

# Mobility Based Policy Control for Overlay Deployments (Smp)

Ericsson Service-Aware Policy Controller

## FACILITY DESCRIPTION

## **Copyright**

© Ericsson España, S.A. 2017. All rights reserved. No part of this document may be reproduced in any form without the written permission of the copyright owner.

## **Trademark List**

All trademarks mentioned herein are the property of their respective owners. These are shown in the document Trademark Information.

## **Abstract**

This document describes the Mobility Based Policy Control for Overlay Deployments function provided by the SAPC.



# Contents

<b>1</b>	<b>Function</b>	<b>1</b>
1.1	Overview	1
1.2	Smp Session Access Control	3
1.3	PDN-GW Selection	3
1.4	SPID Selection	4
1.5	Subscriber Profile Handling	6
<b>2</b>	<b>Network Deployments</b>	<b>6</b>
<b>3</b>	<b>Traffic Cases</b>	<b>6</b>
3.1	Smp Session Lifecycle at UE Attach or PDN Connectivity	7
3.2	Smp Session Lifecycle at Inter SGSN-MME TAU or Handover	9
3.3	Error Handling	12
<b>4</b>	<b>Restrictions</b>	<b>13</b>
	<b>Reference List</b>	<b>15</b>





# 1 Function

## 1.1 Overview

The Mobility Based Policy Control for Overlay Deployments function provides direct communication between the SAPC and the SGSN-MME by using the Smp interface. The SAPC works in Smp only mode and only serves the Smp traffic and other PCRFs in the network serve Gx, Rx, and Sy traffic.

This function enables the SGSN-MME to get the following policy decisions from the SAPC:

- The preferred list of GWs, and
- The SPID to be selected for a specific user based on subscription type, device type, APN, or location, for better network resource efficiency.

The function enables new innovative use cases, for example:

- Dynamically allocation of the best radio resources on a per-user, per-terminal basis.
- Preferred access for subscribers.
- Dynamic selection of the GW based on, for example, the subscriber profile.

The following figure shows an overview of Network Elements providing Mobility Based Policy Control for Overlay Deployments function:

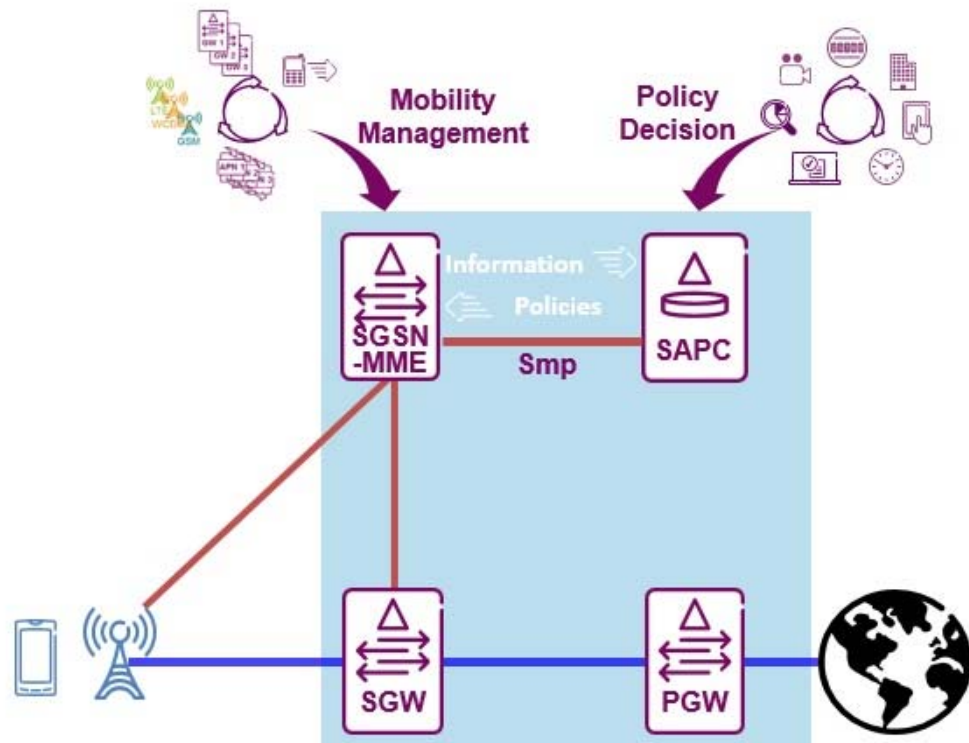


Figure 1 Overview of Mobility Based Policy Control for Overlay Deployments

An Smp session is based on the PDN connection and established between the SGSN-MME and the SPC.

The life cycle of an Smp session includes its establishment and termination. The SPC does not support currently session modification nor reauthorization.

The SGSN-MME establishes an Smp session when:

- UE Attach or PDN connectivity.
- The UE moves to a new SGSN-MME through Inter SGSN-MME Tracking Area Update (TAU) or handover.

**Note:** In the case of inter SGSN-MME TAU or Handover session establishment, the SGSN-MME sends only the International Mobile Subscriber Identity (IMSI) to the SPC.

The SGSN-MME terminates an Smp session when:

- The associated PDN is deleted owing to UE Detach or PDN disconnection.
- The UE moves to a new MME owing to TAU, handover, or it moves to a new Radio Access Type (RAT).
- An abnormal situation occurs on the Smp interface.



## 1.2 Smp Session Access Control

Smp session Access Control is used to allow or reject Smp session establishment. Even if Smp session is rejected, SGSN-MME can continue with the IP-CAN session establishment towards the PGW.

Smp session Access Control policies are evaluated according to the following precedence allocation and applying permit overrides algorithm among them (that is, if any policy evaluates to true, the Smp session is authorized):

1. Subject policy locator.
2. Subject group policy locator. All the active subscriber groups are considered.

Therefore, it is recommended to configure Dynamic Group Selection policies to evaluate only the desired subscriber group policies.

3. Global policy locator.

In case there are conflicts among the rules within a policy, the result for the policy depends on the Rule combining algorithm configured. See Solving Policies Conflicts section in *Subscription and Policy Management*.

In case there are no Smp Session Access Control policies configured, the Smp session is authorized.

## 1.3 PDN-GW Selection

With the PDN-GW selection function, the SAPC can select the IP address (IPv4 and/or IPv6) and/or FQDN of a list of PDN-GWs for a UE when the UE attaches to the network.

**Note:** The maximum number of PDN-GWs in a list is 32.

The SAPC allows to select the list of PDN-GWs based on the following information:

- Subscriber profile, for example, subscriber with content filtering or Deep Packet Inspection (DPI) can be statically associated with a certain PDN-GW,
- User location, for example, users located in a concert hall, stadium, or festival,
- International Mobile Subscriber Identity (IMSI),
- International Mobile Station Equipment Identity (IMEI),
- Device type,
- APN,
- Other data received through the Smp interface

The SAPC selects the list of PDN-GWs applying the mechanism for controls using both Policies and Qualification Data explained in Selection of Data to apply to the Subscriber section in Subscription and Policy Management.

The PDN-GW selection is performed only in the Smp session establishment procedure in the UE Attach or PDN connectivity scenario. During the Smp session lifetime, the selected list of PDN-GWs cannot be changed.

The following figure shows how to perform the PDN-GW selection:

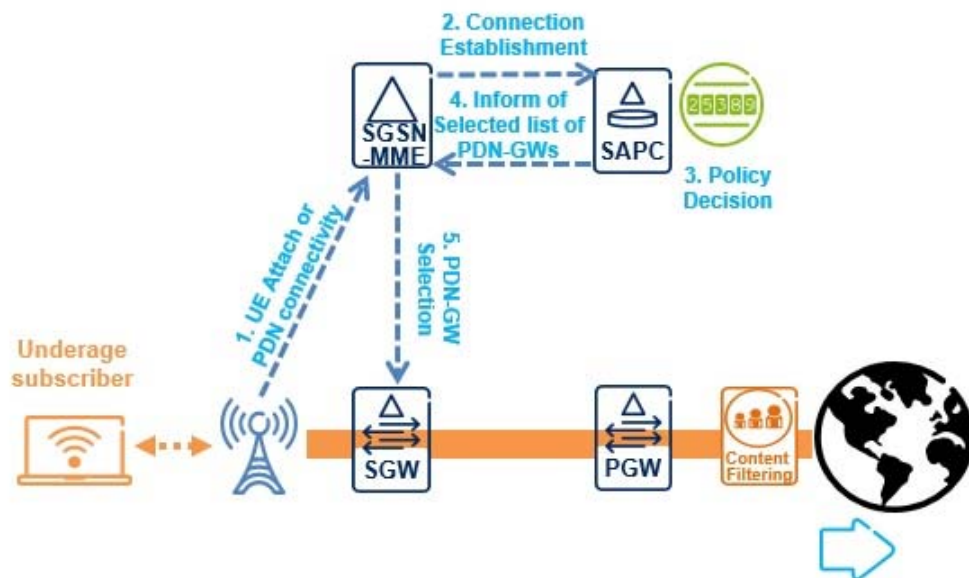


Figure 2 PDN-GW Selection

- 1–2: When a UE attaches to the network, the SGSN-MME establishes the connection to the SAPC depending on the APN.
- 3–4: The SAPC makes a policy decision to select a list of PDN-GWs, for example the PDN-GWs connected with Content Filtering function for the underage subscriber, and informs the SGSN-MME of the list.
- 5: The SGSN-MME selects one PDN-GW from the list provided by the SAPC for the subscriber.

## 1.4 SPID Selection

The SPID selection function enables the SAPC to control the camp priorities in Idle mode and inter-RAT/inter-frequency handover in Active mode for subscribers. This index is mapped by the eNodeB (E-UTRAN), RNC (UTRAN), or BSC (GERAN) to locally defined configuration. For more information, see Reference [3] and Reference [4]. This increases the flexibility and service awareness for radio optimizations.





The SAPC allows to select the SPID based on the following information:

- Subscriber profile, for example, subscriber with content filtering or Deep Packet Inspection (DPI) can be statically associated with a certain PDN-GW,
- User location, for example, users located in a concert hall, stadium, or festival,
- International Mobile Subscriber Identity (IMSI),
- International Mobile Station Equipment Identity (IMEI),
- Device type,
- APN,
- Other data received through the Smp interface

The SAPC selects the SPID applying the mechanism for controls using both Policies and Qualification Data explained in Selection of Data to apply to the Subscriber section in *Subscription and Policy Management*.

The following figure shows how to perform the SPID selection based on user information provided during the Smp session establishment:

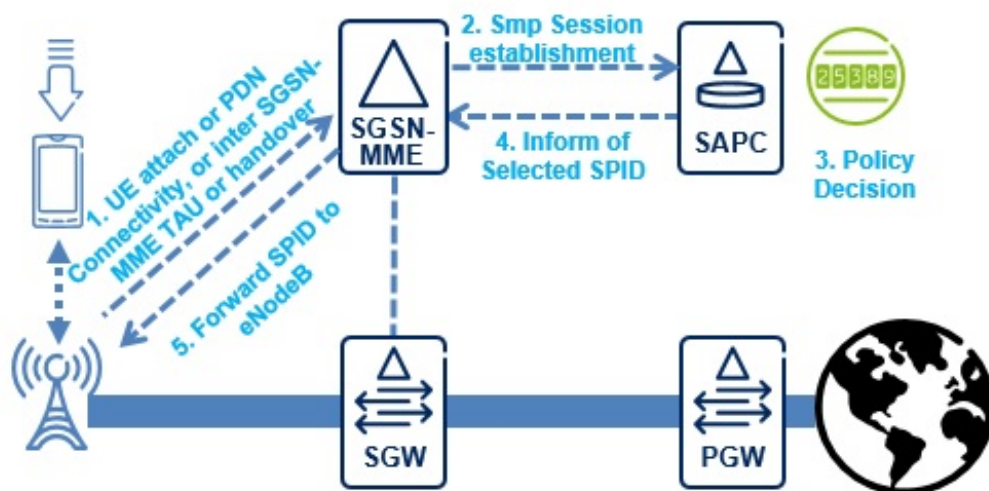


Figure 3 SPID Selection

- 1–2: During the UE attach or PDN connectivity, or during the inter-SGSN-MME TAU or handover procedures, the SGSN-MME receives the location information and reports the ULI to the SAPC, only during the Smp session establishment.
- 3–4: The SAPC makes a policy decision to select an SPID, and informs the SGSN-MME of the selected SPID.
- 5: The SGSN-MME forwards the selected SPID to the eNodeB, and finally to the UE.



## 1.5 Subscriber Profile Handling

The subscriber and subscriber group data can be stored in the SAPC internal or external database.

The SAPC uses the International Mobile Subscriber Identity (IMSI) to obtain the subscriber ID. This subscriber ID is used to access to the subscriber profile.

The subscriber can be associated with subscriber groups, having the possibility to specify the date and time, and the subscriber group priority.

Also, the SAPC supports dynamic selection of the subscribed groups by using Dynamic Group Selection policies.

The autoprovisioning and subscriber unknown functions are also applicable to Smp session procedures.

When any subscriber data is updated, the SAPC does not perform Smp reauthorization to check whether any data need to be added or removed, so updated subscriber data will be applied at next Smp session establishment.

When a subscriber is removed, the SAPC does not indicate the SGSN-MME to terminate the associated Smp sessions.

For more information, refer to [Subscription and Policy Management](#).

## 2 Network Deployments

The SAPC supports the Mobility Based Policy Control for Overlay Deployments function in the following Network Elements:

- Ericsson SGSN-MME

## 3 Traffic Cases

This section describes traffic cases for Smp sessions.

The preconditions to all traffic cases are as follows:

- The availability of this function in the SAPC is under license control.

Only the significant attributes for these traffic cases are described in the following sections. For more information on the supported interfaces, refer to the corresponding interface description documents.

**Note:** The Session-Id AVP is mandatory for all the messages in the Smp protocol. The Session-Id AVP is globally unique and used to identify an Smp session.

### 3.1 Smp Session Lifecycle at UE Attach or PDN Connectivity

This traffic case shows the Smp session lifecycle at the UE Attach or PDN connectivity scenario. The Smp session lifecycle includes Smp session establishment and termination.

The following figure shows the Diameter messages exchanged between the SAPC and the SGSN-MME.

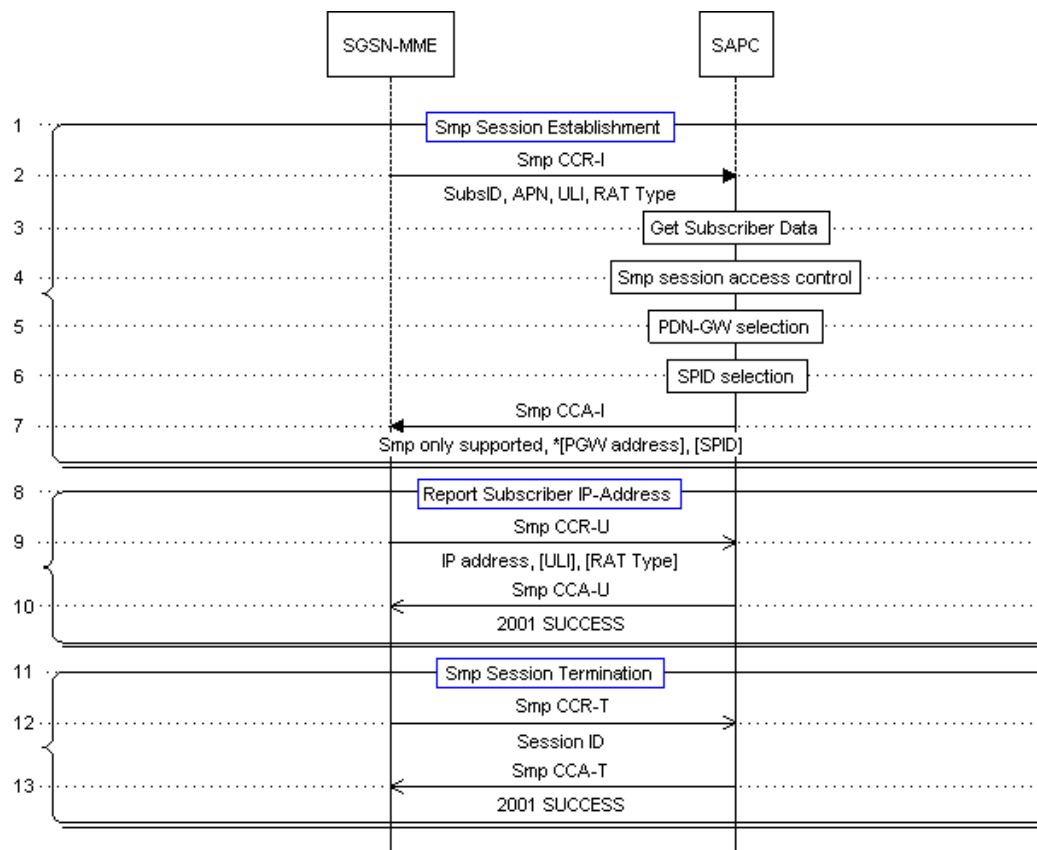


Figure 4 Smp Session Lifecycle at UE Attach or PDN Connectivity

## Smp Session Establishment

- 2: The SAPC receives an Smp CCR-I message from the SGSN-MME, indicating the Smp session establishment. The main information that the SGSN-MME provides includes:

- Subscription-Id AVP: This indicates the subscription ID that the SAPC uses to locate the subscriber profile. This AVP can contain one or several traffic identities (IMSI and MSISDN) received from the Smp sessions. The SGSN-MME always include, at least, the IMSI.
- Called-Station-Id AVP: This indicates the APN for the IP-CAN session.
- 3GPP-User-Location-Info AVP: This indicates the ULI, such as RAI, TAI, and ECGI.
- RAT-Type AVP: This indicates the RAT that is serving the UE.

The SAPC does not receive the IP address in the Smp CCR-I message because the IP address is not assigned.

Upon reception of the Smp CCR-I message, the SAPC checks the license that controls the handling of Smp traffic.

- 3: The SAPC looks for the subscriber and subscriber group profile.

The SAPC maintains a mapping between the different subscriber traffic identities and the subscriber ID. The SAPC uses the International Mobile Subscriber Identity (IMSI) to obtain the subscriber ID. The subscriber ID obtained is used to access to the subscriber profile.

The SAPC evaluates dynamic group selection policies to obtain the set of active subscriber groups applicable to the subscriber.

If the subscriber is not found either in the SAPC internal database or in an external database, refer to Subscribers not known by the SAPC section in Subscription and Policy Management.

- 4: The SAPC performs Smp session access control.

If the SAPC determines that the Smp session cannot be authorized and the IP-CAN session establishment must continue, the SAPC returns Result-Code 4011 (DIAMETER\_CREDIT\_CONTROL\_NOT\_APPLICABLE) in the CCA-I message and does not evaluate any further control. The SGSN-MME then removes the Smp session and continues the PDN connection creation procedure in the UE Attach or PDN connectivity scenario as if no Smp session was created at all. In this case, the SGSN-MME does not send the CCR-T message to terminate the Smp session.

- 5: The SAPC performs PDN-GW selection and includes the selected list of PDN-GWs within the MIP6-Agent-Info AVPs.



- 6: The SAPC performs SPID selection and includes the selected SPID within the RAT-Frequency-Selection-Priority-ID AVP.
- 7: The SAPC sends the Smp CCA-I message to the SGSN-MME including the information previously computed. The SAPC indicates the support of Smp interface only within the Bearer-Control-Mode AVP.

#### **Report Subscriber IP Address**

- 9: The SAPC receives an Smp CCR-U message from the SGSN-MME, including the subscriber IP address, the ULI and the RAT type.
- 10: The SAPC acknowledges the request by sending an Smp CCA-U message with a Result-Code 2001 (DIAMETER\_SUCCESS). The SAPC does not evaluate any policy control at reception of this message.

#### **Smp Session Termination**

- 12: The SAPC receives an Smp CCR-T message from the SGSN-MME to terminate the Smp session.
- 13: The SAPC acknowledges the request by sending an Smp CCA-T message with a Result-Code 2001 (DIAMETER\_SUCCESS).

## **3.2 Smp Session Lifecycle at Inter SGSN-MME TAU or Handover**

The traffic case shows the Smp session lifecycle at the Inter SGSN-MME TAU or Handover scenario. The Smp session lifecycle includes Smp session establishment and termination.

The following figure shows the Diameter messages exchanged between the SAPC and the SGSN-MME.

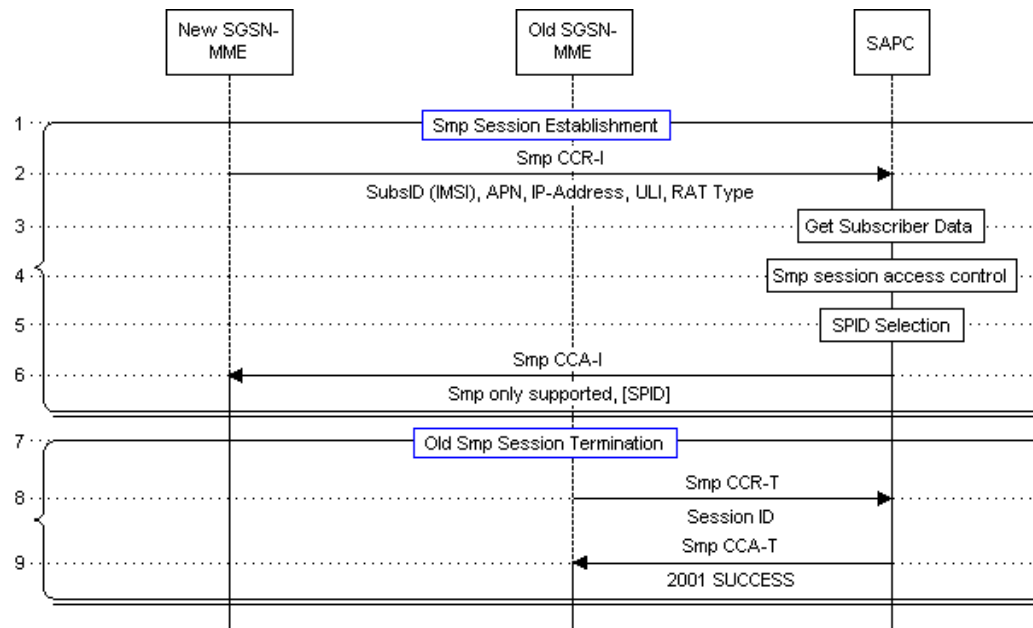


Figure 5 Smp Session Lifecycle at Inter SGSN-MME TAU or Handover

### Smp Session Establishment

- 2: When an Inter SGSN-MME TAU or Handover is performed, the SAPC receives an Smp CCR-I message from the new SGSN-MME, indicating the Smp session establishment. The main information that the SGSN-MME provides includes:
  - Subscription-Id AVP: This indicates the subscription ID that the SAPC uses to locate the subscriber profile. This AVP contains the IMSI traffic identity.
  - Called-Station-Id AVP: This indicates the APN for the IP-CAN session.
  - 3GPP-User-Location-Info AVP: This indicates the ULI, such as RAI, TAI, and ECGI.
  - RAT-Type AVP: This indicates the RAT that is serving the UE.
  - Framed-IP-Address AVP and/or Framed-IPv6-Prefix AVP: This indicates the UE IPv4 address and/or IPv6 prefix. The SGSN-MME always includes the subscriber IP address in the Inter SGSN-MME TAU or Handover scenario.

Upon reception of the Smp CCR-I message, the SAPC checks the license that controls the handling of Smp traffic is active.

- 3: The SAPC looks for the subscriber and subscriber group profile.



The SAPC maintains a mapping between the different subscriber traffic identities and the subscriber ID. The SAPC uses the International Mobile Subscriber Identity (IMSI) to obtain the subscriber ID. The subscriber ID obtained is used to access to the subscriber profile.

The SAPC evaluates dynamic group selection policies to obtain the set of active subscriber groups applicable to the subscriber.

If the subscriber is not found either in the SAPC internal database or in an external database, refer to Subscribers not known by the SAPC section in *Subscription and Policy Management*.

- 4: The SAPC performs Smp session access control.

If the SAPC determines that the Smp session cannot be authorized and the IP-CAN session establishment must continue, the SAPC returns Result-Code 4011 (DIAMETER\_CREDIT\_CONTROL\_NOT\_APPLICABLE) in the CCA-I message and does not evaluate any further control. The SGSN-MME then removes the Smp session and continues the PDN connection creation procedure in the UE Attach or PDN connectivity scenario as if no Smp session was created at all. In this case, the SGSN-MME does not send the CCR-T message to terminate the Smp session.

- 5: The SAPC performs SPID selection and includes the selected SPID within the RAT-Frequency-Selection-Priority-ID AVP.
- 6: The SAPC sends the Smp CCA-I message to the SGSN-MME including the information previously computed. The SAPC indicates the support of Smp interface only within the Bearer-Control-Mode AVP.

### Old Smp Session Termination

- 8: The SAPC receives an Smp CCR-T message from the old SGSN-MME to terminate the old Smp session.
- 9: The SAPC acknowledges the request by sending an Smp CCA-T message with a Result-Code 2001 (DIAMETER\_SUCCESS).

For the subsequent signalling flows, see Section 3.1 on page 7 from Smp Session Termination.



### 3.3 Error Handling

Table 1 Error Handling

Error Condition	Action	Code
The SAPC determines that the SGSN-MME must continue the IP-CAN session and drop the Smp session.	The SAPC returns a CCA with a specific Result-Code	DIAMETER_CREDIT_CONTROL_NOT_APPLICABLE = 4011
A request is received with an AVP with an invalid value in its data portion.	The SAPC returns a CCA indicating an error, including one or more Failed-AVP AVPs containing the AVPs that caused the failure.	DIAMETER_INVALID_AVP_VALUE = 5004
When a request is received including an AVP that is not required to process that request, that AVP is ignored and the request is processed as usual. On the contrary, when a request does not include an AVP that is required to process such request, the SAPC returns a response including Result-Code DIAMETER_MISSING_AVP and the Failed-AVP AVP.	The SAPC returns a CCA indicating an error.	DIAMETER_MISSING_AVP = 5005





Error Condition	Action	Code
This error is returned when the SAPC receives a request and detects an internal error which does not allow to continue processing a request, or the license is not active.	The SAPC returns a CCA indicating an error.	DIAMETER_UNABLE_TO_COMPLY = 5012
This error is returned when the subscriber specified in Subscription-Id AVP is not known in the SAPC at session activation or modification.	The SAPC returns a CCA indicating an error.	DIAMETER_USER_UNKNOWN = 5030

## 4 Restrictions

- No policies are executed on session modification.
- Subscriber profile update or ToD session reauthorization do not trigger a session reauthorization towards the SGSN-MME.





## Reference List

### Ericsson Documents

- [1] Subscription and Policy Management
- [2] Configuration Guide for Mobility Based Policy Control for Overlay Deployments (Smp)

### Standards

- [3] General Packet Radio Service (GPRS); Service Description; Stage 2, 3GPP TS 23.060
- [4] General Packet Radio Service (GPRS) enhancements for Evolved Universal Terrestrial Radio Access Network (E-UTRAN) access, 3GPP TS 23.401