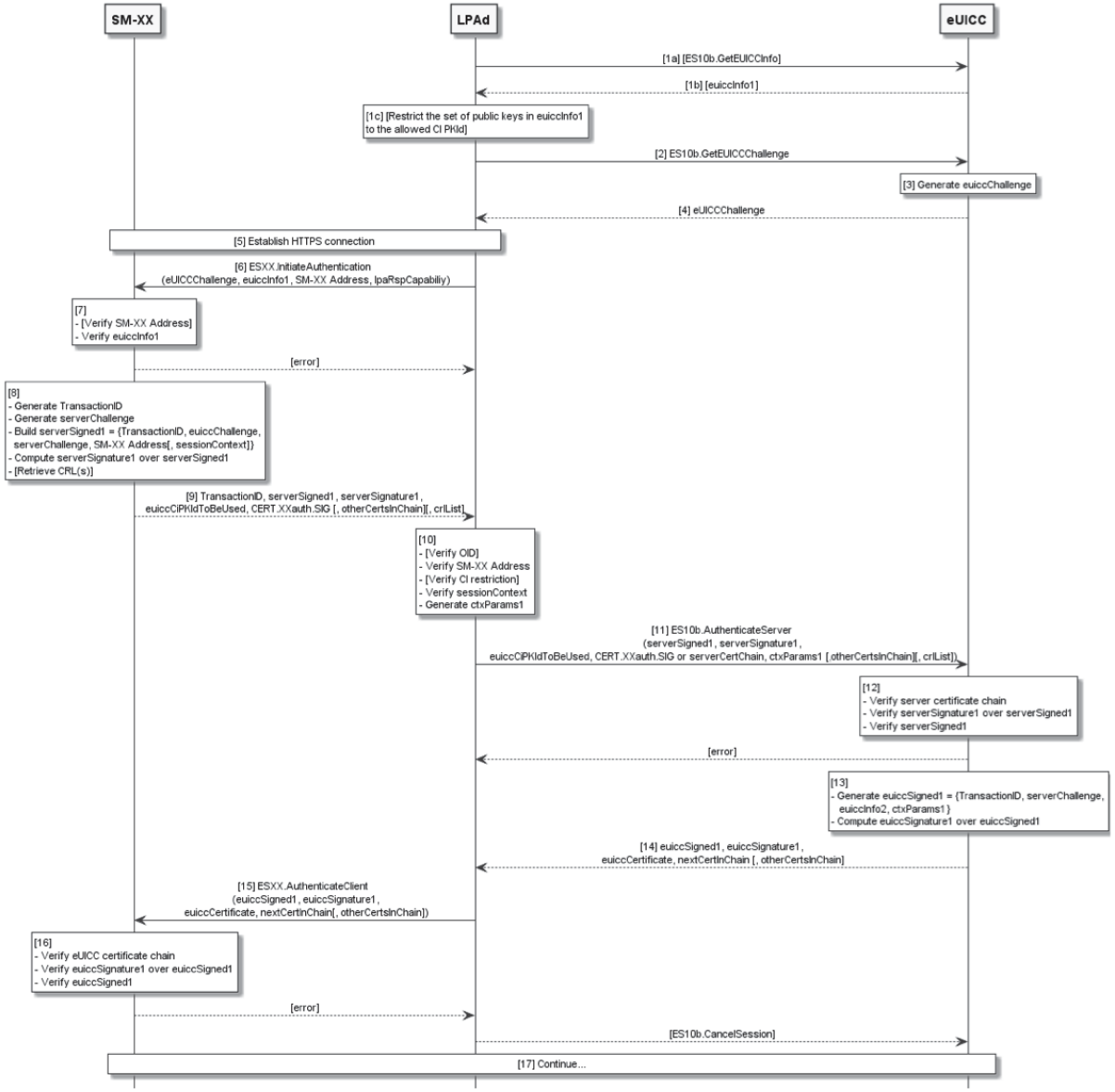


Figure 8a: Common Mutual Authentication Procedure

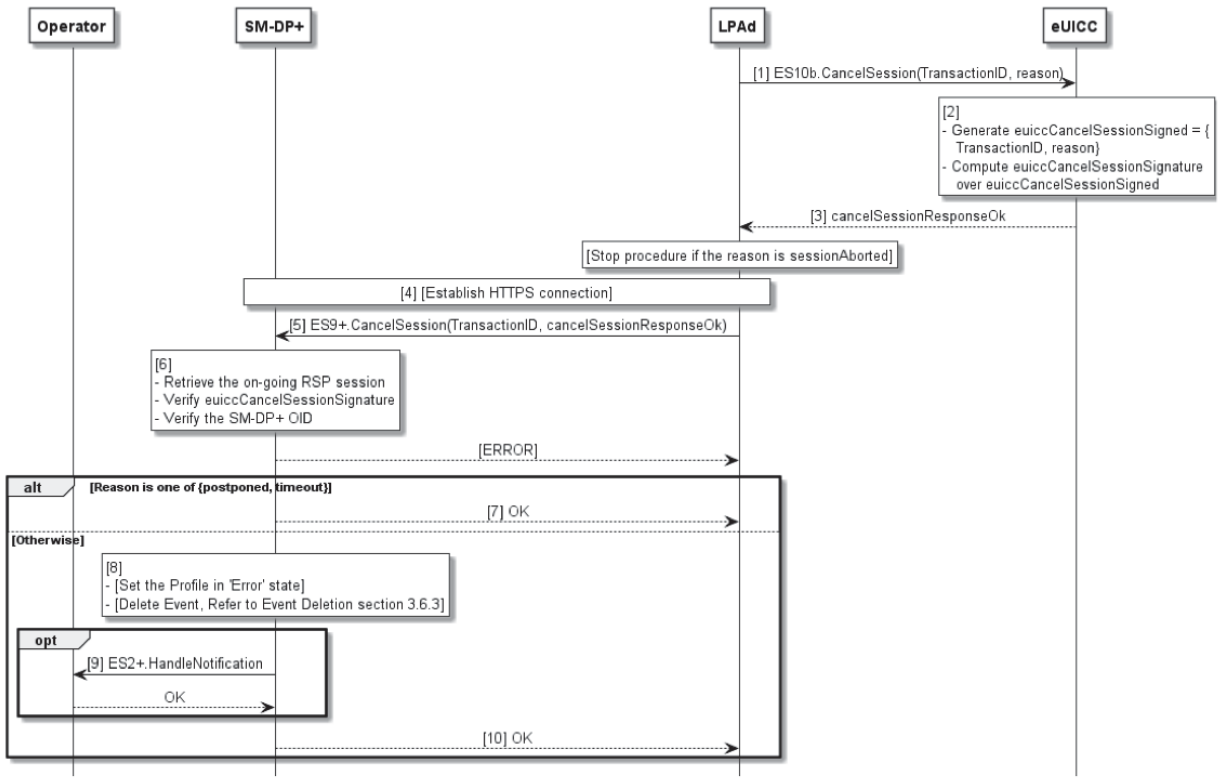


Figure 8b: Common Cancel Session Procedure

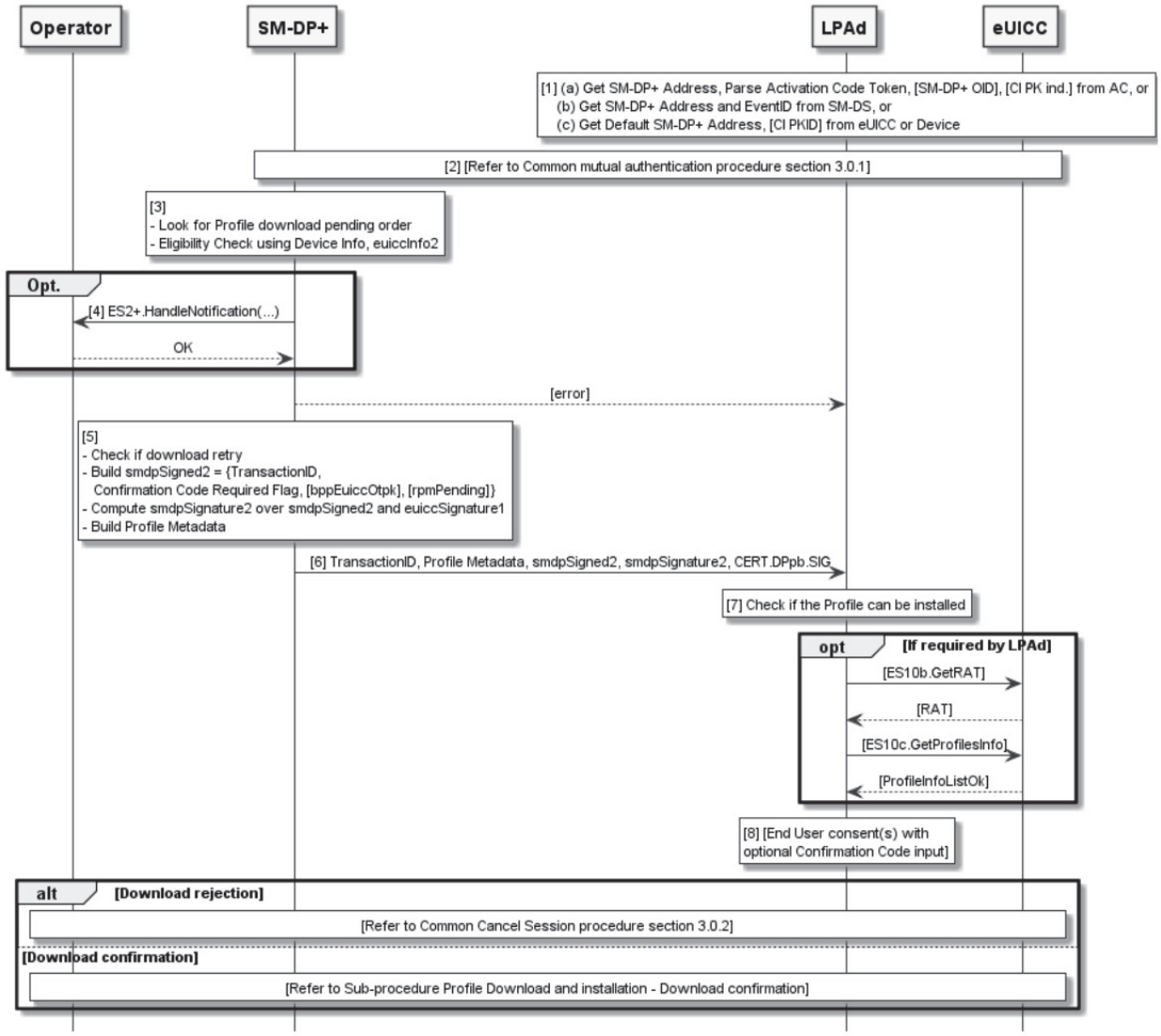


Figure 11: Profile Download and Installation

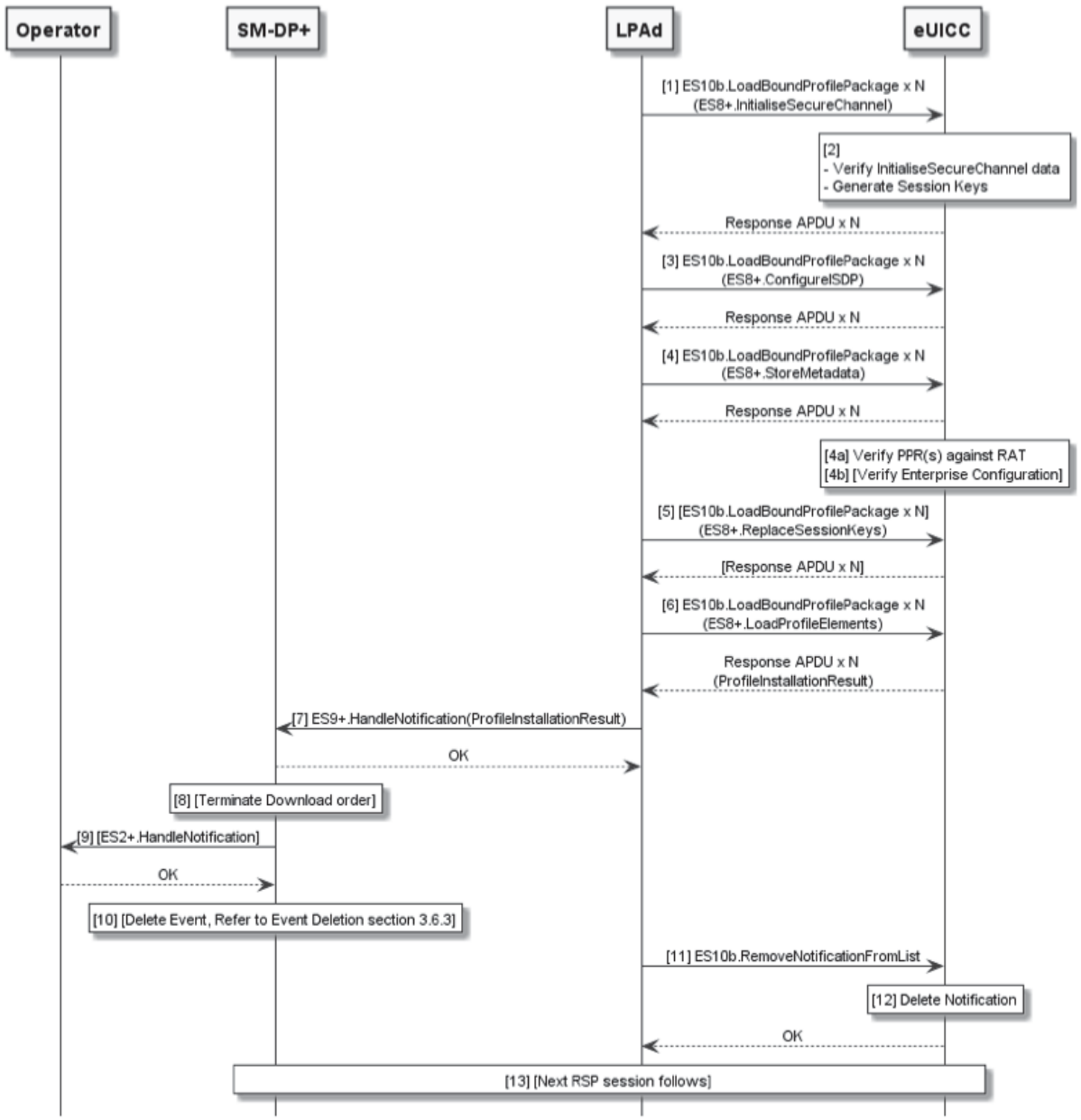


Figure 14: Sub-procedure Profile Installation

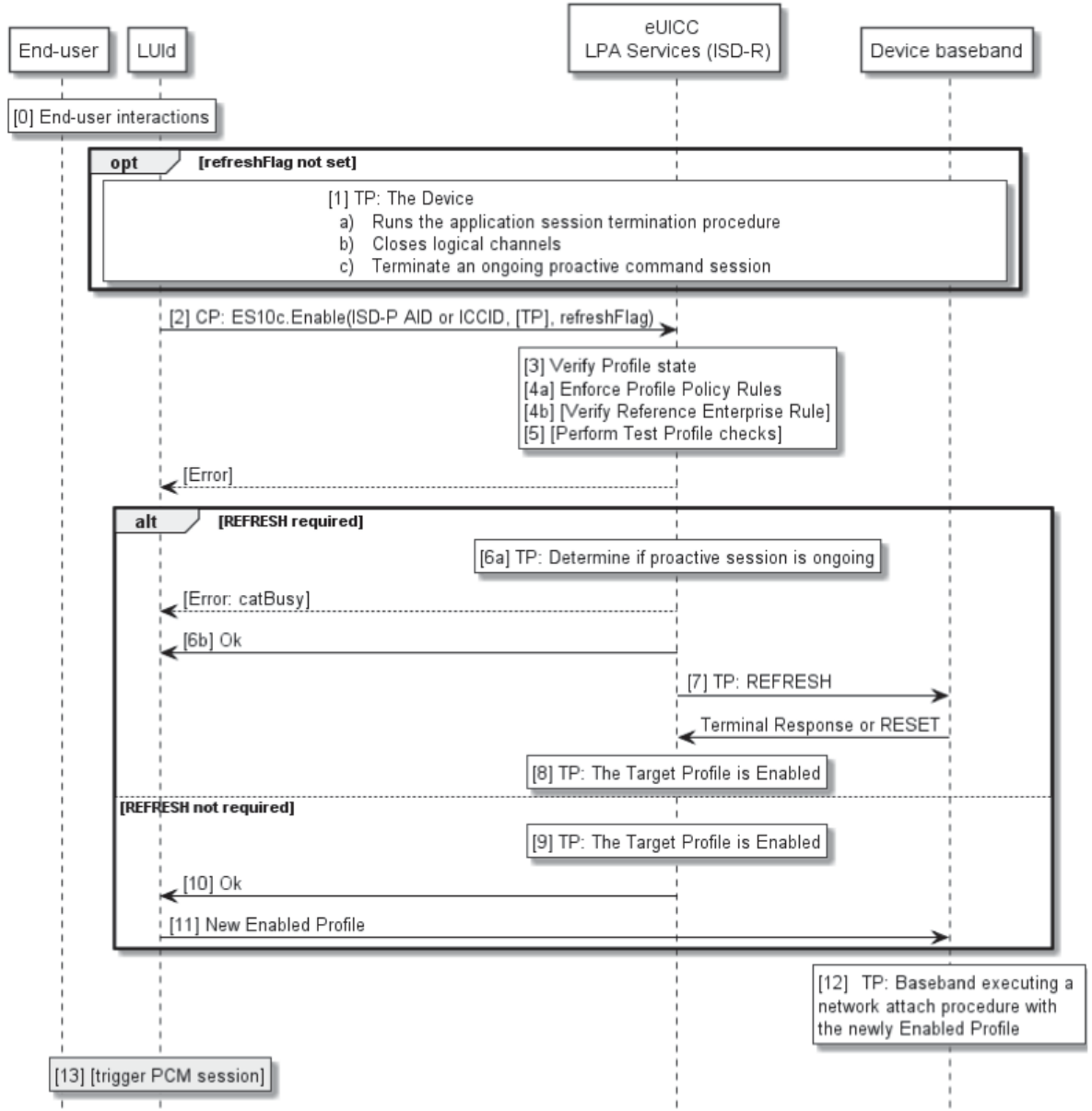


Figure 16: Enable Profile

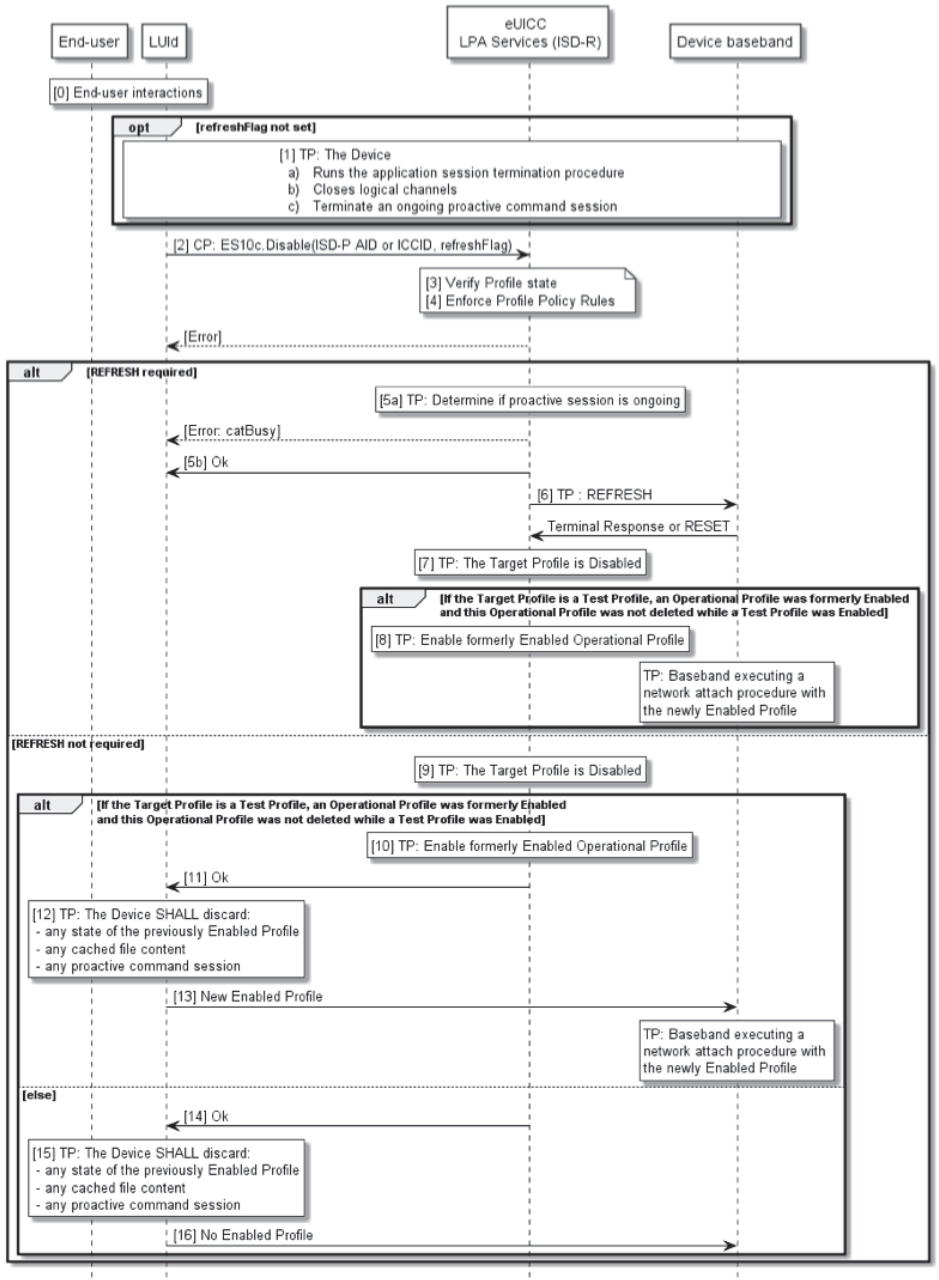


Figure 17: Disable Profile

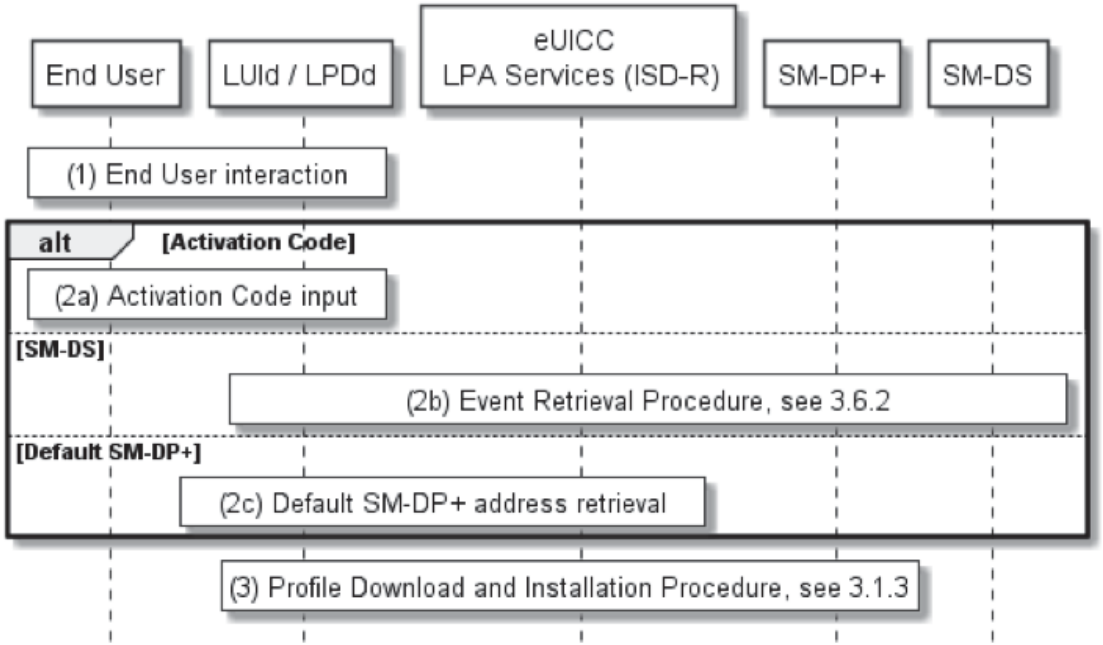


Figure 20: Add Profile

3.7 Remote Profile Management

The Operator initiates Remote Profile Management (RPM) procedure using the ES2+ interface.

RPM is executed by a Managing SM-DP+. A Profile MAY be configured to allow RPM by several Managing SM-DP+s. This specification assumes that a Managing SM-DP+ that prepares an RPM Package has full knowledge of the state of a Profile. How this state is synchronised among multiple Managing SM-DP+s, or procedures where a Managing SM-DP+ does not have full knowledge of the state of a Profile are out of the scope of this specification.

The LPA downloads an RPM Package using the ES9+ interface as described in section 3.7.2. An RPM Package MAY contain one or more RPM Commands.

Each RPM Command SHALL require Confirmation Request enforced by the LPA as described in section 3.7.2. The specific implementation of Confirmation Request by the LPA is out of scope of this specification.

Confirmation Request on multiple RPM Commands for consecutive operations MAY be combined to simplify the user experience and avoid repeated input steps for the End User. For instance, when executing two RPM Commands in an RPM Package, the Strong Confirmation for the first RPM Command and the Simple Confirmation for the second RPM Command MAY be combined. In the case of combined Confirmation Requests, it SHALL be clear to the End User what RPM Commands will be executed, and the highest Confirmation Level SHALL be obtained.

If End User accepts the execution of the RPM Package, the LPA transfers the RPM Package to the eUICC as described in section 3.7.3. The eUICC executes the RPM Command(s) contained in the RPM Package in the received order and generates the Load RPM Package Result specified in section 2.10.2.

Upon completing the execution of an RPM Package, the Operator receives the Load RPM Package Result. Based upon the outcome, the Operator can choose to initiate additional RPM operations. For instance, if a 'Contact PCMP' command resulted in a `noLprConfiguration` error, the Operator could request a new RPM Package containing both an 'Update Metadata' command with `pcmpAddress` and a 'Contact PCMP' command.

3.7.1 RPM Initiation

This procedure is used by Operator to issue an RPM Command(s).

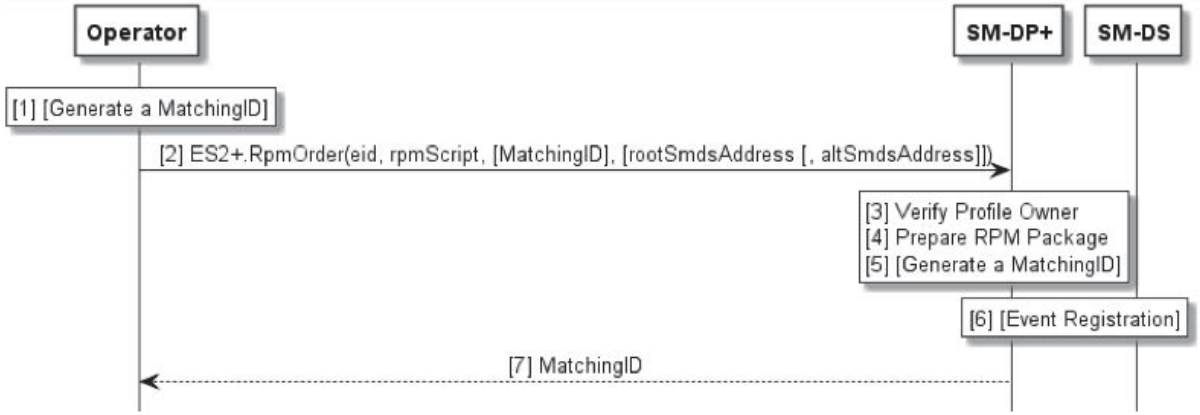


Figure 29a: RPM Initiation

Start Condition:

- The target eUICC has already installed a Profile from the Operator.
- The SM-DP+ is a Managing SM-DP+ of the target Profile.

3.7.2 RPM Download

This procedure is used by LPA to download an RPM Package and to get End User consent on RPM Execution.

The procedure applies for SEP and MEP. The following applies for Command Port:

	Command Port
MEP-A1/A2	0
MEP-B	>=0
SEP	Physical interface

All communication between the LPA and the eUICC in the RPM Download procedure SHALL use the Command Port.

3.7.3 RPM Execution

This procedure is used by LPA to transfer RPM Package to eUICC. The eUICC sequentially executes the RPM Command(s) contained in the RPM Package.

The procedure applies for SEP and MEP. The following applies for Command Port and Target Port:

	Command Port	Target Port
MEP-A1/A2	0	>0
MEP-B	As selected in the RPM Download procedure	>=0, identical to or different from Command Port
SEP	Physical interface	Physical interface

The Target Port is selected in the procedure depending on the presence of Disable or Enable commands.

3.8 Remote Management by the Operator

3.8.1 Metadata Update via ES6

This procedure is used by the Profile Owner to update Metadata of an enabled Profile.

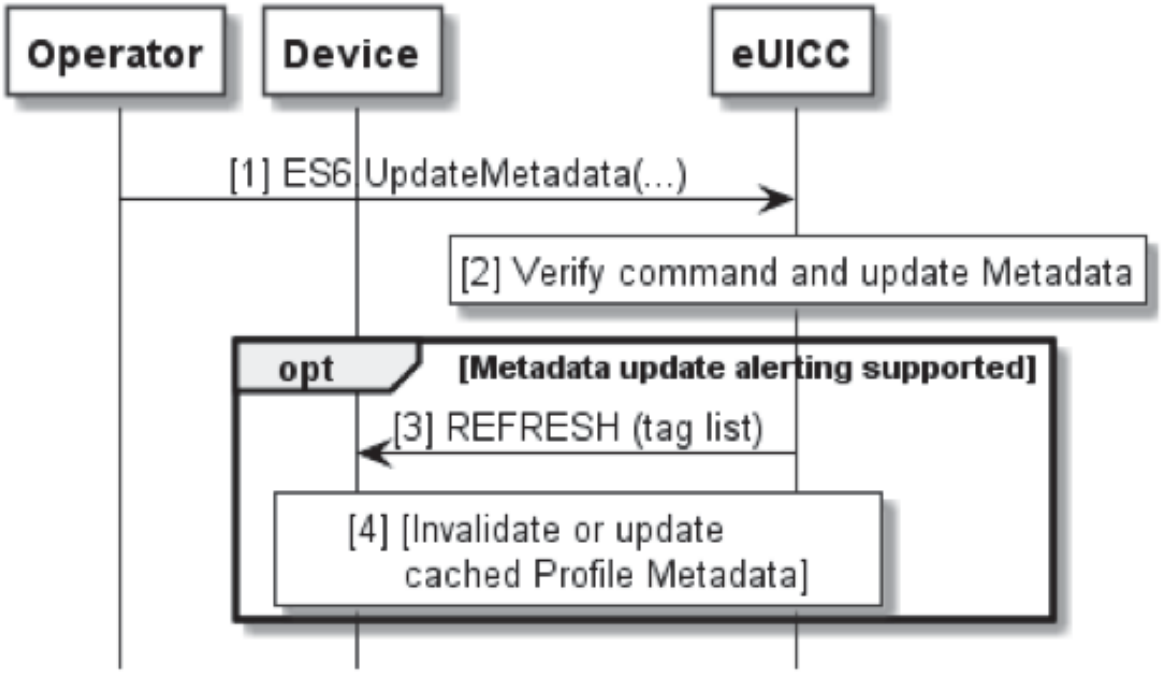


Figure 29j: Metadata Update

3.9 Profile Content Management

This procedure applies when a PCM session is triggered.

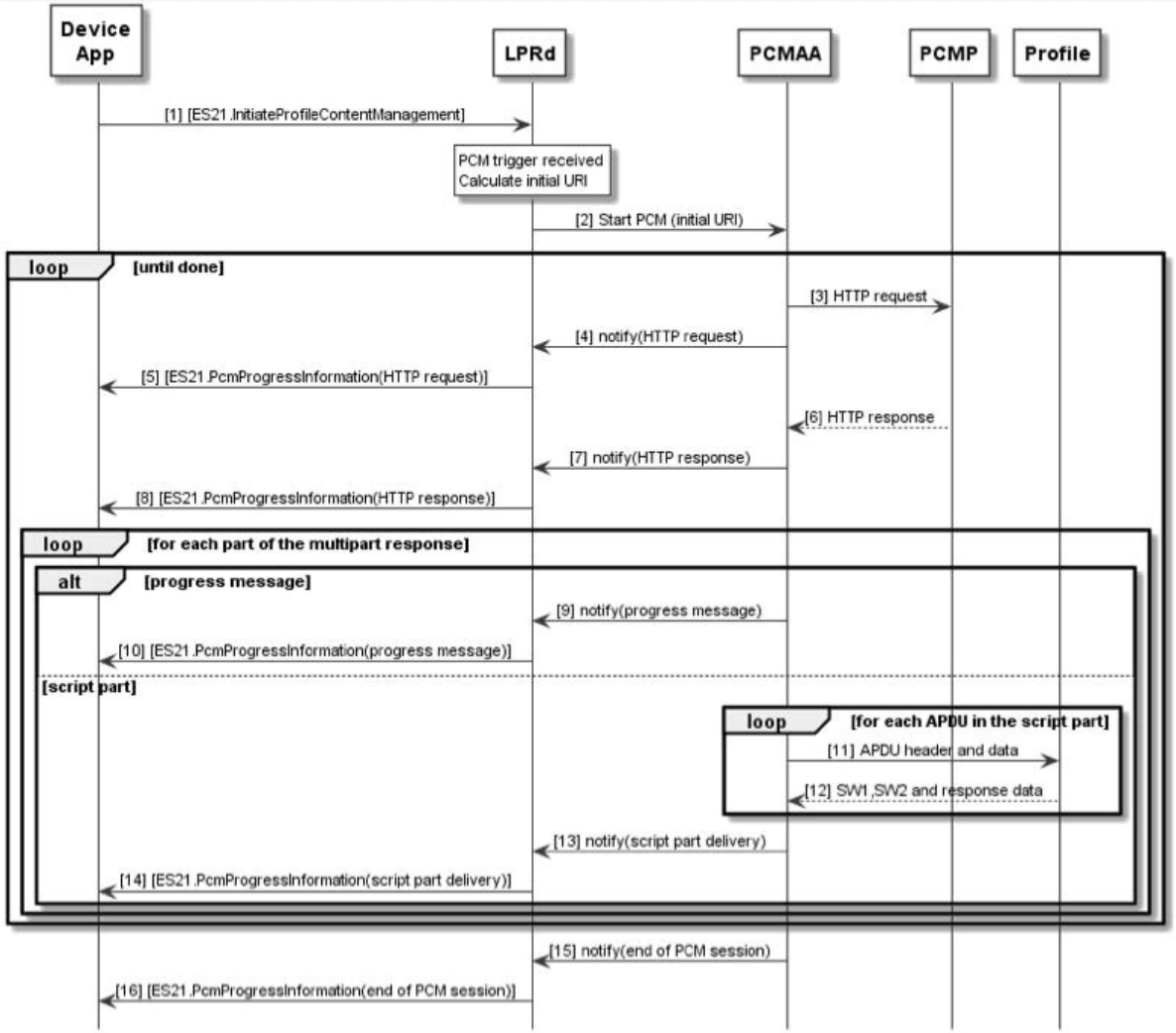
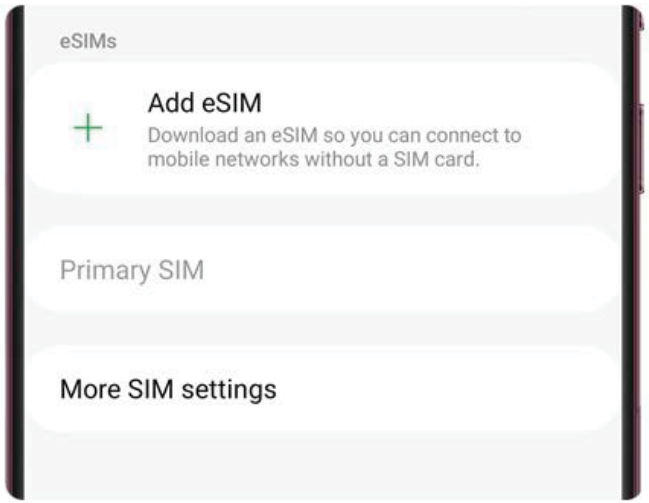


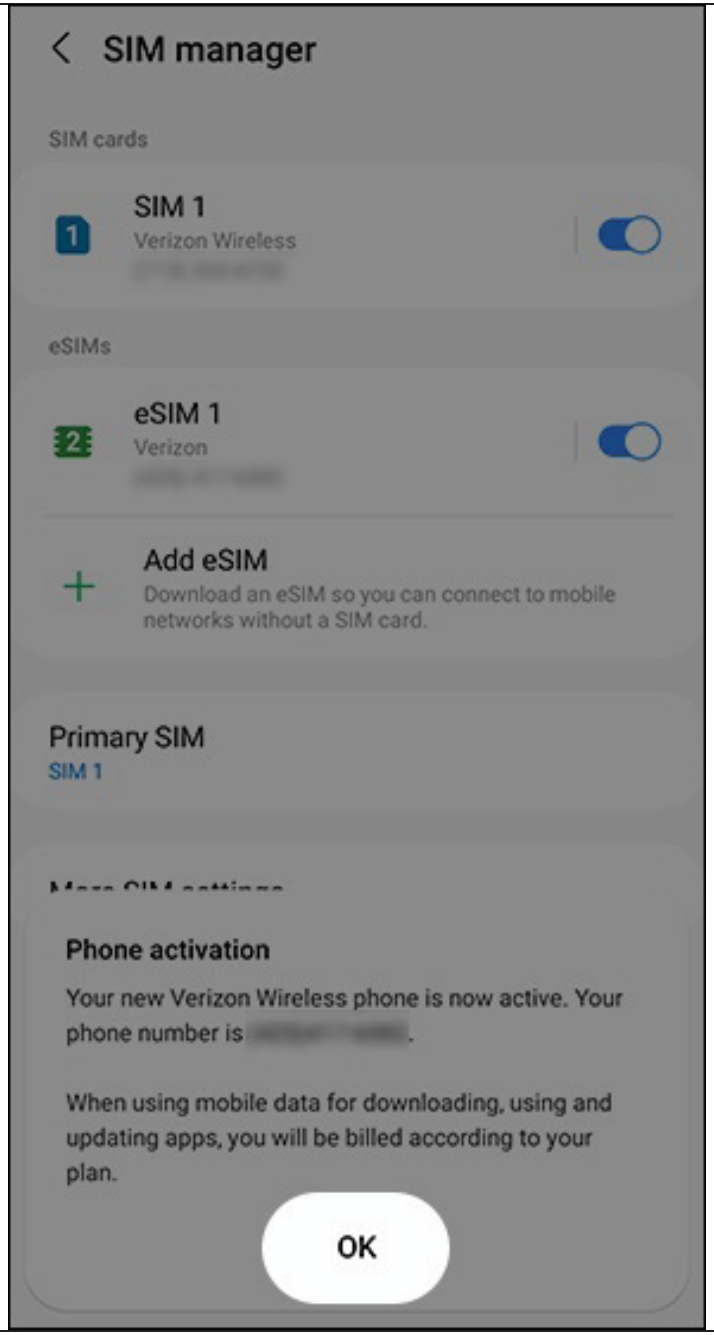
Figure 29I: Profile Content Management

	3.11 Device Change and Profile Recovery **3.11.1 Device Change** This procedure will allow the End User having a Profile in the old Device to add a Profile related to the same Subscription in the new Device. This procedure can further enable the downloaded Profile upon End User consent, which consequently MAY disable a currently Enabled Profile of the new Device (if any). Network connectivity is assumed.

Claim 8

Issued Claim(s)	Public Documentation
8. The wireless device recited in claim 7, wherein the action is to cause a notification to be presented through the user interface, wherein the notification reports that the particular credential has been replaced by the target credential.	The Accused Devices comprise the "wireless device recited in claim 7, wherein the action is to cause a notification to be presented through the user interface, wherein the notification reports that the particular credential has been replaced by the target credential." *See*, for example, the disclosures identified for claim 7. For further example, the Accused Devices comprise a user interface where notifications can be presented. *See, e.g.,* https://www.samsung.com/my/support/mobile-devices/using-your-galaxy-smartphones-with-esim/; https://www.samsung.com/us/support/answer/ANS10001619/ (referring to carrier's instructions for using eSIM):

	An eSIM is an embedded version of the physical SIM card on the device. The eSIM provides connection to your carrier's network, however instead of inserting a card, you will activate it with your carrier account information. You can also use the eSIM alongside a physical SIM to add a second phone number or carrier to your device. **1** Navigate to and open **Settings**, and then tap **Connections**. **2** Tap **SIM manager**. From here, you can tap the **switch** next to your physical SIM or activated eSIM to enable or disable their connections. You can also tap **Primary SIM** to change the default connection for making calls, sending texts, and using data.  ; *see also* https://www.verizon.com/support/knowledge-base-240165/:


SIM manager
SIM cards
SIM 1
Verizon Wireless
eSIMs
eSIM 1
Verizon
Add eSIM
Download an eSIM so you can connect to mobile networks without a SIM card.
Primary SIM
SIM 1
Phone activation
Your new Verizon Wireless phone is now active. Your phone number is .
When using mobile data for downloading, using and updating apps, you will be billed according to your plan.
OK

	; https://www.att.com/support/how-to/wireless/esim-get-started/: **Samsung smartphone** Just turn on your phone and follow the setup prompts. If you have wireless service bars or you can make a call, you're all set. Don't have service? Look for a notification to add your eSIM or go to your phone **Settings.** Tap **Connections,** then **SIM manager** and **Add eSIM.** Having trouble? Get more details for Samsung eSIMs. ; https://www.t-mobile.com/support/devices/device-troubleshooting/samsung-on-device-activation-troubleshooting; https://www.t-mobile.com/support/tutorials/device/samsung/galaxy-s23-plus/topic/esim/activating-esim/36

Claim 9

Issued Claim(s)	Public Documentation
9. The wireless device recited in claim 1, wherein, when executed by the one or more processors, the one or more machine-executable instructions further cause the one or more processors to cause a notification to be presented through the user interface, the notification providing information about a status of the user request to replace the particular credential of the one or more credentials with the target credential.	The Accused Devices comprise the "wireless device recited in claim 1, wherein, when executed by the one or more processors, the one or more machine-executable instructions further cause the one or more processors to cause a notification to be presented through the user interface, the notification providing information about a status of the user request to replace the particular credential of the one or more credentials with the target credential." *See*, for example, the disclosures identified for claims 7 and 8. For further example, the Accused Devices provide notifications through a user interface regarding credentials. *See, e.g.,* https://www.t-mobile.com/support/tutorials/device/samsung/galaxy-s24/topic/esim/activating-esim/:

eSIM > Activating eSIM

All categories | Change device | All topics

9 Searching for linked eSIM profiles.

10 The eSIM profile is being downloaded. This can take up to 5 minutes. **Note:** Choose **Restart** when prompted.

11 The Samsung Galaxy S24 will automatically reboot.

Previous 9 / 49 **Next**

eSIM > Activating eSIM

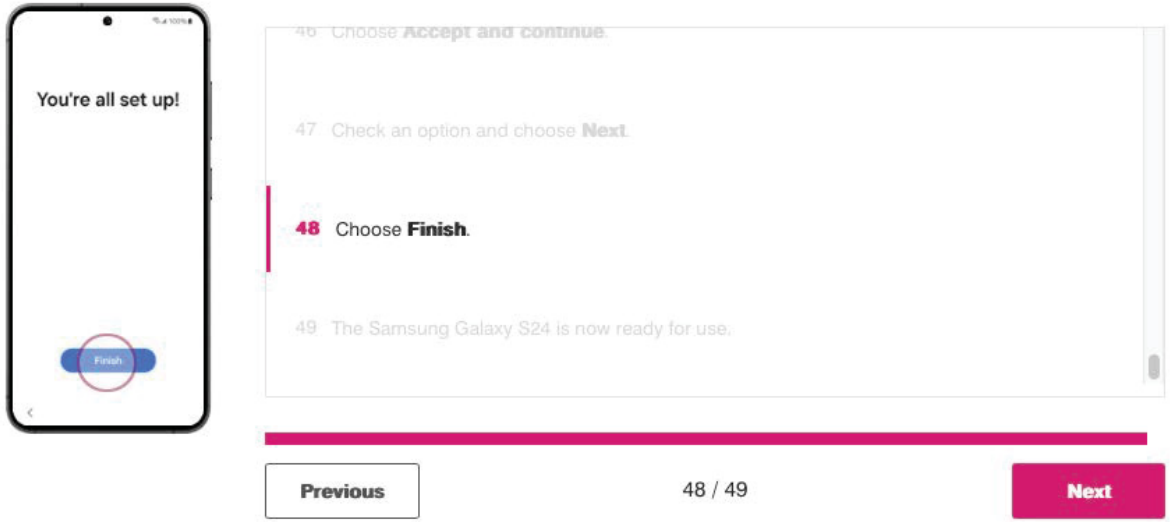
All categories | Change device | All topics

10 The eSIM profile is being downloaded. This can take up to 5 minutes. **Note:** Choose **Restart** when prompted.

11 The Samsung Galaxy S24 will automatically reboot.

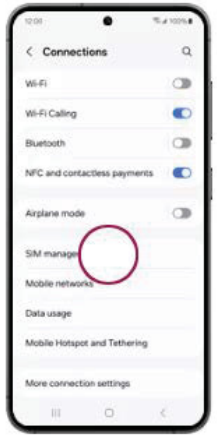
12 Choose an option, in this case, **Set up manually**.

Previous 10 / 49 Next

	Tutorials > Samsung > Galaxy S24 > eSIM > **Activating eSIM** **eSIM > Activating eSIM** All categories | Change device | All topics  ; https://www.t-mobile.com/support/tutorials/device/samsung/galaxy-s24/topic/esim/how-to-remove-delete-an-esim-profile/:

eSIM > How to remove/delete an eSIM profile

All categories | Change device | All topics



5 Choose **SIM manager**.

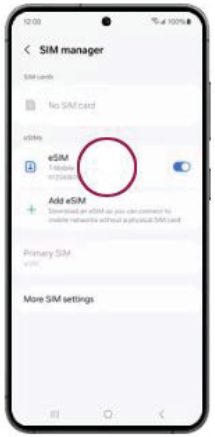
6 Under **eSIMs**, choose the eSIM.

7 Choose **Remove**.

8 Optional: Choose **Move contacts** and follow the onscreen instructions. Choose **Remove**.

Previous 5 / 9 Next

eSIM > How to remove/delete an eSIM profile



6 Under **eSIMs**, choose the eSIM.

7 Choose **Remove**.

8 Optional: Choose **Move contacts** and follow the onscreen instructions. Choose **Remove**.

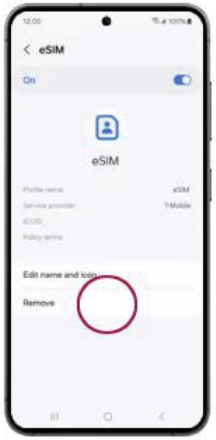
9 The eSIM profile has been removed. Return to the Home screen.

Previous 6 / 9 Next

Tutorials > Samsung > Galaxy S24 > eSIM > **How to remove/delete an eSIM profile**

eSIM > How to remove/delete an eSIM profile

All categories | Change device | All topics



6 Under **eSIMs**, choose the eSIM.

7 Choose **Remove**.

8 Optional: Choose **Move contacts** and follow the onscreen instructions. Choose **Remove**.

9 The eSIM profile has been removed. Return to the Home screen.

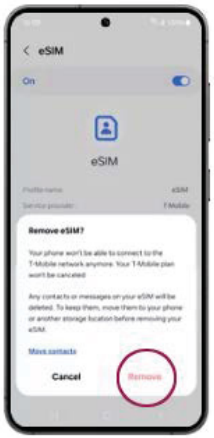
Previous 7 / 9 Next

171

Tutorials > Samsung > Galaxy S24 > eSIM > **How to remove/delete an eSIM profile**

eSIM > How to remove/delete an eSIM profile

All categories | Change device | All topics



6 Under **eSIMs**, choose the eSIM.

7 Choose **Remove**.

8 Optional: Choose **Move contacts** and follow the onscreen instructions. Choose **Remove**.

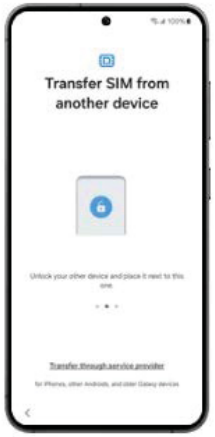
9 The eSIM profile has been removed. Return to the Home screen.

Previous 8 / 9 Next

; https://www.t-mobile.com/support/tutorials/device/samsung/galaxy-s24/topic/esim/how-to-swap-sims-from-an-old-device-to-a-new-device/:

eSIM > How to swap SIMs from an old device to a new device

All categories | Change device | All topics



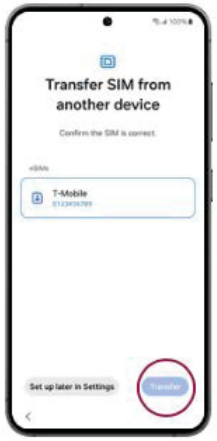
11 Bring your old device near to the new one. **Note:** Make sure your old device is unlocked.

12 On your old device: Choose **Transfer**.

13 A verification code is displayed on your new Samsung Galaxy S24. **Note:** If the old Android phone is not a Samsung device, you will be prompted to scan a QR code with your old device.

Previous 11 / 57 Next

eSIM > How to swap SIMs from an old device to a new device



15 On your new Samsung Galaxy S24: Verify the phone number and choose **Transfer**.

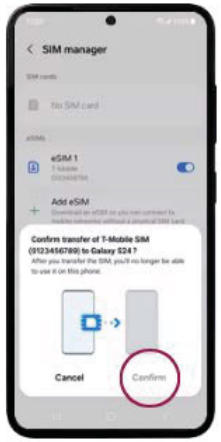
16 On your old device: Choose **Confirm**.

17 Choose **Done**. Proceed with your Samsung Galaxy S24.

18 The eSIM profile is being downloaded. This can take up to 5 minutes. **Note:** Choose

eSIM > How to swap SIMs from an old device to a new device

All categories | Change device | All topics



16 On your old device: Choose **Confirm**.

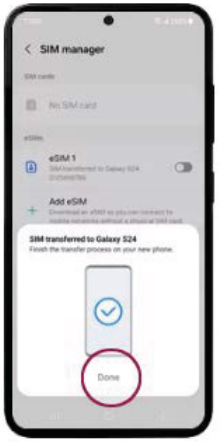
17 Choose **Done**. Proceed with your Samsung Galaxy S24.

18 The eSIM profile is being downloaded. This can take up to 5 minutes. **Note:** Choose **Restart** when prompted.

Previous 16 / 57 **Next**

eSIM > How to swap SIMs from an old device to a new device

All categories | Change device | All topics



17 Choose **Done**. Proceed with your Samsung Galaxy S24.

18 The eSIM profile is being downloaded. This can take up to 5 minutes. **Note:** Choose **Restart** when prompted.

19 The Samsung Galaxy S24 will automatically reboot.

Previous 17 / 57 **Next**

	Tutorials > Samsung > Galaxy S24 > eSIM > **How to swap SIMs from an old device to a new device** **eSIM > How to swap SIMs from an old device to a new device** All categories | Change device | All topics Connecting to the T-Mobile network... **18** The eSIM profile is being downloaded. This can take up to 5 minutes. **Note:** Choose **Restart** when prompted. 19 The Samsung Galaxy S24 will automatically reboot. 20 The eSIM has been transferred and is ready for use. Choose an option, in this case, **Set up manually**. **Previous** 18 / 57 **Next**

Claim 10

Issued Claim(s)	Public Documentation
10. The wireless device recited in claim 1, wherein, when executed by the one or more processors, the one or more machine-executable instructions further cause the one or more processors to cause a notification to be presented through the user interface, the notification requesting	The Accused Devices comprise the "wireless device recited in claim 1, wherein, when executed by the one or more processors, the one or more machine-executable instructions further cause the one or more processors to cause a notification to be presented through the user interface, the notification requesting confirmation of the user request to replace the particular credential with the target credential." *See*, for example, the disclosures identified for claims 1, 4, 5, 7, and 8.

confirmation of the user request to replace the particular credential with the target credential.	For further example, the Accused Devices provide notifications through a user interface regarding credentials. *See, e.g.,* https://www.t-mobile.com/support/tutorials/device/samsung/galaxy-s24/topic/esim/activating-esim/:

Tutorials > Samsung > Galaxy S24 > eSIM > **Activating eSIM**

eSIM > Activating eSIM

All categories | Change device | All topics

9 Searching for linked eSIM profiles.

10 The eSIM profile is being downloaded. This can take up to 5 minutes. **Note:** Choose **Restart** when prompted.

11 The Samsung Galaxy S24 will automatically reboot.

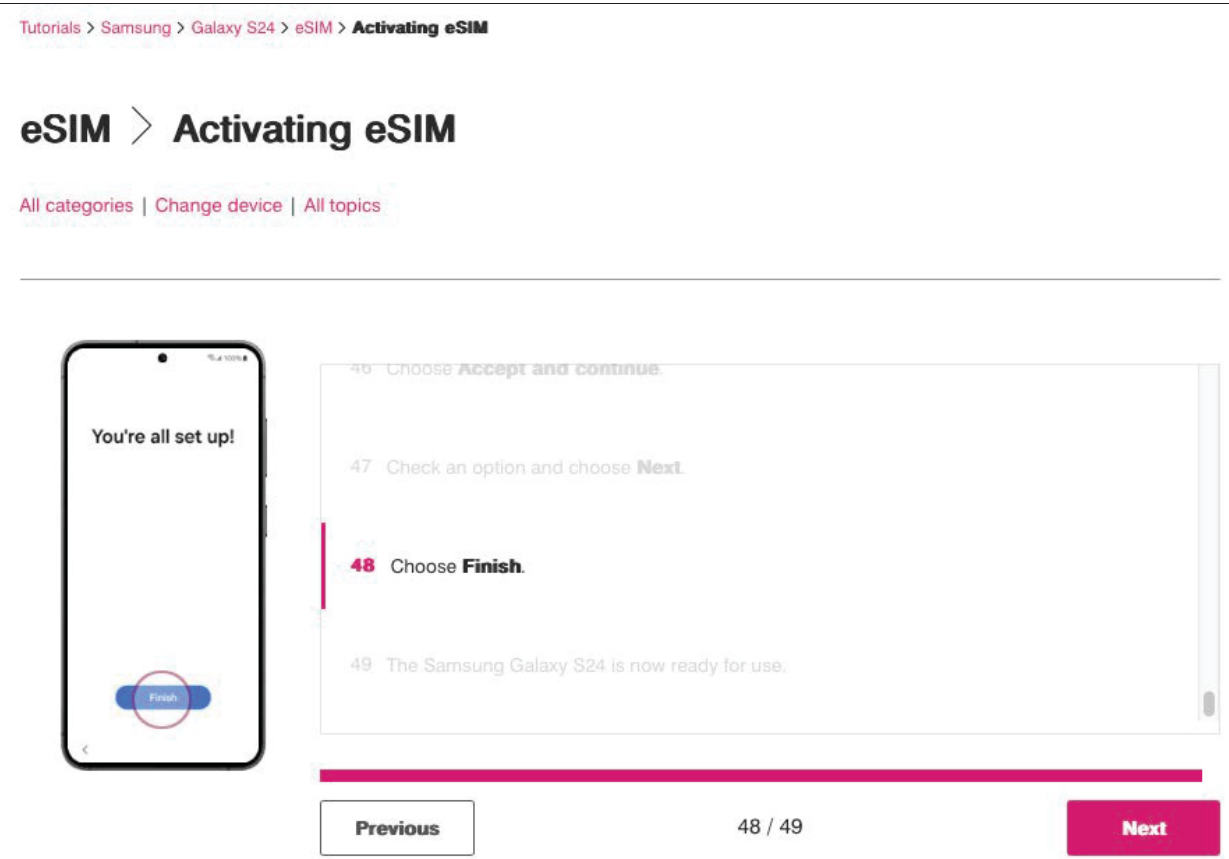
Previous 9 / 49 **Next**

eSIM > Activating eSIM

10 The eSIM profile is being downloaded. This can take up to 5 minutes. **Note:** Choose **Restart** when prompted.

11 The Samsung Galaxy S24 will automatically reboot.

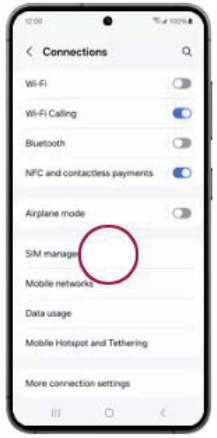
12 Choose an option, in this case, **Set up manually**.



; https://www.t-mobile.com/support/tutorials/device/samsung/galaxy-s24/topic/esim/how-to-remove-delete-an-esim-profile/:

eSIM > How to remove/delete an eSIM profile

All categories | Change device | All topics



5 Choose **SIM manager**.

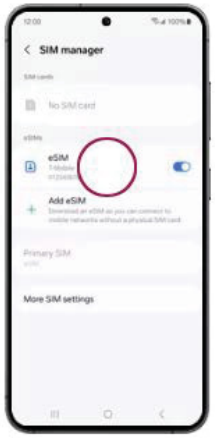
6 Under **eSIMs**, choose the eSIM.

7 Choose **Remove**.

8 Optional: Choose **Move contacts** and follow the onscreen instructions. Choose **Remove**.

Previous 5 / 9 Next

eSIM > How to remove/delete an eSIM profile



6 Under **eSIMs**, choose the eSIM.

7 Choose **Remove**.

8 Optional: Choose **Move contacts** and follow the onscreen instructions. Choose **Remove**.

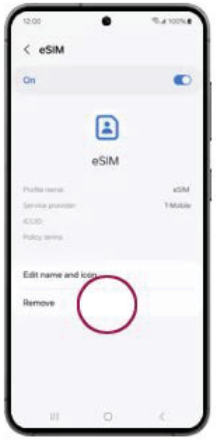
9 The eSIM profile has been removed. Return to the Home screen.

Previous 6 / 9 Next

Tutorials > Samsung > Galaxy S24 > eSIM > **How to remove/delete an eSIM profile**

eSIM > How to remove/delete an eSIM profile

All categories | Change device | All topics



6 Under **eSIMs**, choose the eSIM.

7 Choose **Remove**.

8 Optional: Choose **Move contacts** and follow the onscreen instructions. Choose **Remove**.

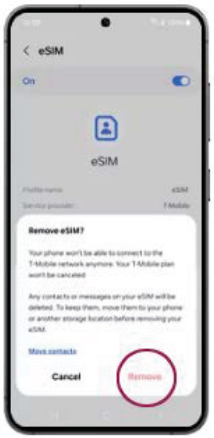
9 The eSIM profile has been removed. Return to the Home screen.

Previous 7 / 9 Next

Tutorials > Samsung > Galaxy S24 > eSIM > **How to remove/delete an eSIM profile**

eSIM > How to remove/delete an eSIM profile

All categories | Change device | All topics



6 Under **eSIMs**, choose the eSIM.

7 Choose **Remove**.

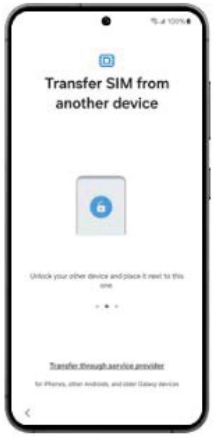
8 Optional: Choose **Move contacts** and follow the onscreen instructions. Choose **Remove**.

9 The eSIM profile has been removed. Return to the Home screen.

Previous 8 / 9 Next

; https://www.t-mobile.com/support/tutorials/device/samsung/galaxy-s24/topic/esim/how-to-swap-sims-from-an-old-device-to-a-new-device/:

eSIM > How to swap SIMs from an old device to a new device

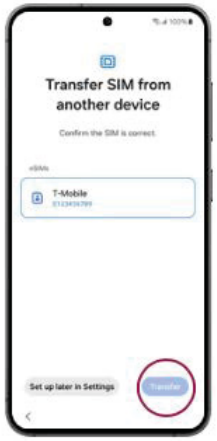


11 Bring your old device near to the new one. **Note:** Make sure your old device is unlocked.

12 On your old device: Choose **Transfer**.

13 A verification code is displayed on your new Samsung Galaxy S24. **Note:** If the old Android phone is not a Samsung device, you will be prompted to scan a QR code with your old device.

eSIM > How to swap SIMs from an old device to a new device



15 On your new Samsung Galaxy S24: Verify the phone number and choose **Transfer**.

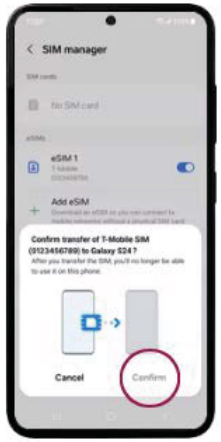
16 On your old device: Choose **Confirm**.

17 Choose **Done**. Proceed with your Samsung Galaxy S24.

18 The eSIM profile is being downloaded. This can take up to 5 minutes. **Note:** Choose

eSIM > How to swap SIMs from an old device to a new device

All categories | Change device | All topics



16 On your old device: Choose **Confirm**.

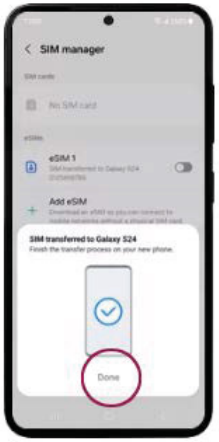
17 Choose **Done**. Proceed with your Samsung Galaxy S24.

18 The eSIM profile is being downloaded. This can take up to 5 minutes. **Note:** Choose **Restart** when prompted.

Previous 16 / 57 **Next**

eSIM > How to swap SIMs from an old device to a new device

All categories | Change device | All topics



17 Choose **Done**. Proceed with your Samsung Galaxy S24.

18 The eSIM profile is being downloaded. This can take up to 5 minutes. **Note:** Choose **Restart** when prompted.

19 The Samsung Galaxy S24 will automatically reboot.

Previous 17 / 57 Next

	Tutorials > Samsung > Galaxy S24 > eSIM > **How to swap SIMs from an old device to a new device** **eSIM > How to swap SIMs from an old device to a new device** All categories | Change device | All topics **18** The eSIM profile is being downloaded. This can take up to 5 minutes. **Note:** Choose **Restart** when prompted. 19 The Samsung Galaxy S24 will automatically reboot. 20 The eSIM has been transferred and is ready for use. Choose an option, in this case, **Set up manually**. **Previous** 18 / 57 **Next**

Claim 11

Issued Claim(s)	Public Documentation
11. The wireless device recited in claim 1, wherein detecting the network-provisioning state change comprises determining that a registration attempt initiated by the wireless device has failed.	The Accused Devices comprise the "wireless device recited in claim 1, wherein detecting the network-provisioning state change comprises determining that a registration attempt initiated by the wireless device has failed." *See*, for example, the disclosures identified for claims 1, 2, and 4. *See also, e.g.,* https://www.gsma.com/esim/wp-content/uploads/2022/10/SGP.22-v3.0-1.pdf:

3.1.6 Profile Lifecycle at SM-DP+

The previous sections provide detailed procedures associated with Remote Provisioning. Each Profile has state information on the SM-DP+ associated with it during the provisioning into an eUICC. The Profile lifecycle state can be one of the states listed in the following table.

Additional states and additional or customised ES2+ functions MAY be agreed between the Operator and the SM-DP+.

State Name	Description
Available	The Profile is available in the inventory of the SM-DP+.
Allocated	The Profile is reserved for downloading without being linked to an EID.
Linked	The Profile is reserved for downloading and is linked to an EID.
Confirmed	The Profile is reserved for downloading (linked or not linked to an EID) with Matching ID and Confirmation Code if required.
Released	The Profile is ready for download and installation after Network Configuration by the Operator (e.g.: HLR Registration).
Downloaded	The Bound Profile was delivered to the LPA.
Installed	The Profile was successfully installed on the eUICC.
Error	The Profile has not been installed because of one of the following error cases: - Confirmation Code Retry Limit exceeded - Download Retry Limit exceeded - End User Rejection - Permanent error during download and installation
Unavailable	The Profile cannot be reused anymore by the SM-DP+.

Table 6b: Profile State in the SM-DP+

Claim 12

Issued Claim(s)	Public Documentation
12. The wireless device recited in claim 1, wherein detecting the network-provisioning state change comprises determining that an attempt by the wireless device to place a voice call has failed.	The Accused Devices comprise the "wireless device recited in claim 1, wherein detecting the network-provisioning state change comprises determining that an attempt by the wireless device to place a voice call has failed." *See*, for example, the disclosures identified for claims 1, 2, and 4. *See also, e.g.,* https://www.gsma.com/esim/wp-content/uploads/2022/10/SGP.22-v3.0-1.pdf:

3.1.6 Profile Lifecycle at SM-DP+

The previous sections provide detailed procedures associated with Remote Provisioning. Each Profile has state information on the SM-DP+ associated with it during the provisioning into an eUICC. The Profile lifecycle state can be one of the states listed in the following table.

Additional states and additional or customised ES2+ functions MAY be agreed between the Operator and the SM-DP+.

State Name	Description
Available	The Profile is available in the inventory of the SM-DP+.
Allocated	The Profile is reserved for downloading without being linked to an EID.
Linked	The Profile is reserved for downloading and is linked to an EID.
Confirmed	The Profile is reserved for downloading (linked or not linked to an EID) with Matching ID and Confirmation Code if required.
Released	The Profile is ready for download and installation after Network Configuration by the Operator (e.g.: HLR Registration).
Downloaded	The Bound Profile was delivered to the LPA.
Installed	The Profile was successfully installed on the eUICC.
Error	The Profile has not been installed because of one of the following error cases: - Confirmation Code Retry Limit exceeded - Download Retry Limit exceeded - End User Rejection - Permanent error during download and installation
Unavailable	The Profile cannot be reused anymore by the SM-DP+.

Table 6b: Profile State in the SM-DP+

192

Claim 13

Issued Claim(s)	Public Documentation
13. The wireless device recited in claim 1, wherein detecting the network-provisioning state change comprises determining that an attempt by the wireless device to send a text message has failed.	The Accused Devices comprise the "wireless device recited in claim 1, wherein detecting the network-provisioning state change comprises determining that an attempt by the wireless device to send a text message has failed." *See*, for example, the disclosures identified for claims 1, 2, and 4. *See also, e.g.,* https://www.gsma.com/esim/wp-content/uploads/2022/10/SGP.22-v3.0-1.pdf:

3.1.6 Profile Lifecycle at SM-DP+

The previous sections provide detailed procedures associated with Remote Provisioning. Each Profile has state information on the SM-DP+ associated with it during the provisioning into an eUICC. The Profile lifecycle state can be one of the states listed in the following table.

Additional states and additional or customised ES2+ functions MAY be agreed between the Operator and the SM-DP+.

State Name	Description
Available	The Profile is available in the inventory of the SM-DP+.
Allocated	The Profile is reserved for downloading without being linked to an EID.
Linked	The Profile is reserved for downloading and is linked to an EID.
Confirmed	The Profile is reserved for downloading (linked or not linked to an EID) with Matching ID and Confirmation Code if required.
Released	The Profile is ready for download and installation after Network Configuration by the Operator (e.g.: HLR Registration).
Downloaded	The Bound Profile was delivered to the LPA.
Installed	The Profile was successfully installed on the eUICC.
Error	The Profile has not been installed because of one of the following error cases: - Confirmation Code Retry Limit exceeded - Download Retry Limit exceeded - End User Rejection - Permanent error during download and installation
Unavailable	The Profile cannot be reused anymore by the SM-DP+.

Table 6b: Profile State in the SM-DP+

194

Claim 14

Issued Claim(s)	Public Documentation
14. The wireless device recited in claim 1, wherein detecting the network-provisioning state change comprises determining that an attempt by the wireless device to authenticate with the network element has failed.	The Accused Devices comprise the "wireless device recited in claim 1, wherein detecting the network-provisioning state change comprises determining that an attempt by the wireless device to authenticate with the network element has failed." *See*, for example, the disclosures identified for claims 1, 2, 3, and 4. *See also, e.g.,* https://www.gsma.com/esim/wp-content/uploads/2022/10/SGP.22-v3.0-1.pdf:

3.1.6 Profile Lifecycle at SM-DP+

The previous sections provide detailed procedures associated with Remote Provisioning. Each Profile has state information on the SM-DP+ associated with it during the provisioning into an eUICC. The Profile lifecycle state can be one of the states listed in the following table.

Additional states and additional or customised ES2+ functions MAY be agreed between the Operator and the SM-DP+.

State Name	Description
Available	The Profile is available in the inventory of the SM-DP+.
Allocated	The Profile is reserved for downloading without being linked to an EID.
Linked	The Profile is reserved for downloading and is linked to an EID.
Confirmed	The Profile is reserved for downloading (linked or not linked to an EID) with Matching ID and Confirmation Code if required.
Released	The Profile is ready for download and installation after Network Configuration by the Operator (e.g.: HLR Registration).
Downloaded	The Bound Profile was delivered to the LPA.
Installed	The Profile was successfully installed on the eUICC.
Error	The Profile has not been installed because of one of the following error cases: - Confirmation Code Retry Limit exceeded - Download Retry Limit exceeded - End User Rejection - Permanent error during download and installation
Unavailable	The Profile cannot be reused anymore by the SM-DP+.

Table 6b: Profile State in the SM-DP+

Claim 15

Issued Claim(s)	Public Documentation
15. The wireless device recited in claim 1, wherein detecting the network-provisioning state change comprises determining that an attempt by the wireless device to be authorized for a service has failed.	The Accused Devices comprise the "wireless device recited in claim 1, wherein detecting the network-provisioning state change comprises determining that an attempt by the wireless device to be authorized for a service has failed." *See*, for example, the disclosures identified for claims 1, 2, and 4. *See also, e.g.,* https://www.gsma.com/esim/wp-content/uploads/2022/10/SGP.22-v3.0-1.pdf:

3.1.6 Profile Lifecycle at SM-DP+

The previous sections provide detailed procedures associated with Remote Provisioning. Each Profile has state information on the SM-DP+ associated with it during the provisioning into an eUICC. The Profile lifecycle state can be one of the states listed in the following table.

Additional states and additional or customised ES2+ functions MAY be agreed between the Operator and the SM-DP+.

State Name	Description
Available	The Profile is available in the inventory of the SM-DP+.
Allocated	The Profile is reserved for downloading without being linked to an EID.
Linked	The Profile is reserved for downloading and is linked to an EID.
Confirmed	The Profile is reserved for downloading (linked or not linked to an EID) with Matching ID and Confirmation Code if required.
Released	The Profile is ready for download and installation after Network Configuration by the Operator (e.g.: HLR Registration).
Downloaded	The Bound Profile was delivered to the LPA.
Installed	The Profile was successfully installed on the eUICC.
Error	The Profile has not been installed because of one of the following error cases: - Confirmation Code Retry Limit exceeded - Download Retry Limit exceeded - End User Rejection - Permanent error during download and installation
Unavailable	The Profile cannot be reused anymore by the SM-DP+.

Table 6b: Profile State in the SM-DP+

198

Claim 16

Issued Claim(s)	Public Documentation
16. The wireless device recited in claim 1, wherein detecting the network-provisioning state change comprises determining that a network access error has occurred.	The Accused Devices comprise the "wireless device recited in claim 1, wherein detecting the network-provisioning state change comprises determining that a network access error has occurred." *See*, for example, the disclosures identified for claims 1, 2, and 4. *See also, e.g.,* https://www.gsma.com/esim/wp-content/uploads/2022/10/SGP.22-v3.0-1.pdf:

3.1.6 Profile Lifecycle at SM-DP+

The previous sections provide detailed procedures associated with Remote Provisioning. Each Profile has state information on the SM-DP+ associated with it during the provisioning into an eUICC. The Profile lifecycle state can be one of the states listed in the following table.

Additional states and additional or customised ES2+ functions MAY be agreed between the Operator and the SM-DP+.

State Name	Description
Available	The Profile is available in the inventory of the SM-DP+.
Allocated	The Profile is reserved for downloading without being linked to an EID.
Linked	The Profile is reserved for downloading and is linked to an EID.
Confirmed	The Profile is reserved for downloading (linked or not linked to an EID) with Matching ID and Confirmation Code if required.
Released	The Profile is ready for download and installation after Network Configuration by the Operator (e.g.: HLR Registration).
Downloaded	The Bound Profile was delivered to the LPA.
Installed	The Profile was successfully installed on the eUICC.
Error	The Profile has not been installed because of one of the following error cases: - Confirmation Code Retry Limit exceeded - Download Retry Limit exceeded - End User Rejection - Permanent error during download and installation
Unavailable	The Profile cannot be reused anymore by the SM-DP+.

Table 6b: Profile State in the SM-DP+

Claim 17

Issued Claim(s)	Public Documentation
17. The wireless device recited in claim 1, wherein detecting the network-provisioning state change comprises receiving a provisioning-state-change message.	The Accused Devices comprise the "wireless device recited in claim 1, wherein detecting the network-provisioning state change comprises receiving a provisioning-state-change message." *See*, for example, the disclosures identified for claims 1, 2, 4, and 7. *See also, e.g.,* https://www.gsma.com/esim/wp-content/uploads/2022/10/SGP.22-v3.0-1.pdf:

3.1.6 Profile Lifecycle at SM-DP+

The previous sections provide detailed procedures associated with Remote Provisioning. Each Profile has state information on the SM-DP+ associated with it during the provisioning into an eUICC. The Profile lifecycle state can be one of the states listed in the following table.

Additional states and additional or customised ES2+ functions MAY be agreed between the Operator and the SM-DP+.

State Name	Description
Available	The Profile is available in the inventory of the SM-DP+.
Allocated	The Profile is reserved for downloading without being linked to an EID.
Linked	The Profile is reserved for downloading and is linked to an EID.
Confirmed	The Profile is reserved for downloading (linked or not linked to an EID) with Matching ID and Confirmation Code if required.
Released	The Profile is ready for download and installation after Network Configuration by the Operator (e.g.: HLR Registration).
Downloaded	The Bound Profile was delivered to the LPA.
Installed	The Profile was successfully installed on the eUICC.
Error	The Profile has not been installed because of one of the following error cases: - Confirmation Code Retry Limit exceeded - Download Retry Limit exceeded - End User Rejection - Permanent error during download and installation
Unavailable	The Profile cannot be reused anymore by the SM-DP+.

Table 6b: Profile State in the SM-DP+

Claim 18

Issued Claim(s)	Public Documentation
18. The wireless device recited in claim 17, wherein the provisioning-state-change message comprises a text message.	The Accused Devices comprise the "wireless device recited in claim 17, wherein the provisioning-state-change message comprises a text message." *See*, for example, the disclosures identified for claim 17.

Claim 19

Issued Claim(s)	Public Documentation
19. The wireless device recited in claim 17, wherein the provisioning-state-change message comprises a push message from a push server communicatively coupled to the wireless device over the wireless access network.	The Accused Devices comprise the "wireless device recited in claim 17, wherein the provisioning-state-change message comprises a push message from a push server communicatively coupled to the wireless device over the wireless access network." *See*, for example, the disclosures identified for claim 17. For further example, the Accused Devices receive push messages from a push messaging server. *See, e.g.,* https://www.samsung.com/us/support/answer/ANS10001619/:

	eSIM Activation Options: Carrier Discovery Server 1 Existing eSIM profile is found; tap **Add**. 2 eSIM profile is downloaded. 3 Restart the device to apply the eSIM profile. Carrier Push Notification 1 eSIM ready notification appears. Tap the notification, and then tap **Add**. 2 eSIM profile is downloaded. 3 eSIM profile added to the device. Restart the device to apply. ; https://www.gsma.com/esim/wp-content/uploads/2022/10/SGP.22-v3.0-1.pdf:

	2.13 Overview of Push Service A Push Service is a service that allows an application server to send push notifications to an application on a Device. This specification allows an SM-DS and LDS to leverage a Push Service so that the LDS is informed in a timely manner when a relevant Event Record is available on the SM-DS. Figure 8aa shows the entities required for Push Service. A Push Service is implemented by a combination of a push server and a push client on the Device. The interfaces between the push server and the push client, between the push client and the LPAd, and between the SM-DS and the push server, as well as the interactions between them, are out of scope of this specification.

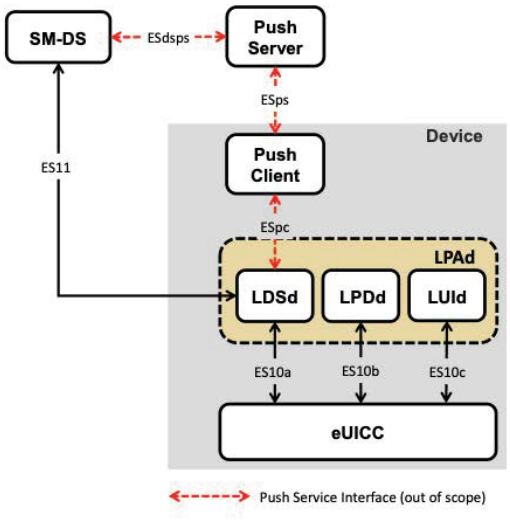


Figure 8aa: Entities for Push Service, LPA in the Device

The SM-DS and a Device MAY support one or more Push Services. The LPAd and SM-DS perform the Push Service registration so that the SM-DS can subsequently send push notifications to the LPAd, following the general sequence that follows:

The SM-DS indicates, during Common Mutual Authentication, one or more Push Service(s) that it supports. If the Device supports at least one of these Push Services, the LPAd requests the corresponding push client on the Device to allow the LPAd to use this Push Service. The push client and its related push server perform an operation to generate a Push Token dedicated to the LPAd. The LPAd then forwards its Push Token together with the EID of its associated eUICC to the SM-DS (see section 3.6.5).

Later, to inform the LPAd that an Event Record is pending for this LPAd on the SM-DS, the SM-DS requests the push server to send a push notification for this Push Token. The push server routes this notification to the push client, which forwards it to the LPAd. The LPAd MAY then perform an Event Retrieval procedure.

A Push Service MAY limit the validity of a Push Token depending on its implementation. Upon expiration of the validity, the LPAd SHOULD re-register a Push Token to the SM-DS to remain able to receive push notifications.

The SM-DS MAY also clean its database of Push Tokens to avoid keeping obsolete Push Tokens. The LPAd and Push Service may not know about when this happens. An SM-DS that enacts such a clean-up policy SHOULD instruct the LPAd of a maximum Push Token retention time. It is the responsibility of the LPAd to register a Push Token, which was previously used or is newly generated, to the SM-DS when this retention time expires.

Claim 20

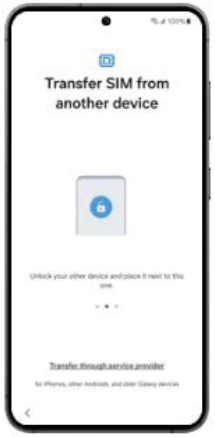
Issued Claim(s)	Public Documentation
20. The wireless device recited in claim 17, wherein the provisioning-state-change message comprises a message received by an application program on the wireless device.	The Accused Devices comprise the "wireless device recited in claim 17, wherein the provisioning-state-change message comprises a message received by an application program on the wireless device." *See*, for example, the disclosures identified for claims 17 and 18. *See also, e.g.,* https://source.android.com/docs/core/connect/esim-euicc-api; https://source.android.com/docs/core/connect/esim-error-handling; https://source.android.com/docs/core/connect/esim-mep; https://source.android.com/docs/core/connect/esim-overview: **Make a carrier app** The eUICC APIs in Android 9 make it possible for mobile network operators to create carrier-branded apps to manage their profiles directly. This includes downloading and deleting subscription profiles owned by the carrier, as well as switching to a profile owned by a carrier.

Claim 21

Issued Claim(s)	Public Documentation
21. The wireless device recited in claim 1, wherein the one or more credentials comprise a phone number.	The Accused Devices comprise the "wireless device recited in claim 1, wherein the one or more credentials comprise a phone number." *See*, for example, the disclosures identified for claims 1, 2, and 7-10. *See also, e.g.,* https://www.t-mobile.com/support/tutorials/device/samsung/galaxy-s24/topic/esim/how-to-swap-sims-from-an-old-device-to-a-new-device/:

eSIM > How to swap SIMs from an old device to a new device

All categories | Change device | All topics

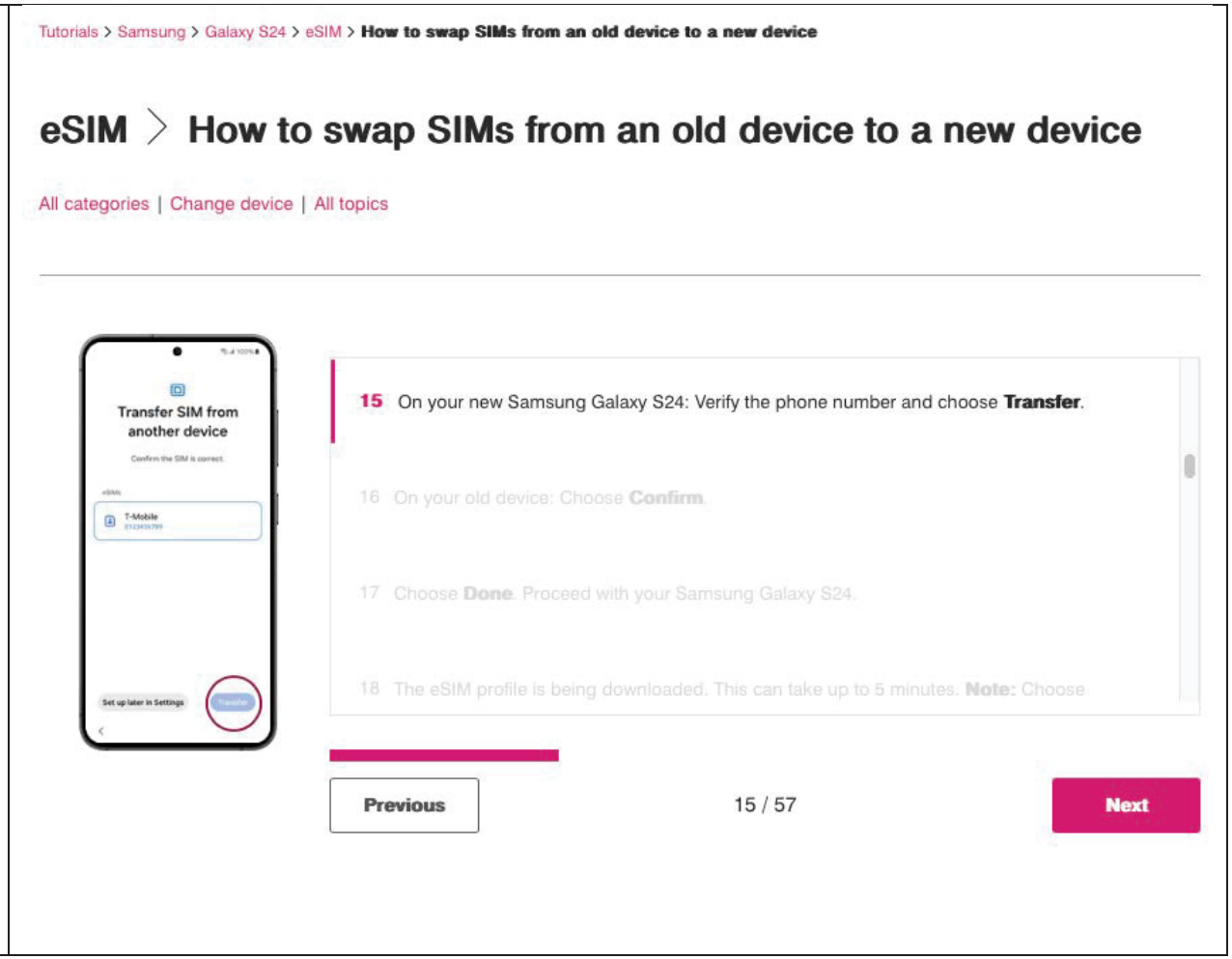


11 Bring your old device near to the new one. **Note:** Make sure your old device is unlocked.

12 On your old device: Choose **Transfer**.

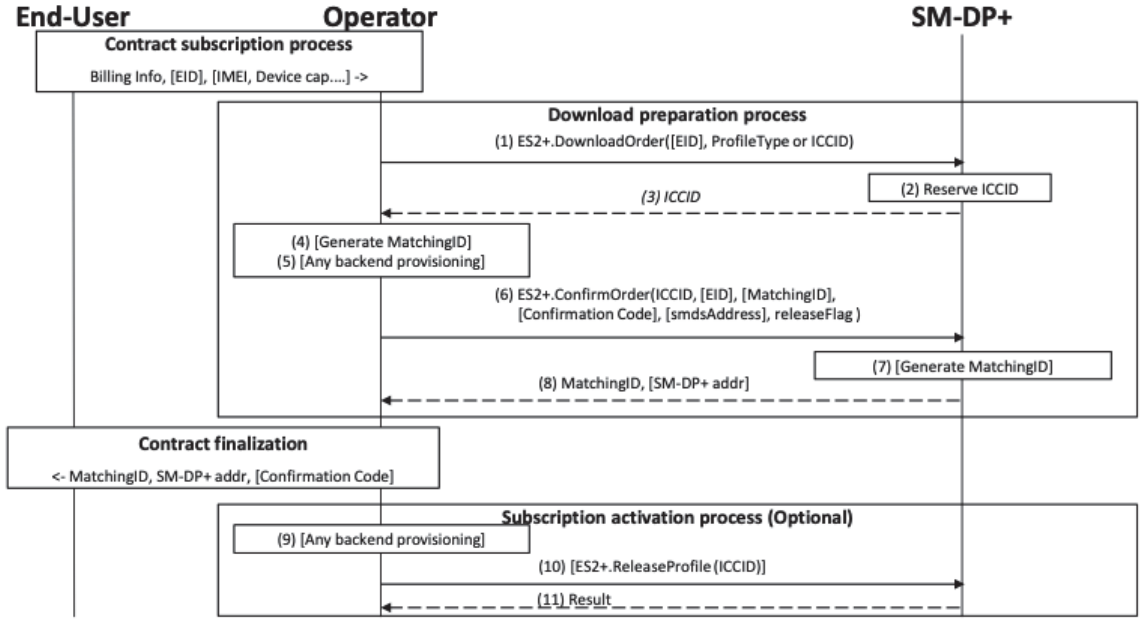
13 A verification code is displayed on your new Samsung Galaxy S24. **Note:** If the old Android phone is not a Samsung device, you will be prompted to scan a QR code with your old device.

Previous 11 / 57 Next



Claim 22

Issued Claim(s)	Public Documentation
22. The wireless device recited in claim 1, wherein the one or more credentials comprise an international mobile subscriber identifier (IMSI), a mobile	The Accused Devices comprise the "wireless device recited in claim 1, wherein the one or more credentials comprise an international mobile subscriber identifier (IMSI), a mobile station identifier (MSID), a mobile station international ISDN number (MSISDN), a subscriber information module (SIM) identifier, an electronic serial number (ESN), a mobile equipment

station identifier (MSID), a mobile station international ISDN number (MSISDN), a subscriber information module (SIM) identifier, an electronic serial number (ESN), a mobile equipment identifier (MEID), an international mobile equipment identity (IMEI), a device identifier, a subscriber identifier, a service account identifier, a media access control (MAC) address, an Internet protocol (IP) address, a token, a one-time token, a mobile directory number (MDN), a network access identifier (NAI), a user name, a password, access point name (APN) configuration information, an encryption key (Ki), a Wi-Fi service set identifier (SSID), a Wi-Fi network configuration, an IP address, or a combination of these.	identifier (MEID), an international mobile equipment identity (IMEI), a device identifier, a subscriber identifier, a service account identifier, a media access control (MAC) address, an Internet protocol (IP) address, a token, a one-time token, a mobile directory number (MDN), a network access identifier (NAI), a user name, a password, access point name (APN) configuration information, an encryption key (Ki), a Wi-Fi service set identifier (SSID), a Wi-Fi network configuration, an IP address, or a combination of these." *See*, for example, the disclosures identified for claim 1. For further example, the Accused Devices use one or more identifiers as credentials. *See, e.g.,* https://www.gsma.com/esim/wp-content/uploads/2022/10/SGP.22-v3.0-1.pdf: **3.1 Remote Provisioning** **3.1.1 Profile Download Initiation**  **Figure 9: Profile Download Initiation**

NOTE: The following table summarizes the input data to be provided in "ES2+.DownloadOrder" and "ES2+.ConfirmOrder" functions.

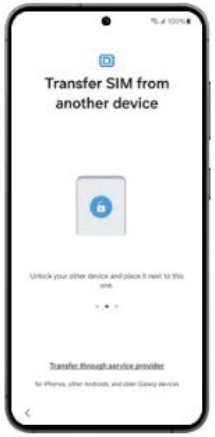
ES2+ Function	Input Parameters	Profile Download Use Cases		
		Default SM-DP+	Activation Code	SM-DS
DownloadOrder (Section 5.3.1)	eid	O	O	O
	iccid	O	O	O
	profileType	C (1)	C (1)	C (1)
ConfirmOrder (Section 5.3.2)	iccid	M	M	M
	eid	C (2)	O	C (2)
	matchingId	M (3)	O (4)	O (5)
	confirmationCode	O	O	O
	smdsAddress	Not Present	Not Present	C (6)
	rootSmdsAddress	Not Present	Not Present	C (6)
	releaseFlag	M	M	M

NOTE 1: Required if iccid is not present for DownloadOrder
NOTE 2: Required if it is not present for DownloadOrder
NOTE 3: Value SHALL have zero-length
NOTE 4: If present, value SHALL have non-zero-length. If not present, SM-DP+ generates matchingId for ActivationCodeToken
NOTE 5: If present, value SHALL have non-zero-length. If not present, SM-DP+ generates matchingId. It is used as EventID
NOTE 6: One or both of smdsAddress and rootSmdsAddress SHALL be present

Table 6a: "ES2+.DownloadOrder" and "ES2+.ConfirmOrder" input data

Claim 23

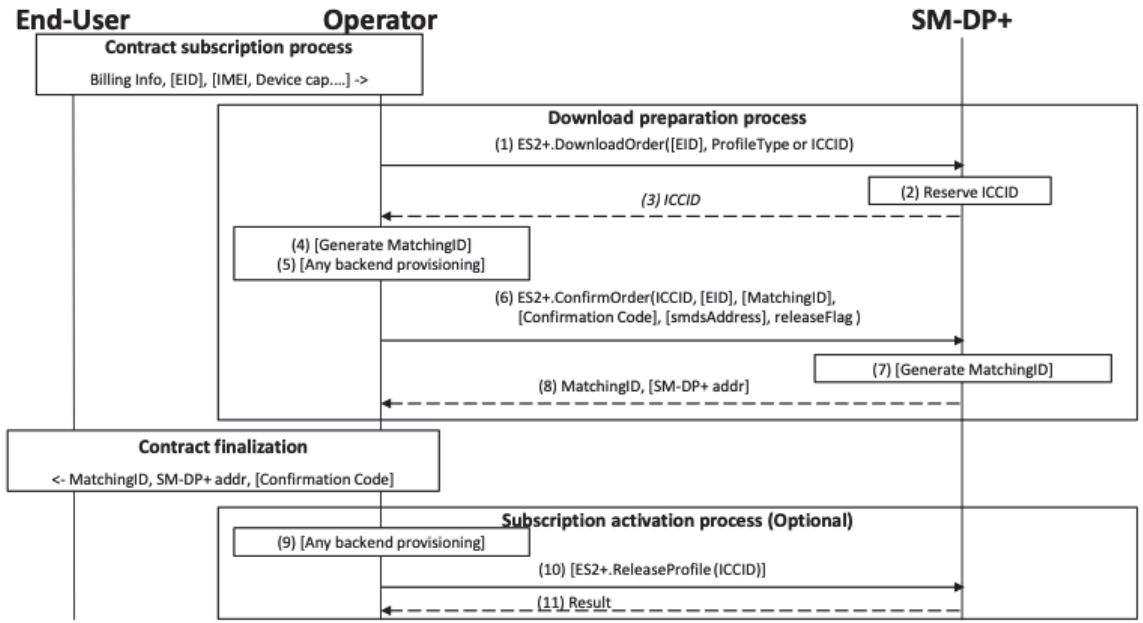
Issued Claim(s)	Public Documentation

23. The wireless device recited in claim 1, wherein the target credential comprises a phone number.	The Accused Devices comprise the "wireless device recited in claim 1, wherein the target credential comprises a phone number." *See*, for example, the disclosures identified for claims 1, 2, and 7-10. *See also, e.g.,* https://www.t-mobile.com/support/tutorials/device/samsung/galaxy-s24/topic/esim/how-to-swap-sims-from-an-old-device-to-a-new-device/: Tutorials > Samsung > Galaxy S24 > eSIM > **How to swap SIMs from an old device to a new device** **eSIM > How to swap SIMs from an old device to a new device** All categories | Change device | All topics  **11** Bring your old device near to the new one. **Note:** Make sure your old device is unlocked. 12 On your old device: Choose **Transfer**. 13 A verification code is displayed on your new Samsung Galaxy S24. **Note:** If the old Android phone is not a Samsung device, you will be prompted to scan a QR code with your old device. **Previous** 11 / 57 **Next**

	Tutorials > Samsung > Galaxy S24 > eSIM > **How to swap SIMs from an old device to a new device** **eSIM > How to swap SIMs from an old device to a new device** All categories | Change device | All topics **15** On your new Samsung Galaxy S24: Verify the phone number and choose **Transfer**. 16 On your old device: Choose **Confirm**. 17 Choose **Done**. Proceed with your Samsung Galaxy S24. 18 The eSIM profile is being downloaded. This can take up to 5 minutes. **Note:** Choose **Previous** 15 / 57 **Next**

Claim 24

Issued Claim(s)	Public Documentation
24. The wireless device recited in claim 1, wherein the target credential comprises an international mobile subscriber identifier (IMSI), a mobile station	The Accused Devices comprise the "wireless device recited in claim 1, wherein the target credential comprises an international mobile subscriber identifier (IMSI), a mobile station identifier (MSID), a mobile station international ISDN number (MSISDN), a subscriber information module (SIM) identifier, an electronic serial number (ESN), a mobile equipment

identifier (MSID), a mobile station international ISDN number (MSISDN), a subscriber information module (SIM) identifier, an electronic serial number (ESN), a mobile equipment identifier (MEID), an international mobile equipment identity (IMEI), a device identifier, a subscriber identifier, a service account identifier, a media access control (MAC) address, an Internet protocol (IP) address, a token, a one-time token, a mobile directory number (MDN), a network access identifier (NAI), a user name, a password, access point name (APN) configuration information, an encryption key (Ki), a Wi-Fi service set identifier (SSID), a Wi-Fi network configuration, an IP address, or a combination of these.	identifier (MEID), an international mobile equipment identity (IMEI), a device identifier, a subscriber identifier, a service account identifier, a media access control (MAC) address, an Internet protocol (IP) address, a token, a one-time token, a mobile directory number (MDN), a network access identifier (NAI), a user name, a password, access point name (APN) configuration information, an encryption key (Ki), a Wi-Fi service set identifier (SSID), a Wi-Fi network configuration, an IP address, or a combination of these." *See*, for example, the disclosures identified for claim 1. For further example, the Accused Devices use one or more identifiers as credentials. *See, e.g.,* https://www.gsma.com/esim/wp-content/uploads/2022/10/SGP.22-v3.0-1.pdf: **3.1 Remote Provisioning** **3.1.1 Profile Download Initiation**  **Figure 9: Profile Download Initiation**

NOTE: The following table summarizes the input data to be provided in "ES2+.DownloadOrder" and "ES2+.ConfirmOrder" functions.

ES2+ Function	Input Parameters	Profile Download Use Cases		
		Default SM-DP+	Activation Code	SM-DS
DownloadOrder (Section 5.3.1)	eid	O	O	O
	iccid	O	O	O
	profileType	C (1)	C (1)	C (1)
ConfirmOrder (Section 5.3.2)	iccid	M	M	M
	eid	C (2)	O	C (2)
	matchingId	M (3)	O (4)	O (5)
	confirmationCode	O	O	O
	smdsAddress	Not Present	Not Present	C (6)
	rootSmdsAddress	Not Present	Not Present	C (6)
	releaseFlag	M	M	M

NOTE 1: Required if iccid is not present for DownloadOrder
NOTE 2: Required if it is not present for DownloadOrder
NOTE 3: Value SHALL have zero-length
NOTE 4: If present, value SHALL have non-zero-length. If not present, SM-DP+ generates matchingId for ActivationCodeToken
NOTE 5: If present, value SHALL have non-zero-length. If not present, SM-DP+ generates matchingId. It is used as EventID
NOTE 6: One or both of smdsAddress and rootSmdsAddress SHALL be present

Table 6a: "ES2+.DownloadOrder" and "ES2+.ConfirmOrder" input data

Claim 25

Issued Claim(s)	Public Documentation

25. The wireless device recited in claim 1, wherein the particular credential comprises a first phone number currently associated with the wireless device, and wherein the target credential comprises a second phone number.	The Accused Devices comprise the "wireless device recited in claim 1, wherein the particular credential comprises a first phone number currently associated with the wireless device, and wherein the target credential comprises a second phone number." *See*, for example, the disclosures identified for claim 1, 2, 7-10, 21 and 23.

Claim 26

Issued Claim(s)	Public Documentation
26. The wireless device recited in claim 25, wherein the wireless device is a first wireless device, and wherein the second phone number is, prior to the user request to replace the particular credential with the target credential, associated with a second wireless device.	The Accused Devices comprise the "wireless device recited in claim 25, wherein the wireless device is a first wireless device, and wherein the second phone number is, prior to the user request to replace the particular credential with the target credential, associated with a second wireless device." *See*, for example, the disclosures identified for claim 1, 2, 7-10, 21 and 23.

Claim 27

Issued Claim(s)	Public Documentation
27. The wireless device recited in claim 25, wherein the second phone number is, prior to the user request to replace the particular credential with the target credential, associated with a land line.	The Accused Devices comprise the "wireless device recited in claim 25, wherein the second phone number is, prior to the user request to replace the particular credential with the target credential, associated with a land line." *See*, for example, the disclosures identified for claim 1, 2, 7-10, 21 and 23. *See also, e.g.,* https://www.verizon.com/support/local-number-portability-faqs/:

About Before During transfer

How do I bring my phone number to Verizon from another carrier?

When you activate a new line with Verizon you'll have the option to transfer your current mobile or landline number from another carrier.

You can also visit our Switch to Verizon page online, contact us or visit a store to transfer your number to Verizon.

How do I know if I can bring my number?

Most phone numbers are eligible to be brought to Verizon:*

- Some numbers may not be eligible based on geography, service area coverage, technology or ownership of the line you're transferring the number from.
- Check if your phone number is eligible on our Switch to Verizon page.

*Local Number Portability, a government mandate, requires mobile and landline service providers to let customers keep their eligible phone numbers when switching carriers.

How long will it take to bring my number to Verizon?

How long it takes to bring your number to Verizon depends on your old carrier and on when you activate your device on the Verizon network. We text you a link to track the status of your number transfer.

Typical timelines are:

- Mobile – 4-24 business hours to complete your transfer.
- Landline – 2-10 business days to complete your transfer.

Note: These are average time frames. With certain circumstances, it could take more or less time.

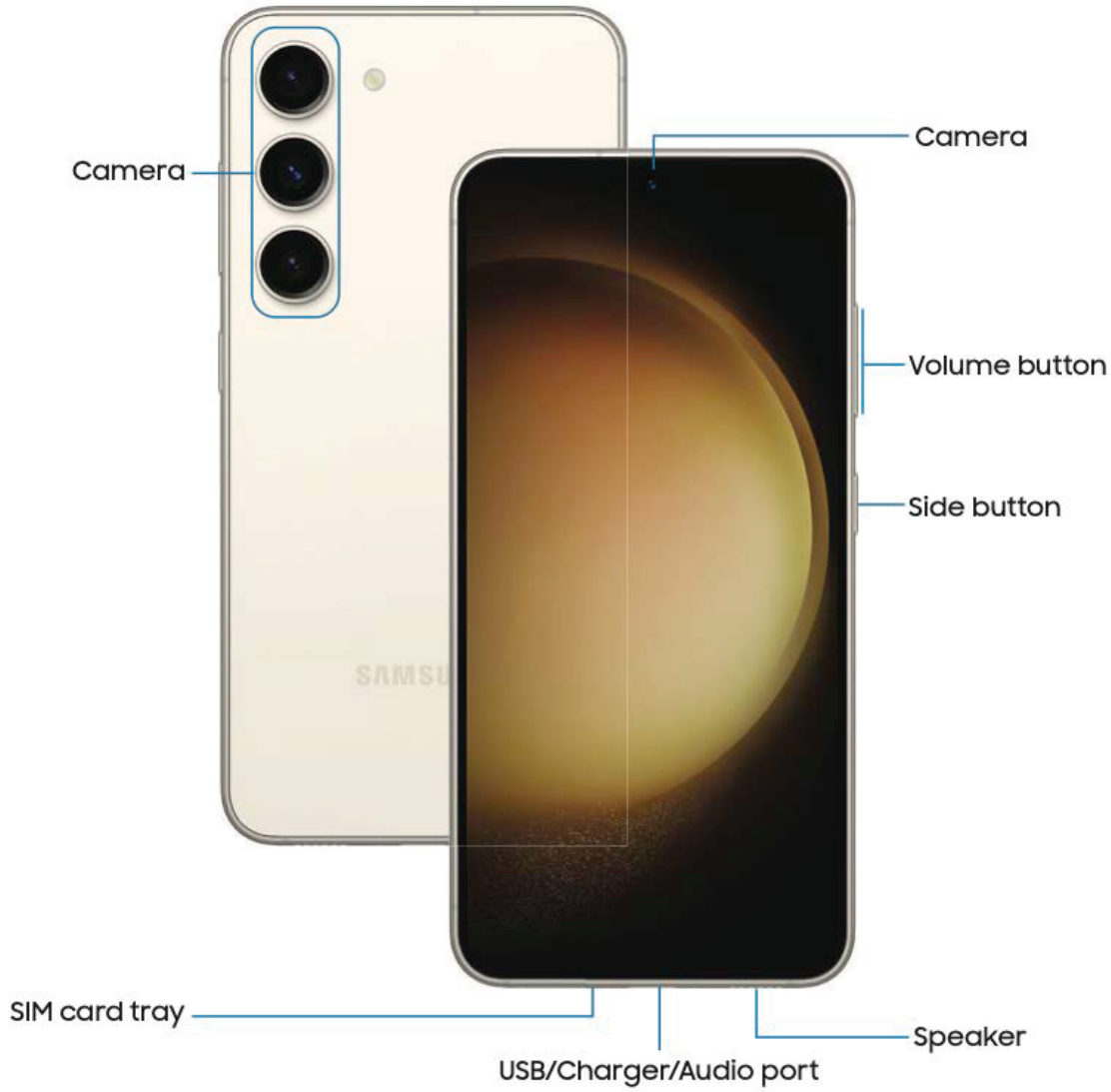
Claim 28

Issued Claim(s)	Public Documentation
28. The wireless device recited in claim 1, wherein the user interface comprises a display.	The Accused Devices comprise the "wireless device recited in claim 1, wherein the user interface comprises a display." *See*, for example, the disclosures identified for claim 1. For further example, the Accused Devices comprise a display. https://www.samsung.com/us/smartphones/galaxy-s23/buy/galaxy-s23-128gb-unlocked-sm-s911uzkaxaa/: Display **Resolution (Main Display)** 2340 x 1080 (FHD+) **Main Display Size** 153.9mm (6.1" full rectangle) / 149.9mm (5.9" rounded corners) **Technology (Main Display)** Dynamic AMOLED 2X **Color Depth (Main Display)** 16M

Claim 29

Issued Claim(s)	Public Documentation
29. The wireless device recited in claim 1, wherein the user interface comprises a speaker.	The Accused Devices comprise the "wireless device recited in claim 1, wherein the user interface comprises a display." *See*, for example, the disclosures identified for claim 1. For further example, the Accused Devices comprise a speaker. *See, e.g.,* https://downloadcenter.samsung.com/content/UM/202404/20240418062905861/SAM_S911_S916_S918_EN_UG_OS14_041624_FINAL_REV_1.1.pdf:

Galaxy S23


Camera
Camera
Volume button
Side button
SIM card tray
USB/Charger/Audio port
Speaker

Claim 30

Issued Claim(s)	Public Documentation
30. The wireless device recited in claim 1, wherein the one or more services comprise a voice service, a messaging service, or a data service.	The Accused Devices comprise the "wireless device recited in claim 1, wherein the one or more services comprise a voice service, a messaging service, or a data service." *See*, for example, the disclosures identified for claim 1. For further example, the Accused Devices support one or more voice services, messaging services, or a data services. *See, e.g.,* https://downloadcenter.samsung.com/content/UM/202404/20240418062905861/SAM_S911_S916_S918_EN_UG_OS14_041624_FINAL_REV_1.1.pdf:

	SIM manager Your wireless service provider and service plan may support the ability to use a dual SIM (two physical SIM cards) or an eSIM (embedded SIM) so that you can manage two mobile accounts without carrying two devices. Options may vary by service provider. Devices that support dual SIM contain two SIM card slots. It may also have a microSD card slot for expandable storage if supported. Devices that support dual SIM will receive software updates that enable the built-in dual SIM capability after launch. Devices that support an eSIM can be programmed to work independently of the physical SIM card in the device. This allows for either the eSIM or the physical SIM card to be used for voice call/text and data. Devices that support eSIM will receive software updates that enable the built-in eSIM capability after launch. ○ From Settings, tap **Connections** > **SIM manager** for the following options: • **SIM cards**: Enable, disable, or rename installed physical SIM cards in your device. • **eSIMs**: Tap + **Add eSIM** to sign up for a new eSIM mobile plan or to add a plan from an old device. • **Primary SIM**: When using multiple SIM cards, set a primary card to be used for calls, texts, and data. • **More SIM settings**: Tap to explore additional management options for your SIM cards.

Claim 31

Issued Claim(s)	Public Documentation
31. The wireless device recited in claim 1, wherein the one or more machine-executable instructions comprise an program.	The Accused Devices comprise the "wireless device recited in claim 1, wherein the one or more machine-executable instructions comprise an application program."

	See, for example, the disclosures identified for claim 1, including, for example, the "Settings" application. *See also, e.g.,* https://source.android.com/docs/core/connect/esim-euicc-api; https://source.android.com/docs/core/connect/esim-error-handling; https://source.android.com/docs/core/connect/esim-mep; https://source.android.com/docs/core/connect/esim-overview: **Make a carrier app** The eUICC APIs in Android 9 make it possible for mobile network operators to create carrier-branded apps to manage their profiles directly. This includes downloading and deleting subscription profiles owned by the carrier, as well as switching to a profile owned by a carrier.

Claim 32

Issued Claim(s)	Public Documentation
32. The wireless device recited in claim 1, wherein the one or more machine-executable instructions comprise an operating system (OS) component, an OS function, an OS service, a modem programming agent, a modem software or firmware agent, an over-the-air (OTA) mobile device parameter programming agent, an Open Mobile Alliance (OMA) agent, a secure communication agent configured to communicate number porting and number provisioning information, a software agent, a firmware agent, or a combination of these.	The Accused Devices comprise the "wireless device recited in claim 1, wherein the one or more machine-executable instructions comprise an operating system (OS) component, an OS function, an OS service, a modem programming agent, a modem software or firmware agent, an over-the-air (OTA) mobile device parameter programming agent, an Open Mobile Alliance (OMA) agent, a secure communication agent configured to communicate number porting and number provisioning information, a software agent, a firmware agent, or a combination of these." *See*, for example, the disclosures identified for claims 1 and 31.

Claim 33

Issued Claim(s)	Public Documentation

33. The wireless device recited in claim 1, wherein the user request comprises an indication of the target credential, a phone number, a user name, a password, an account number, a subscriber name, a company name, at least a portion of a billing address, at least a portion of a social security number, a personal identification number (PIN), or a combination of these.	The Accused Devices comprise the "wireless device recited in claim 1, wherein the user request comprises an indication of the target credential, a phone number, a user name, a password, an account number, a subscriber name, a company name, at least a portion of a billing address, at least a portion of a social security number, a personal identification number (PIN), or a combination of these." *See*, for example, the disclosures identified for claims 1.

Claim 34

Issued Claim(s)	Public Documentation
34. The wireless device recited in claim 1, wherein obtaining the indication of the user request to replace the particular credential of the one or more credentials with the target credential comprises obtaining information from a website.	The Accused Devices comprise the "wireless device recited in claim 1, wherein obtaining the indication of the user request to replace the particular credential of the one or more credentials with the target credential comprises obtaining information from a website." *See*, for example, the disclosures identified for claims 1. For further example, credential information can be obtained from a website, such as by using a link or a QR code. *See, e.g.,* https://www.samsung.com/us/support/answer/ANS10001619/:

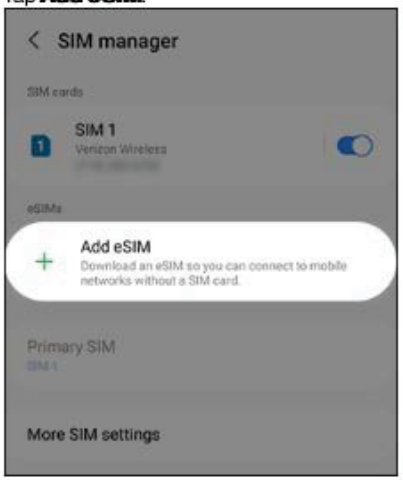
	Add an eSIM Options: Carrier QR Code 1 Navigate to and open **Settings**, then tap **Connections**, then tap **SIM manager**, and then tap **Add eSIM**. 2 Tap **Scan QR code**, and then scan your carrier's QR code. 3 Restart the device to apply the eSIM profile. Carrier Discovery Server 1 Navigate to and open **Settings**, then tap **Connections**, then tap **SIM manager**, and then tap **Add eSIM**. 2 The device will search for a carrier plan. Once it's found, the eSIM profile will download. **Note**: You may need to select your carrier depending on the software version and device. 3 Restart the device to apply the eSIM profile. ; https://www.samsung.com/my/support/mobile-devices/using-your-galaxy-smartphones-with-esim/:

	Scan a QR code Most of the mobile carriers that support eSIM provide a QR code that is assigned to your current mobile plan. Contact your carrier to receive a QR code. To add using the QR code, follow the below steps: 1 Go to Settings > Connections > SIM card manager 2 Tap Add mobile plan 3 Tap Add using QR code 4 Scan a QR code that your carrier provided 5 Your mobile plan is downloaded and activated on eSIM ; https://www.verizon.com/support/knowledge-base-240165/:

1. From a Home screen, swipe up from the center of the display to access all apps.

2. Navigate: **Settings** ⚙ › **Connections** › **SIM manager**.

3. Tap **Add eSIM**.



4. If prompted for a QR code, scan the image below using your device's camera.

5. If prompted, tap **Search for eSIMs**.

6. When 'Add VZW eSIM?' displays, tap **Add**.
→ It may take several minutes to add your plan.
→ If 'No plans found' appears, tap **Try again**.

Claim 35

Issued Claim(s)	Public Documentation
35. The wireless device recited in claim 1, wherein obtaining the indication of the user request to replace the particular credential of the one or more credentials with the target credential comprises obtaining information associated with the user request through the user interface.	The Accused Devices comprise the "wireless device recited in claim 1, wherein obtaining the indication of the user request to replace the particular credential of the one or more credentials with the target credential comprises obtaining information associated with the user request through the user interface." *See*, for example, the disclosures identified for claims 1, 28, 29, and 34.

Claim 36

Issued Claim(s)	Public Documentation
36. The wireless device recited in claim 1, wherein the network element comprises a programming server.	The Accused Devices comprise the "wireless device recited in claim 1, wherein the network element comprises a programming server." *See*, for example, the disclosures identified for claims 1 and 3.

Claim 37

Issued Claim(s)	Public Documentation
37. The wireless device recited in claim 1, wherein initiating the programming session with the network element communicatively coupled to the wireless device over the wireless access network comprises contacting the network element using at least a portion of the one or more credentials associated with the wireless device.	The Accused Devices comprise the "wireless device recited in claim 1, wherein initiating the programming session with the network element communicatively coupled to the wireless device over the wireless access network comprises contacting the network element using at least a portion of the one or more credentials associated with the wireless device." *See*, for example, the disclosures identified for claims 1-3, 5, and 7. For further example, a programming sessions may be initiated with a network element using at least a portion of one or more credentials associated with a device through a "Common Mutual Authentication Procedure. *See, e.g.,* https://www.gsma.com/esim/wp-content/uploads/2022/10/SGP.22-v3.0-1.pdf:

3.0 Common Procedures

3.0.1 Common Mutual Authentication Procedure

This section describes the common mutual authentication call flow that is used in various others places in this document.

In this section the following notations are used:

- SM-XX denotes either an SM-DP+ or an SM-DS.
- CERT.XXauth.SIG denotes either CERT.DPauth.SIG or CERT.DSauth.SIG.
- SK.XXauth.SIG denotes either SK.DPauth.SIG or SK.DSauth.SIG.
- CERT.XX.TLS denotes either CERT.DP.TLS or CERT.DS.TLS.
- SK.XX.TLS denotes either SK.DP.TLS or SK.DS.TLS.
- ESXX denotes either ES9+ when communicating with an SM-DP+ or an ES11 when communicating with an SM-DS.
- SM-XX SubCA Certificates denote one or more of CERT.CISubCA.SIG, CERT.DPSubCA.SIG, CERT.DSSubCA.SIG, or SubCA Certificates in a trust chain from CERT.XX.TLS to a public RootCA.

This procedure implies the use of CERT.XXauth.SIG. Following this common mutual authentication procedure, if any other Certificates of the SM-XX are used, e.g., the CERT.DPpb.SIG, these Certificates SHALL have a trust chain leading to the same eSIM CA RootCA Certificate as CERT.XXauth.SIG.

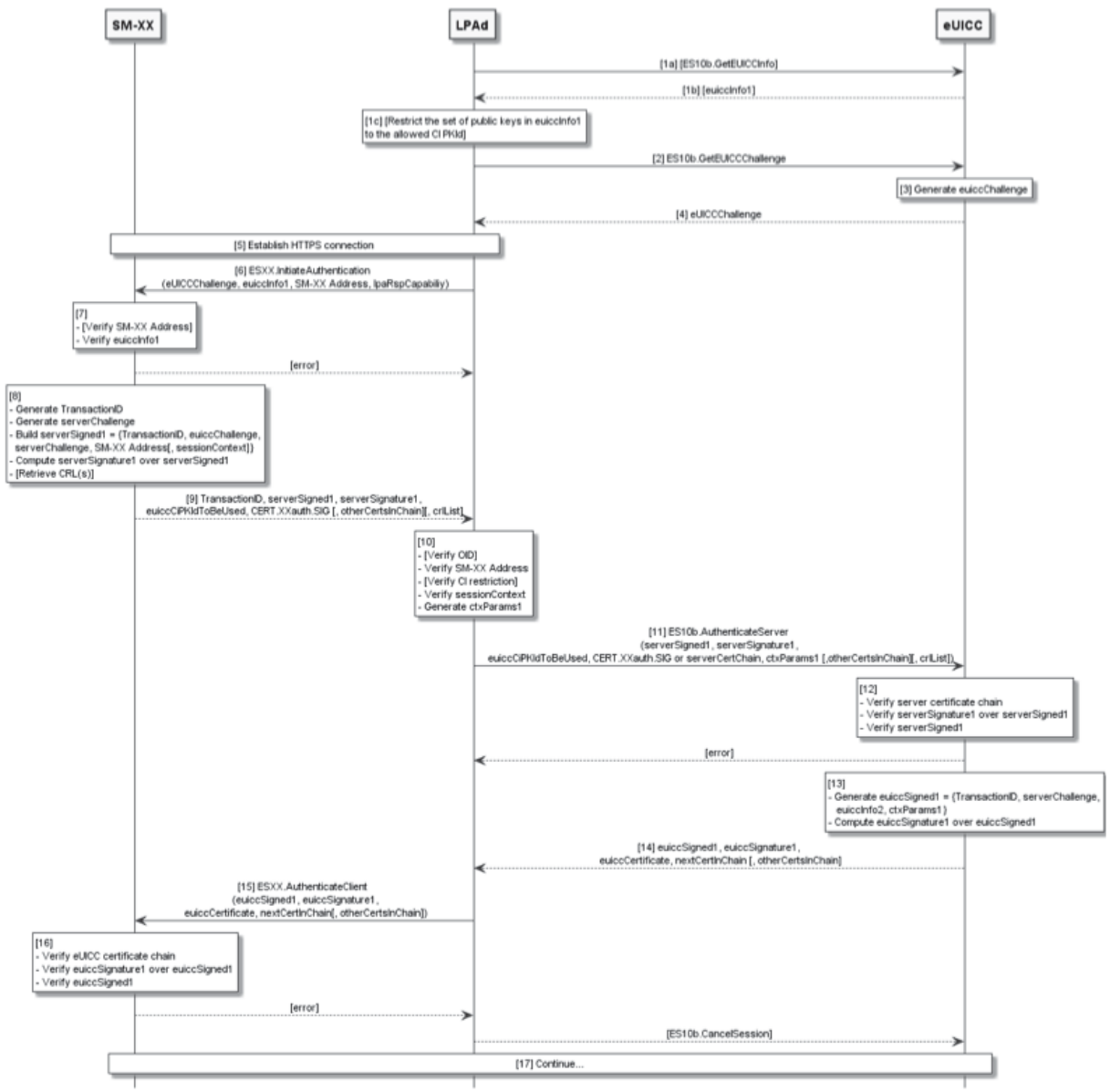


Figure 8a: Common Mutual Authentication Procedure

Claim 38

Issued Claim(s)	Public Documentation
38. The wireless device recited in claim 1, wherein initiating the programming session with the network element communicatively coupled to the wireless device over the wireless access network comprises contacting the network element using a temporary credential.	The Accused Devices comprise the "wireless device recited in claim 1, wherein initiating the programming session with the network element communicatively coupled to the wireless device over the wireless access network comprises contacting the network element using a temporary credential." *See*, for example, the disclosures identified for claims 1-3, 5, 7, and 37.

Claim 39

Issued Claim(s)	Public Documentation
39. The wireless device recited in claim 38, wherein, when executed by the one or more processors, the one or more machine-executable instructions further cause the one or more processors to obtain the temporary credential from memory.	The Accused Devices comprise the "wireless device recited in claim 38, wherein, when executed by the one or more processors, the one or more machine-executable instructions further cause the one or more processors to obtain the temporary credential from memory." *See*, for example, the disclosures identified for claim 38.

Claim 40

Issued Claim(s)	Public Documentation
40. The wireless device recited in claim 38, wherein, when executed by the one or more processors, the one or more machine-executable instructions further cause the one or more processors to obtain the temporary credential from a network system communicatively coupled to the wireless device.	The Accused Devices comprise the "wireless device recited in claim 38, wherein, when executed by the one or more processors, the one or more machine-executable instructions further cause the one or more processors to obtain the temporary credential from a network system communicatively coupled to the wireless device." *See*, for example, the disclosures identified for claim 38.

Claim 41

Issued Claim(s)	Public Documentation
41. The wireless device recited in claim 1, wherein initiating the programming session with the network element communicatively coupled to the wireless device over the wireless access network comprises contacting the network element using a default credential.	The Accused Devices comprise the "wireless device recited in claim 1, wherein initiating the programming session with the network element communicatively coupled to the wireless device over the wireless access network comprises contacting the network element using a default credential." *See*, for example, the disclosures identified for claims 1-3, 5, 7, and 37.

Claim 42

Issued Claim(s)	Public Documentation
42. The wireless device recited in claim 1, wherein initiating the programming session with the network element communicatively coupled to the wireless device over the wireless access network comprises communicating with the network element over the wireless access network.	The Accused Devices comprise the "wireless device recited in claim 1, wherein initiating the programming session with the network element communicatively coupled to the wireless device over the wireless access network comprises communicating with the network element over the wireless access network." *See*, for example, the disclosures identified for claims 1-3, 5, 7, and 37.

Claim 43

Issued Claim(s)	Public Documentation
43. The wireless device recited in claim 1, wherein initiating the programming session with the network element communicatively coupled to the wireless device over the wireless access network comprises communicating with the network element over a Wi-Fi network.	The Accused Devices comprise the "wireless device recited in claim 1, wherein initiating the programming session with the network element communicatively coupled to the wireless device over the wireless access network comprises communicating with the network element over a Wi-Fi network." *See*, for example, the disclosures identified for claims 1-3, 5, 7, and 37.

	For further example, one way to communicate with the network element is via Wi-Fi. *See, e.g.,* https://www.t-mobile.com/support/devices/device-troubleshooting/samsung-on-device-activation-troubleshooting **Phone with Dual SIM** Get help if you can't activate your eSIM. For help with these steps, pick your device on the **Device tutorials** page and use the search bar. 1. If the device wasn't purchased from T-Mobile, make sure that it's unlocked. 2. Make sure you're connected to a Wi-Fi network and the internet works. 3. Update the device software to the latest version. 4. Restart your device and try again. 5. Select the specific errors that you're getting and follow any steps.

Claim 44

Issued Claim(s)	Public Documentation
44. The wireless device recited in claim 1, wherein initiating the programming session with the network element communicatively coupled to the wireless device over the wireless access network comprises communicating with the network element through a voice call.	The Accused Devices comprise the "wireless device recited in claim 1, wherein initiating the programming session with the network element communicatively coupled to the wireless device over the wireless access network comprises communicating with the network element through a voice call." *See*, for example, the disclosures identified for claims 1-3, 5, 7, and 37.

Claim 45

Issued Claim(s)	Public Documentation
45. The wireless device recited in claim 1, wherein, when executed by the one or more processors, the one or more machine-executable instructions further cause the one or more processors to at least assist in restricting communications	The Accused Devices comprise the "wireless device recited in claim 1, wherein, when executed by the one or more processors, the one or more machine-executable instructions further cause the one or more processors to at least assist in restricting communications over the wireless access network until the updated credential has been obtained." *See*, for example, the disclosures identified for claims 1 and 6.

over the wireless access network until the updated credential has been obtained.	

Claim 46

Issued Claim(s)	Public Documentation
46. The wireless device recited in claim 1, wherein the target credential comprises a configuration state indicator.	The Accused Devices comprise the "wireless device recited in claim 1, wherein the target credential comprises a configuration state indicator." *See*, for example, the disclosures identified for claim 1. For further example, credentials compromise various states. *See, e.g.,* https://www.gsma.com/esim/wp-content/uploads/2022/10/SGP.22-v3.0-1.pdf:

3.1.6 Profile Lifecycle at SM-DP+

The previous sections provide detailed procedures associated with Remote Provisioning. Each Profile has state information on the SM-DP+ associated with it during the provisioning into an eUICC. The Profile lifecycle state can be one of the states listed in the following table.

Additional states and additional or customised ES2+ functions MAY be agreed between the Operator and the SM-DP+.

State Name	Description
Available	The Profile is available in the inventory of the SM-DP+.
Allocated	The Profile is reserved for downloading without being linked to an EID.
Linked	The Profile is reserved for downloading and is linked to an EID.
Confirmed	The Profile is reserved for downloading (linked or not linked to an EID) with Matching ID and Confirmation Code if required.
Released	The Profile is ready for download and installation after Network Configuration by the Operator (e.g.: HLR Registration).
Downloaded	The Bound Profile was delivered to the LPA.
Installed	The Profile was successfully installed on the eUICC.
Error	The Profile has not been installed because of one of the following error cases: - Confirmation Code Retry Limit exceeded - Download Retry Limit exceeded - End User Rejection - Permanent error during download and installation
Unavailable	The Profile cannot be reused anymore by the SM-DP+.

Table 6b: Profile State in the SM-DP+

235

Claim 47

Issued Claim(s)	Public Documentation
47. A non-transitory computer-readable storage medium storing one or more machine-executable instructions that, when executed by one or more processors of a wireless device, cause the one or more processors to:	The Accused Devices comprise a "non-transitory computer-readable storage medium storing one or more machine-executable instructions that, when executed by one or more processors of a wireless device, cause the one or more processors to." *See*, for example, the disclosures identified for claim 1.
obtain, through a user interface, an indication of a user request to replace a particular credential of one or more credentials, for authorizing the wireless device to use a wireless access network to access one or more services, with a target credential;	The Accused Devices comprise a "obtain, through a user interface, an indication of a user request to replace a particular credential of one or more credentials, for authorizing the wireless device to use a wireless access network to access one or more services, with a target credential." *See*, for example, the disclosures identified for claim 1.
detect a network-provisioning state change; and	The Accused Devices comprise a "detect a network-provisioning state change." *See*, for example, the disclosures identified for claim 1.
based on the detected network-provisioning state change, automatically determine that the particular credential does not match the target credential,	The Accused Devices comprise a "based on the detected network-provisioning state change, automatically determine that the particular credential does not match the target credential." *See*, for example, the disclosures identified for claim 1.
initiate a programming session with a network element communicatively coupled to the wireless device over a wireless access network,	The Accused Devices comprise a "initiate a programming session with a network element communicatively coupled to the wireless device over a wireless access network." *See*, for example, the disclosures identified for claim 1.
obtain an updated credential from the network element, and	The Accused Devices comprise a "obtain an updated credential from the network element." *See*, for example, the disclosures identified for claim 1.
assist in storing, in memory, the updated credential as the particular credential.	The Accused Devices comprise a "assist in storing, in memory, the updated credential as the particular credential." *See*, for example, the disclosures identified for claim 1.

Claim 48

Issued Claim(s)	Public Documentation
48. The wireless device of claim 1, wherein the memory configured to store the one or more credentials comprises a protected memory that does not allow direct user modification of the particular credential.	The Accused Devices comprise a "wireless device of claim 1, wherein the memory configured to store the one or more credentials comprises a protected memory that does not allow direct user modification of the particular credential." *See*, for example, the disclosures identified for claim 1.