

Integration with OCS for Monetary Spending Limit Reporting (Sy)

Ericsson Service-Aware Policy Controller

Facility Description

Copyright

© Ericsson AB 2018. All rights reserved. No part of this document may be reproduced in any form without the written permission of the copyright owner.

Disclaimer

The contents of this document are subject to revision without notice due to continued progress in methodology, design and manufacturing. Ericsson shall have no liability for any error or damage of any kind resulting from the use of this document.

Trademark List

All trademarks mentioned herein are the property of their respective owners. These are shown in the document [Trademark Information](#).



Contents

1	Integration with OCS for Monetary Spending Limit Reporting (Sy) Introduction	1
2	Integration with OCS Function	2
2.1	Overview	2
2.2	Policy Counter	3
2.3	Determination of Policy and Charging Control Information to Install in PCEF	4
2.4	Ericsson Sy: Integration with Charging System	6
2.4.1	Policy Group	7
2.4.2	Subscriber Data Distribution	8
2.5	Integration with Multiple Online Charging Systems	12
3	Network Deployments	14
4	Traffic Cases	15
4.1	Bill Shock Prevention	16
4.1.1	Use of Policy Counters Status during IP-CAN session Life Cycle	16
4.1.2	Policy Counter Status Change	19
4.2	Centralized Management of Operator Service Offering	21
4.2.1	Use of Policy Counters and Policy Group Information during IP-CAN session Life Cycle	21
4.2.2	Policy Counter Status Change	25
4.2.2.1	Counter Status Change, Bearer QoS Change	25
4.2.3	Policy Group Update: Turbo Button Purchase	26
4.2.3.1	New Policy Group Added	27
4.3	Operator Network Policies, Abusers Example	28
4.4	Connectivity with the Online Charging System	31
4.5	Failure Handling	33
4.5.1	SLR Failure	34
4.5.2	SNR Failure	35
4.5.3	STR Failure	36
5	Reference List	37





1 Integration with OCS for Monetary Spending Limit Reporting (Sy) Introduction

This document describes the Charging and Policy Control functionality provided by the SAPC when using monetary spending limit reporting over 3GPP Sy interface or ESy interface with an Online Charging System.

This function provides Policy and Charging control differentiated per subscriber taking into account information about the monetary balance of the subscriber account stored in the Online Charging System. The control is performed basing the Policy decisions applying to IP session life cycle (Bearer QoS control, Bandwidth Management, and so forth) on the account status information received from the Online Charging System.



2 Integration with OCS Function

2.1 Overview

Service offers are moving from simple Data Products based on volume addressed to all mobile broadband subscribers to differentiated Data Products tailored to specific subscribers' requirements for bandwidth, volume, and willingness to pay.

With Integration with the Online Charging System for Monetary Spending Limit Reporting, the SAPC is enabled to perform Policy (such as Bearer QoS Control, Access Control) control decisions based on information only available in the Online Charging System, that is, based on real-time information about the status of the monetary balance of a particular subscriber.

The Integration with the Online Charging System for Monetary Spending Limit Reporting function is centered around the Sy Reference Point. The Sy Reference Point is a Diameter interface between the Online Charging System and the SAPC that enables the transport of the status of the subscriber account (indication of the monetary balance) in a piece of information called Policy Counter.

The SAPC supports two versions for the Sy Reference Point: the Ericsson Sy - a pre-standard version of 3GPP Sy; and 3GPP Sy compliant version of the interface *Policy and Charging Control: Spending Limit Reporting over Sy Reference Point*.

The following picture shows a simplified network overview with the Sy Reference Point:

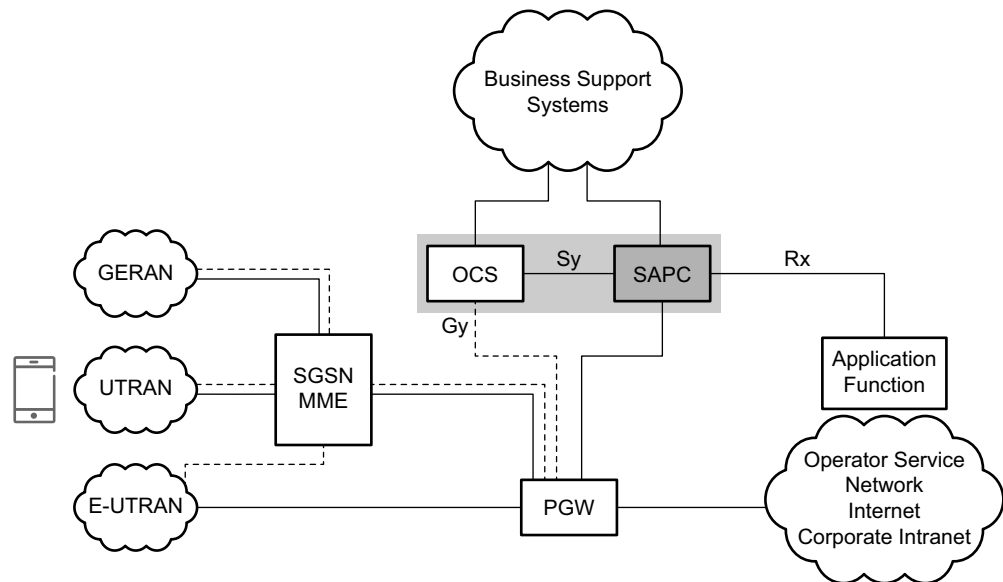


Figure 1 Network Overview for Sy Reference Point

During the establishment of the first IP-CAN session for a subscriber, the SAPC determines whether the data to install in the PCEF depends on monetary balance status information of the subscriber stored in the Online Charging System. If it is so, the SAPC first selects the Online Charging System, then sends a request to the selected one and uses the received information, together with the subscriber data stored in the SAPC, to decide the data to install in the PCEF.

Subsequent IP-CAN session updates or new IP-CAN session establishments are processed in the SAPC considering the balance status previously obtained from the Online Charging System and temporarily stored in the Sy session or ESy session for the subscriber, being not necessary to contact again the Online Charging System. The same happens in a multiple Gx scenario at new Gx session establishment or modification for an ongoing IP-CAN session.

Updates in the balance account of the subscriber are notified to the SAPC by the Online Charging System, so that the SAPC can reevaluate its policies and determine if the ongoing IP-CAN sessions must be updated.

The SAPC releases the balance status information temporarily stored when the last active IP-CAN session is terminated for the subscriber.

2.2 Policy Counter

Policy control decisions for a subscriber can vary depending on Online Charging System information, as for example spending thresholds reached for a subscribed Data Product.

A Policy Counter is the piece of information that transports thresholds information. The Policy Counter allows the SAPC to be informed in real time by



the Online Charging System about any relevant monetary related events (for example if the subscriber has exceeded a spend threshold that may lead to modifying the QoS of the session), volume consumed related events, time spent related events, or any other type of events.

The Policy Counter information consists of:

Steps

1. Policy Counter identifier, that is, the name of the event. For example, "VolumeAccumulated".
2. Policy Counter status, that is, the value of event. For example, "80%LimitReached".
3. Policy Group Identifier, that is, the Policy Group the event is linked to. For example, "PayAsyouGo". Policy Group Identifier is only applicable in ESy interface.

The Policy Counter is used in the SAPC Policy engine as policy conditions.

2.3 Determination of Policy and Charging Control Information to Install in PCEF

The SAPC determines the Policy and Charging Control Information to convey to the PCEF using the status of the Policy Counters received from the Online Charging System for the evaluation of the policies of the different controls (together with subscribed Subscriber Group static and dynamic information, application context, network context, time conditions, and so on).

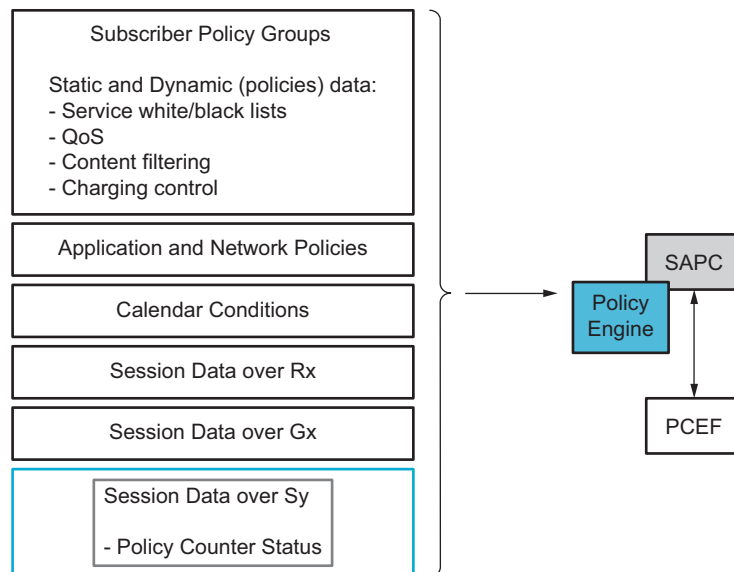


Figure 2 Policy Counter Status for Policy Evaluation

For example, for the following controls, the SAPC proceeds as follows:

- Access control: denying the access for a certain service or group of services when a specific Policy Counter indicates a particular status. For example, let's consider a Data Plan called 'Facebook and Twitter Service Pass' that allows up to 4 hours of these applications per day, and once these four hours are reached, denies the access to both services; for this Data Plan the SAPC configures a Subscriber Group "Facebook&Twitter" whose policies indicate that when the status of Policy Counter "Facebook&Twitter" is "4hoursreached" the access to the subscriber to Facebook and Twitter services has to be denied.
- Default Bearer QoS control: changing the default bearer QoS profile (QCI, MBR, and so on) when a certain status for a Policy Counter is received.
- Throttling: downgrading the MBR upon indication of a particular value of a Policy Counter status. For example, let us consider a Data Plan 'P2P' that allows in a month up to 1 GB of data of a P2P application within one day with a maximum bandwidth of 3 Mbps, and once this limit is reached, the maximum bandwidth is reduced to 500 kbps; for this Data Plan the SAPC configures policies for the Subscriber Group 'P2P' that indicates that when P2P Policy Counter status is 'P2Psurpassed' the bandwidth to a subscriber subscribed to Subscriber Group 'P2P' has to be limited to 500 kbps.
- Sending of notifications: sending for example an SMS or email when the counter status changes to a particular value.
- Charging control: for example, rating group change for a certain Subscriber Group, when a particular value for a Policy Counter status is received the subscriber loses the flat rate and is charged again as the subscriber used to.

These actions are configured with policies in the SAPC. See more information about how policies are evaluated in the SAPC in [Subscription and Policy Management](#).

2.4 Ericsson Sy: Integration with Charging System

The basic Integration with the Online Charging System for Monetary Spending Limit Reporting function allows setting the policies for the IP-CAN session of a subscriber considering the changes in Counter Status reported by the Online Charging System. The subscription of the Data Products applicable to the subscriber is provisioned and handled in both, the SAPC and the Online Charging System. Rating policies and accumulation data are handled in the Online Charging System, while user policies that consider changes in the Counter Status to set the policies for the IP-CAN session are handled in the SAPC. The Sy interface only conveys (changes in) the status of Policy Counters. This is the 3GPP standard behavior *Policy and Charging Control: Spending Limit Reporting over Sy Reference Point*.

The Ericsson Sy for the Integration with the Online Charging System for Monetary Spending Limit Reporting function allows the centralization of the subscriber subscription to Data Products in Ericsson Online Charging System:

The management of the subscriber subscription to the Operator Service Offering is centralized in Ericsson Online Charging System. Ericsson Online Charging System indicates to the SAPC the set of Data Products available to the subscriber by the ESy interface, using an Ericsson concept called Policy Groups.

The ESy interface conveys then, together with Policy Counter status, the Policy Groups available to the subscriber.

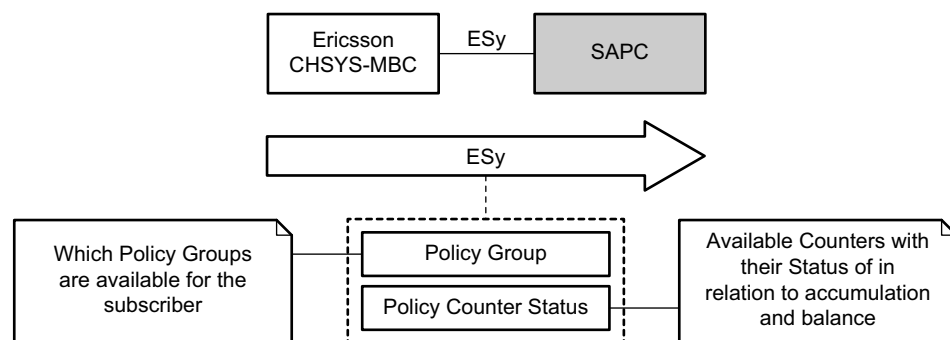


Figure 3 ESy interface: Handling of Policy Groups

During the establishment of the first IP-CAN session for a subscriber, the SAPC determines if the data to install in the PCEF depends on monetary balance status information of the subscriber' stored in Online Charging System. The SAPC first selects the right Online Charging System, then sends a request to the selected one and considers the information related to Policy Groups assigned to the subscriber to decide the data to install in the PCEF.



Subsequent IP-CAN session updates or new IP-CAN session establishments are processed in the SAPC considering the Policy Groups and Policy Counters status previously obtained from the Online Charging System and temporarily stored in the ESy session, being not necessary to contact again the Online Charging System. The same happens in a multiple Gx scenario at new Gx session establishment or modification for an ongoing IP-CAN session

Updates in the subscription to the Policy Groups are notified to the SAPC by Ericsson Online Charging System, so that the SAPC can reevaluate its policies and determine if the ongoing IP-CAN sessions must be updated.

The SAPC releases the Policy Groups information temporarily stored in ESy session when the last active IP-CAN session is terminated for the subscriber.

2.4.1 Policy Group

The Policy Group is an Ericsson concept.

The Policy Groups are assigned to a subscriber and are sent over ESy interface to indicate the Service Offering applicable to a subscriber. The Policy Group is implemented in the SAPC by using Subscriber Groups. By configuration, the set of services (static data) and the set of conditions (dynamic data) that have to be applied to a Policy Group are configured in the associated Subscriber Group. The Policy Group identifier conveyed in Ericsson Sy Reference Point allows the SAPC to be informed in real time by Ericsson Online Charging System about the Data Products (or derived subscription information) subscribed by a particular subscriber.

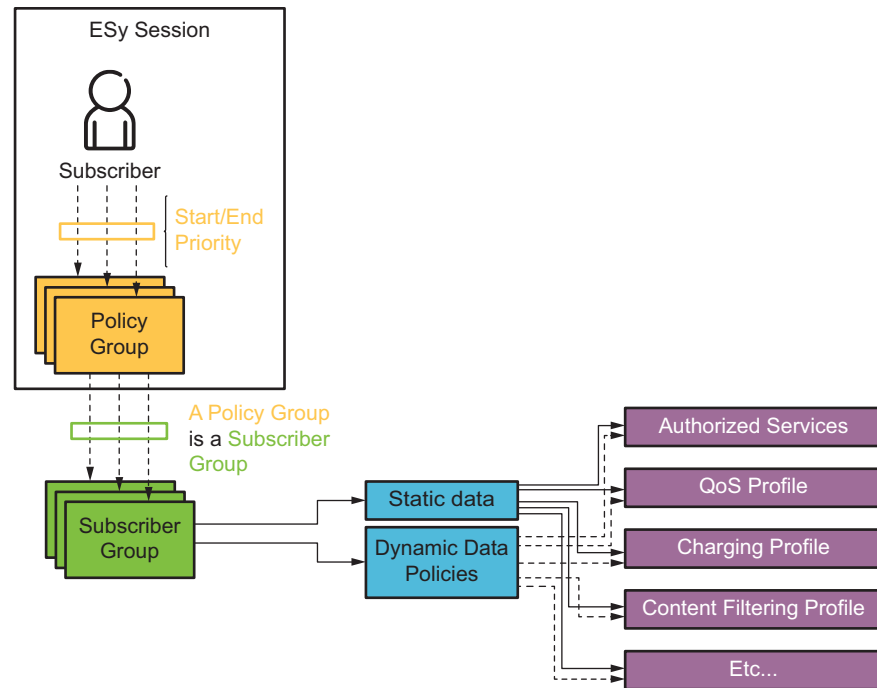


Figure 4 Relation between Policy and Subscriber Groups

The Policy Group information consists of:

- Policy Group Identifier, that is, the identifier of the Policy Group. For example, "PayAsYouGo".
- Policy Activation/Deactivation Time: Start and End date for the Policy Group association.
- Priority: the relative priority to be used by the SAPC to sort out precedence among groups, Policy Groups, and Subscriber Groups. It depends on the priority of the applicable Data Products.

Also, the SAPC allows to select dynamically the received Policy Groups, with using **Group Selection policies** including operator configured conditions (refer to Subscription and Policy Management).

2.4.2

Subscriber Data Distribution

For a Subscriber and an IP-CAN session, the SAPC combines Operator Network policies, User polices related to subscribed Service Offering, and Application polices to set the authorized data to apply for the IP-CAN session. The SAPC takes decisions using its flexible Policy Engine that evaluates operator configured conditions which make use of user data, such as subscriber data, subscriber dynamic information, accumulated usage, time and date conditions.

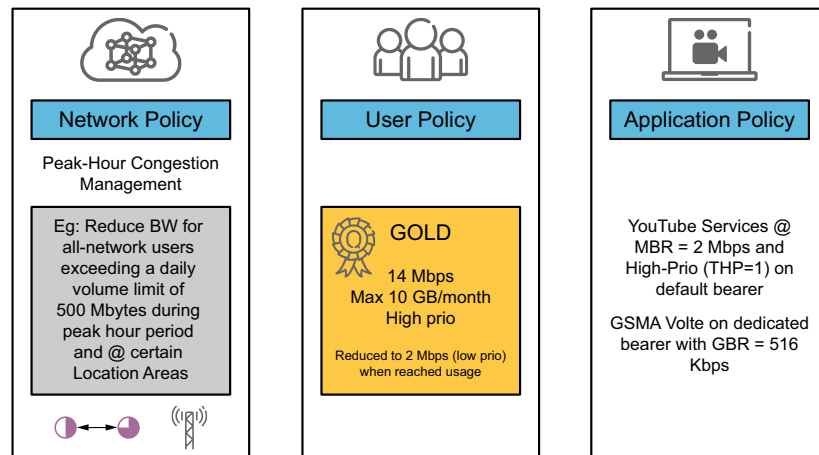


Figure 5 Policies Are Combined to Set the Policy for the Subscriber's IP-CAN session

In a scenario of enhanced Integration with the Online Charging System for Monetary Spending Limit Reporting, the subscription to the Data Products offered by the operator can be centralized in Ericsson Online Charging System, whereas subscriber data relative to Network Policies and Application Policies can remain in the SAPC, giving place to the following subscriber data distribution:

- Subscriber data and accumulation data relative to Operator Network Policies are stored in the SPR (SAPC internal or external repository).
- Subscriber data relative to Application policies are stored in the SPR (SAPC internal or external repository).
- The piece of subscriber data that indicates the Data Products subscribed by the subscriber (that is, the Policy Groups), is centralized in Ericsson Online Charging System.

Rating policies and accumulation usage for the contracted Data Products are handled in the Online Charging System.

User policies that define the allowed services, bandwidth limits, and so on, that apply to the IP-CAN session according to the Data Products subscribed by subscriber are handled in the SAPC.

When Operator Network policies and Application policies are bound to Data Products (for example, the policies to apply during Busy Hour and the policies to apply to YouTube service depend on whether the subscriber subscribed to "Gold", "Silver" or "Bronze" Data Products), it is possible to deploy the SAPC without subscribers populated in the SPR.

But when Operator Network policies and Application policies are independent of the Data Products (for example, the policies to apply during Busy Hour depend on whether the subscriber is defined as belonging to the Subscriber Group

"Abuser"), it is necessary to populate the subscribers in the SPR and assign to them the subscriber's static data and policies or the Subscriber Groups static data and policies related to these Operator Network policies and Application policies. The SAPC then combines this information stored in the SPR with the Policy Groups retrieved from the Online Charging System to determine the data to install in the PCEF.

The combination of the Policy Groups obtained from Ericsson Online Charging System with subscribed Subscriber Groups is performed as follows:

- Policy Group Priority and Policy Group Activation/Deactivation time of the received Policy Groups is used together with the Subscriber Group Priority and Subscriber Group Start/End date provisioned to the subscriber to obtain the Policy Group and Subscriber Groups applicable to the subscriber. The mechanism to decide which are the active Groups is the same as the one used in *Subscription and Policy Management* to determine the set of active Subscriber Groups for a subscriber:

- Policy Group Activation/Deactivation time

It has the same meaning as the Subscriber group date and time. It implies that the service offering indicated by the Policy Group is only applicable during the period comprised between the activation and deactivation instant.

If there is not any date associated to the Policy Group, it is considered that the Policy Group applies without time restrictions. If only the Deactivation time is received, then the Policy Group can be applied from current date until the Deactivation time. If only the Activation time is received, the Policy Group can be applied from the Activation time to unlimited date.

It is possible to receive the UE time zone offset from the Enforcement Function, if so the time used when Activation/Deactivation time of the Policy Group is evaluated is corrected with this offset. When time zone information is not received, just local time is considered.

A Policy Group applies to a subscriber only when the current time is between the Activation and Deactivation times.

Also, the SAPC allows to select dynamically the received Policy Groups, with using **Group Selection policies** including operator configured conditions (refer to *Subscription and Policy Management*). The result of this policies evaluation is the set of active Policy Groups, that is, the applicable Policy Groups for the subscriber. If no Dynamic Group Selection policies are configured, the active policy groups are the received ones only if current date is between activation and deactivation time.

- Policy Group priority

As for the case of the Subscriber Group priority, the minimum priority value assigned to a Policy Group has the higher priority. For the Policy



Groups, the default priority value (no priority is assigned to the Policy Group) is 0, that is, the maximum priority. The priority is used as criteria to decide which Policy Group or Subscriber Group to apply in case there are conflicts between the different services offerings data. See more information about how SAPC selects the data to apply to the subscriber in *Subscription and Policy Management*.

The following figure shows an example of Subscriber data distribution between the SAPC and the Online Charging System:

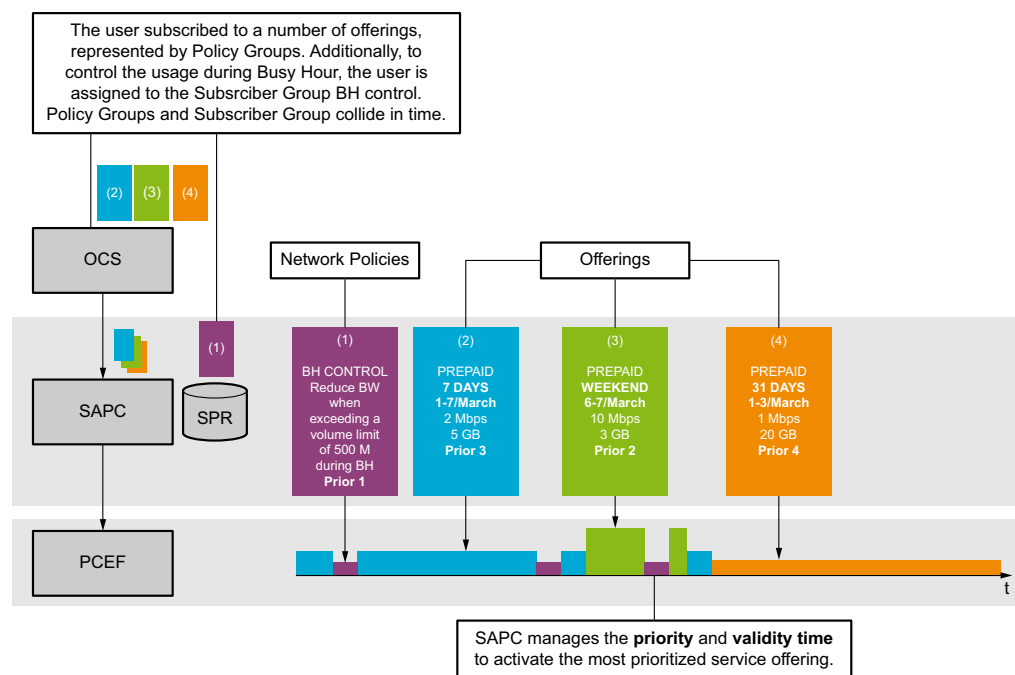


Figure 6 Combination of Policy Groups and Subscriber Groups

A Policy Group assigned to the subscriber by ESy interface, and Subscriber Groups provisioned to the subscriber through the SAPC provisioning interfaces must be disjoint sets of Groups, that is, the same Group must not be assigned to the subscriber by both, ESy interface and the SAPC provisioning interfaces.

The combination of the information of Policy Groups and Subscriber Groups for a given subscriber occurs for the subscribers populated in the SAPC that have both, Policy Groups assigned in Ericsson Online Charging System and received by ESy interface and Subscriber Groups subscribed in the SAPC. The provisioning of Subscriber Groups to the subscriber can be performed by the SAPC provisioning interfaces or by the Auto-provisioning function, refer to *Subscription and Policy Management*.

When a subscriber profile is removed from the SPR (SAPC internal or external repository), and only Policy Groups are available, the SAPC does not request to the PCEF the IP-CAN session termination for any associated active IP-CAN

session of the subscriber. Each IP-CAN session remains alive and it is reauthorized considering those Policy Groups (refer to [Subscription and Policy Management](#)).

2.5 Integration with Multiple Online Charging Systems

The SAPC allows the integration with multiple Online Charging Systems by Sy interface or ESy interface, for example in the case where prepaid subscribers are provisioned in standard 3GPP Online Charging System by Sy interface while postpaid subscribers are provisioned in Ericsson Online Charging System by ESy interface.

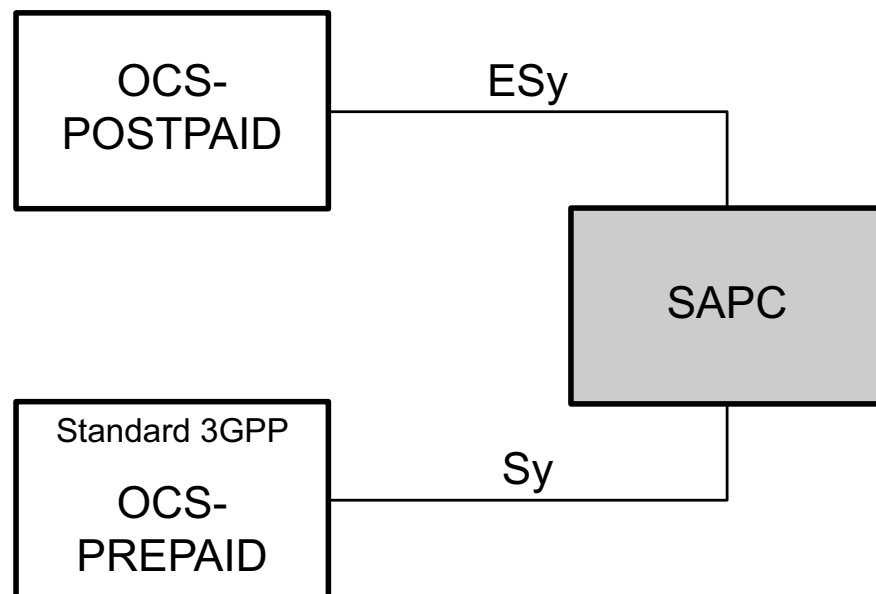


Figure 7 Integration with Multiple Online Charging System

The SAPC determines the applicable Online Charging System for a subscriber during the establishment of the first IP-CAN session. The selection of the applicable Online Charging System can be done based on static or dynamic configuration. Dynamic selection of the Online Charging System is performed using policies whose conditions can take into account information received through Gx. The criteria to select the corresponding Online Charging System during the establishment of an IP-CAN session for a subscriber is described below:

- If the subscriber has an already established session with an Online Charging System then the Policy Counters are already available in the SAPC. No Online Charging System is selected at this step, as it was selected in a previous request for the subscriber. In other case:



- If the subscriber is provisioned in the SAPC and a specific Online Charging System is statically provisioned to the subscriber, this one is selected: In other case:
- If a global policy for Online Charging System selection returns an Online Charging System, this one is selected. In other case,
- If a default Online Charging System is defined in the SAPC at node level, this one is selected.

It can be configured for each Online Charging System with either Sy interface or ESy interface.



3 Network Deployments

The SAPC can provide Policy and Charging Control based on Spending Limit Reporting over Sy Reference Point together with the following network elements:

- In the bearer plane (PCEFs) side through Gx interface:
 - Ericsson EPG.
 - Ericsson MSP.
 - Standard 3GPP PCEF.
- In the Business Support System (BSS) side:
 - Ericsson Charging System - MBC, through ESy interface.
 - Standard 3GPP OCS, through Sy interface

Note: The SAPC also allows multiple PCEFs scenario for Integration with the Online Charging System for Monetary Spending Limit Reporting.



4 Traffic Cases

This chapter explains the traffic interactions between the network nodes involved in the function Integration with the Online Charging System for Monetary Spending Limit Reporting.

All these interactions are enabled by any supported Gx and Ericsson Gx release. For detailed description of each of the interfaces supported, it shall be consulted the indicated interface descriptions.

The Traffic Cases developed in the following chapters consider the following scenarios:

- Bill shock prevention. According to EU regulation, a mobile operator has to impose a monthly default cut-off limit of EUR 50 for data roaming. The subscriber could also select a different cut-off limit or discard the bill shock safeguard entirely. In this traffic case, a mobile network operator implements EU's roaming rules using the basic functionality supported by the Integration with the Online Charging System for Monetary Spending Limit Reporting.
- Centralized management in Ericsson Online Charging System of the Operator Service Offering. The subscriber Service Offering for this traffic case consists initially of a "Mobile Broadband Basic" Data Product, that later on is upgraded with a "Turbo Button" voucher. The "Mobile Broadband Basic" Data Product is a monthly package that allows QoS of 2 Mbps up to EUR 10 limit, charging at EUR 0.5 per 100 Mbytes; once the EUR 10 limit is reached, QoS is reduced to 500 Kbps. The "Turbo Button" Data Product is a 2 hours valid package that allows QoS at 1 Gbps and high priority up to 1 GB volume limit. In this traffic case, the operator handles the subscriber's Service Offering using the extended functionality offered by the feature Integration with the Online Charging System for Monetary Spending Limit Reporting.
- Control of abusers by Operator Network Policies. A network operator might be interested in controlling the use of network resources independently of the subscriber subscription to Data Products. For this traffic case, let us assume, the network operator has defined in the SAPC the Subscriber Group 'Abusers', which is assigned to the subscriber because of accumulated usage historical data. This Subscriber Group, defines policies that indicate that the session has to be terminated at certain usage accumulation limit reached during the IP-CAN session, and that the QoS for a particular service has to be reduced if certain daily usage accumulation limit is reached for this service. The Subscriber Group 'Abusers' is part of the subscriber profile stored in the SPR, and is considered during IP-CAN session life cycle together with the subscription information, Policy Groups, and Policy Counters, retrieved from in Ericsson Online Charging System. In this traffic case, the operator is using the extended functionality for the Integration with the Online Charging System for Monetary Spending Limit Reporting.



4.1 Bill Shock Prevention

According to EU regulation, a mobile operator has to impose a monthly default cut-off limit of EUR 50 for data roaming. In this traffic case, a mobile network operator implements EU roaming rules using the basic functionality supported by the Integration with the Online Charging System for Monetary Spending Limit Reporting.

The flows show the Sy session life cycle in relation to the IP-CAN session life cycle, in a scenario where the accumulation data is centralized in the Online Charging System. When the EUR 50 limit for roaming data is reached for the subscriber, the Online Charging System indicates so to the SAPC, which terminates the IP-CAN session of the subscriber.

4.1.1 Use of Policy Counters Status during IP-CAN session Life Cycle

This traffic case describes the request of Policy Counters status to the Online Charging System, how the received Policy Counters statuses are temporarily stored in the SAPC for the subscriber, and how they are used to obtain the policies to set in the PCEF during IP-CAN session establishment and IP-CAN session update. This flow also describes the termination of the Sy session at IP-CAN session termination.

Updates in the IP-CAN session owing to changes in the Policy Counters status are covered in [Policy Counter Status Change](#) on page 19

Only the significant attributes for this Traffic Case are described in the following subchapters.

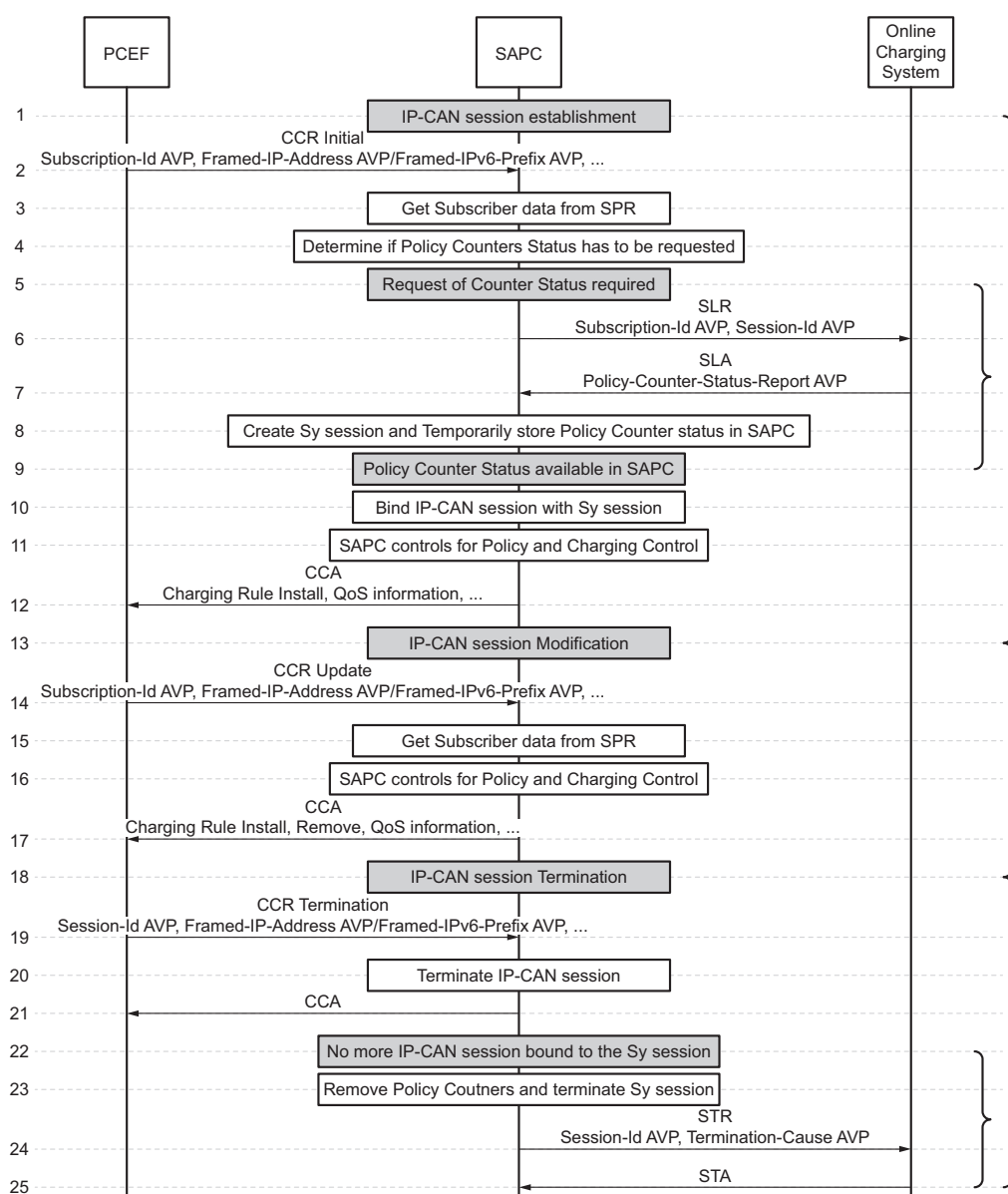


Figure 8 Handling of Policy Counters Status During IP-CAN session Life Cycle

IP-CAN session establishment

- 2: The SAPC receives a Gx CCR-initial message from the PCEF indicating IP-CAN session establishment.
- 3: The SAPC looks for the subscriber and subscriber group profile. The subscriber is populated in the SPR (the subscriber could have been populated by provisioning interfaces or because of the auto-provisioning function) and has a Subscriber Group assigned that allows data roaming. This Subscriber Group has configured a policy that indicates that when the bill shock roaming data limit is reached (the status Policy Counter



"BillShockPrevention" is "LimitSurpassed"), the access of the subscriber is not authorized.

- 4: The SAPC determines if for this subscriber there are Policy Counters available in the selected Online Charging System (as described in [Integration with Multiple Online Charging Systems](#) on page 12). If a valid Online Charging System is returned

The SAPC requests the available Policy Counters to the selected Online Charging System (steps 6–8).

If a Sy session exists for the subscriber, then the Policy Counters are already available in the SAPC and the flow continues in step 10.

Note: For those cases where a subscriber is provisioned in the SAPC with an administrative identifier and with multiple traffic identifiers (for example, one MSISDN and IMSI or multiple MSISDNs), the SAPC creates a new Sy session for each IP-CAN session established with different traffic identifier (then flow continues in step 6).

Request of Policy Counters Policy Counters are requested to the Online Charging System.

- 6: The SAPC sends an SLR message to the Online Charging System to request the available Policy Counters. SLR-Request-Type AVP is set to INITIAL_REQUEST (0).

The SAPC uses in Subscription-Id AVP of the SLR message the traffic identity selected in the Gx session to access the subscriber profile.

- 7: The SAPC receives a SLA message from the Online Charging System with the Policy Counters assigned to the subscriber. In this example, the SAPC receives the Policy Counter "BillShockPrevention" with status "LimitNotSurpassed"
- 8: The SAPC creates Sy session and temporarily stores the received Policy Counters "BillShockPrevention" with status "LimitNotSurpassed".

The flow continues in step 10.

Policy Counter Status available in the SAPC When the Sy session exists, the SAPC uses the Policy Counters status temporarily stored in Sy session. The flow continues in step 10.

- 10: The SAPC binds the IP-CAN session with the Sy session .
- 11: The SAPC applies the controls for Policy and Charging control applicable for the PCEF (IP-CAN Session Access Control, Service Access Control, and so on) considering the Policy Counter Status values received: Policy Counter "BillShockPrevention" with status "LimitNotSurpassed".
- 12: Since the Bill Shock limit for the subscriber is not surpassed, the access is allowed, and the CCA message is sent to the PCEF with the corresponding



the information according to the subscriber subscription and applicable policies (PCC rules, QoS, and so on).

IP-CAN session modification

- 14: The SAPC receives a CCR Update message from the PCEF indicating IP-CAN session modification

The CCR triggered by default IP-CAN session modification only contains the new/modified parameters.

- 15: The SAPC looks for the subscriber and subscriber group profile.
- 16: The SAPC applies the controls for Policy and Charging control applicable for the PCEF and for IP-CAN session modification (Bearer Control Mode selection, IP-CAN Session Access Control, Service Access Control, and so on) considering the Policy Counter Status value stored in the Sy session.

The status of the Policy Counter "BillShockPrevention" has not changed, and continue being "LimitNotSurpassed".

- 17: The CCA message is sent to the PCEF only including the new/modified Policy and Charging Control information.

IP-CAN session termination

- 19: The SAPC receives a CCR Termination from the PCEF indicating IP-CAN session termination.
- 20: The SAPC terminates the IP-CAN session for the requesting PCEF.
- 21: The SAPC sends a CCA message to the PCEF including Result-Code AVP with value SUCCESS.

No more IP-CAN sessions bound to Sy session

- 23: Remove Policy Counters and Terminate Sy session.
- 24: The SAPC sends STR message to Online Charging System.
- 25: The SAPC receives STA message from Online Charging System.

4.1.2 Policy Counter Status Change

The following subsection describes the traffic case of PCEF reauthorization owing to a change in the status of the Policy Counter "BillShockPrevention" to "LimitSurpassed" during an ongoing IP-CAN session. The policies defined in the SAPC for Access Control determine that the access is not allowed when the Policy Counter "BillShockPreventions" gets the value "LimitSurpassed", which in this case results in the IP-CAN session termination.

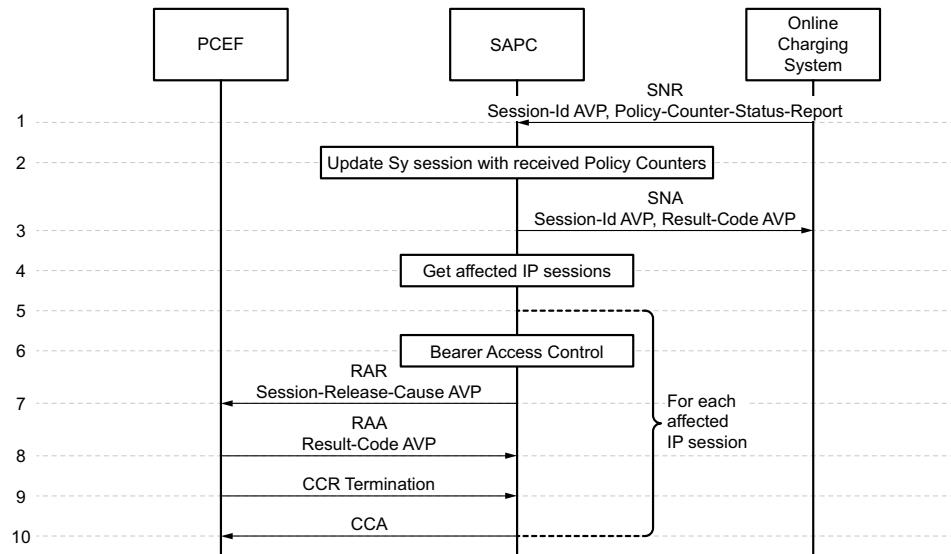


Figure 9 Counter Status Change: IP-CAN Session Access Control with Negative Result

- 1: When the Online Charging System detects that the status of a Policy Counter changes, it sends an SNR message to the SAPC, including the Policy Counters that change their status. In this use case, the Online Charging System sends Policy-Counter-Status-Report AVP including Policy-Counter-Identifier AVP the name of the Policy Counter, "BillShockPrevention", and Policy-Counter-Status AVP the status "LimitSurpassed".
- 2: The SAPC updates the Sy session with the Policy Counter status received.
- 3: SNA message is returned from the SAPC to the Online Charging System.
- 4: The SAPC looks for the IP-CAN sessions bound to the subscriber and Sy session.
- 5: For each affected IP-CAN session, the SAPC executes a session reauthorization process, considering the Policy Counter "BillShockPrevention" with status "LimitSurpassed" during the evaluation of the policies for the different controls.
- 6: IP-CAN Session Access Control gives as result that the IP-CAN session has to be terminated for the subscriber.
- 7: To terminate the IP-CAN session a RAR message is sent to the corresponding PCEF for each affected IP-CAN session, in this example, with Session-Release-Cause AVP set to UE_SUBSCRIPTION_REASON
- 8: RAA message is returned by the PCEF.



- 9: The SAPC retrieves a CCR Termination requesting IP-CAN session termination.
- 10: The SAPC sends a CCA message to the PCEF including Result-Code AVP with value SUCCESS.

When all the IP-CAN sessions bound to the subscriber are terminated, the Sy session is terminated with the Online Charging System.

4.2 Centralized Management of Operator Service Offering

The subscriber Service Offering for this traffic case consists initially of a "Mobile Broadband Basic" Data Product, that is later on upgraded with a "Turbo Button" voucher. The "Mobile Broadband Basic" Data Product is a monthly package that allows QoS of 2 Mbps up to EUR 10 limit, charging at EUR 0.5 per 100 Mbytes; once the EUR 10 limit is reached, QoS is reduced to 500 Kbps. The "Turbo Button" Data Product is a 2 hours valid package that allows QoS at 1 Gbps and high priority up to 1 GB volume limit. In this traffic case, the operator handles the Service Offering of the subscriber using the extended functionality offered by the feature Integration with the Online Charging System for Monetary Spending Limit Reporting.

To develop this use case, it is considered that the subscriber is not populated in the SAPC.

4.2.1 Use of Policy Counters and Policy Group Information during IP-CAN session Life Cycle

This traffic case describes the request of Policy Counters and Policy Groups to the Ericsson Online Charging System for the Data Product "Mobile Broadband Basic" for a subscriber that has this subscriber group subscribed, but who is not populated in the SAPC. As in the traffic case for Bill Shock Prevention, it shows how the information retrieved from the Ericsson Online Charging System is used to determine the policies to set in the PCEF for IP-CAN session establishment and IP-CAN session update. The flow ends with the termination of the temporal relation of the subscriber with the Policy Counters and Policy Groups at IP-CAN session termination.

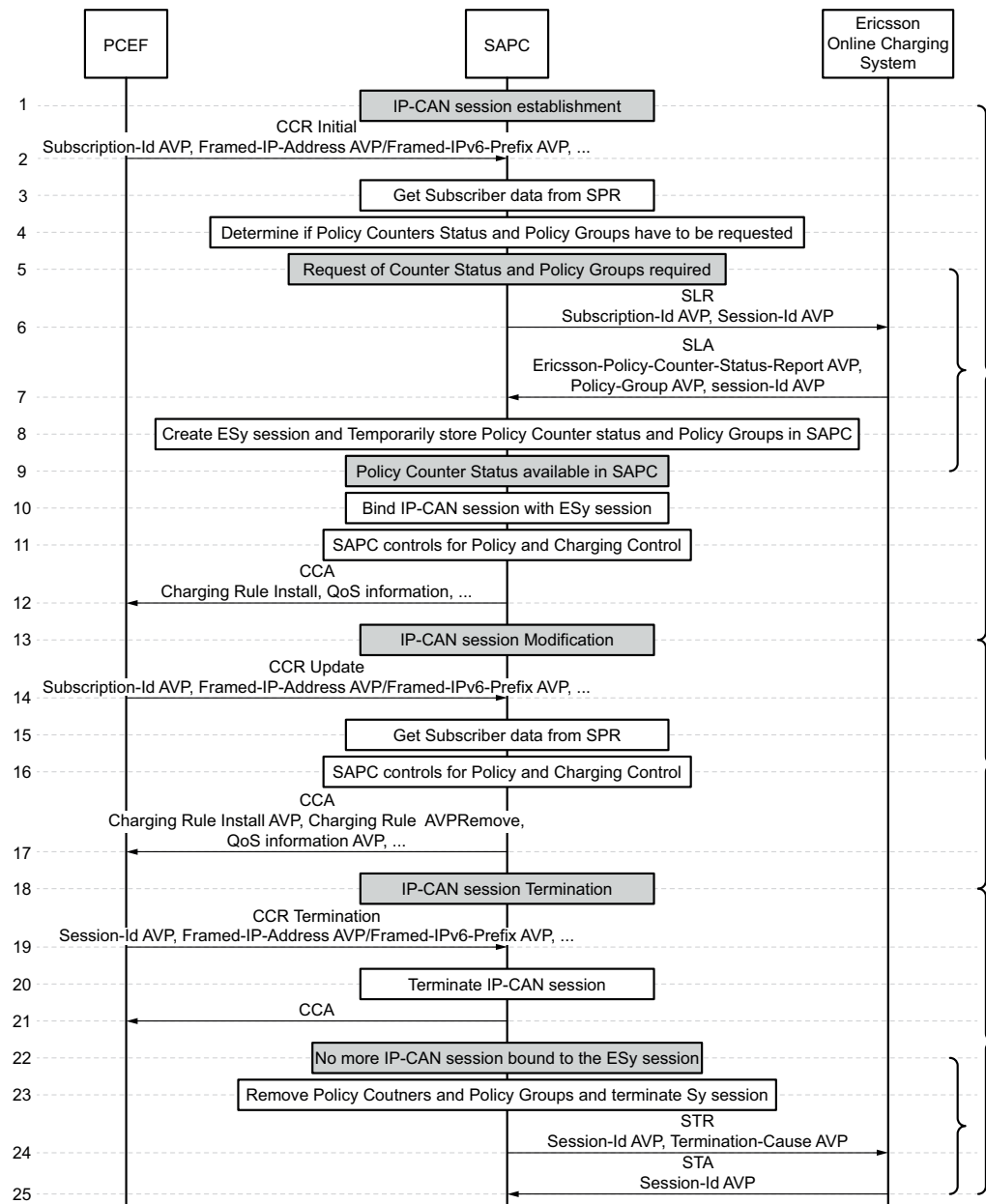


Figure 10 Handling of Policy Counters and Policy Group Information During IP-CAN session Life Cycle

IP-CAN session establishment

- 2: The SAPC receives a Gx CCR-initial message from the PCEF indicating IP-CAN session establishment.
- 3: The SAPC looks for the subscriber and subscriber group profile.



- 4: If the subscriber is not found in the SPR and Auto-provisioning function is not enabled, the SAPC determines if for this subscriber there are Policy Counters and Policy Groups available in the selected Ericsson Online Charging System (as described in [Integration with Multiple Online Charging Systems](#) on page 12). If a valid Online Charging System is returned: the SAPC requests the available Policy Counters and Policy Groups to the Ericsson Online Charging System (steps 6–8).

If an ESy session exists for the subscriber, then the Policy Counters and Policy Groups are already available in the SAPC and the flow continues in step 10.

Note: For those cases where a subscriber is provisioned in the SAPC with an administrative identifier and with multiple traffic identifiers (for example, one MSISDN and IMSI or multiple MSISDNs), the SAPC creates a new ESy session for each IP-CAN session established with different traffic identifier (then flow continues in step 6).

Request of Policy Counters and Policy Groups Policy Counters and Policy Groups are required to the Online Charging System.

- 6: The SAPC sends an SLR message to the Online Charging System to request the available Policy Counters and Policy Groups. Ericsson-SLR-Request-Type is set to INITIAL_REQUEST (0)

The SAPC uses in the Subscription-Id AVP of the SLR message the traffic identity selected in the Gx session to access the subscriber profile.

- 7: The SAPC receives an SLA message from the Online Charging System with the Policy Counters and Policy Groups assigned to the subscriber. In this example, the SAPC receives in the AVP Policy-Group AVP the Policy Group with Policy-Group-Name AVP "MobileBroadbandBasic" and Ericsson-Policy-Counter-Status-Report AVP the Policy Counter with identifier Ericsson-Policy-Counter-Identifier AVP "10€limitforMBB" and status Ericsson-Policy-Counter-Status AVP "LimitNotSurpassed". The Ericsson Online Charging System includes also Ericsson-Policy-Counter-Policy-Group-Name AVP with value "MobileBroadbandBasic" to indicate that the given Policy Counter name and status is for the Policy Counter belonging to this Policy Group (the Ericsson Online Charging System can assign the same Policy Counter name to several Policy Groups).
- 8: The SAPC creates an ESy session and temporarily stores the received Policy Group "MobileBroadbandBasic" and the Policy Counter "10€limitforMBB" with status "LimitNotSurpassed".

The flow continues in step 10.

Policy Counter Status and Policy Groups available in the SAPC When the ESy session exists, the SAPC uses the Policy Counters status and Policy Groups temporarily stored in ESy session. The flow continues in step 10.

- 10: The SAPC binds the IP-CAN session with the ESy session .



- 11: The SAPC applies the controls for Policy and Charging control applicable for the PCEF (IP-CAN Session Access Control, Service Access Control, and so on) considering the static data and dynamic data defined for the Policy Group "MobileBroadbandBasic" and the Policy Counter Status values received: Policy Counter "10€limitforMBB" with status "LimitNotSurpassed".
- 12: Since the monetary spending limit for the subscriber is not surpassed, the access is allowed, and the CCA message is sent to the PCEF with to install the services and QoS defined for the "Mobile Broadband Basic" Group (PCC rules, QoS of 2 Mbps, and so on).

IP-CAN session modification

- 14: The SAPC receives a CCR Update message from the PCEF indicating IP-CAN session modification

The CCR triggered by default IP-CAN session modification only contains the new/modified parameters.

- 15: The SAPC looks for the subscriber and subscriber group profile. The subscriber is not populated in the SPR.
- 16: The SAPC then takes the Policy Groups and Policy Counter status stored in the ESy session and applies the controls for Policy and Charging control applicable for the PCEF and for IP-CAN session modification (Bearer Control Mode selection, IP-CAN Session Access Control, Service Access Control, and so on). The SAPC considers the status "LimitNotSurpassed" of the Policy Counter "10€limitforMBB" when evaluating the policies linked to the Policy Group "MobileBroadbandBasic".
- 17: The CCA message is sent to the PCEF only including the new/modified Policy and Charging Control information.

IP-CAN session termination

- 19: The SAPC receives a CCR Termination from the PCEF indicating IP-CAN session termination.
- 20: The SAPC terminates the IP-CAN session for the requesting PCEF.
- 21: The SAPC sends a CCA message to the PCEF including Result-Code AVP with value SUCCESS.

No more IP-CAN sessions bound to ESy session

- 23: Remove Policy Counters and Policy Groups and Terminate ESy session
- 24: The SAPC sends STR message to the Online Charging System.
- 25: The SAPC receives STA message from the Online Charging System.



4.2.2 Policy Counter Status Change

The following subsection describes the traffic case of PCEF reauthorization owing to a change in the status of the Policy Counter of the "Mobile Broadband Basic" Data Product from "LimitNotSurpassed" to "LimitSurpassed". Owing to this change in the status of the Policy Counter "10€limitforMBB", the QoS is decreased to 500 Kbps.

4.2.2.1 Counter Status Change, Bearer QoS Change

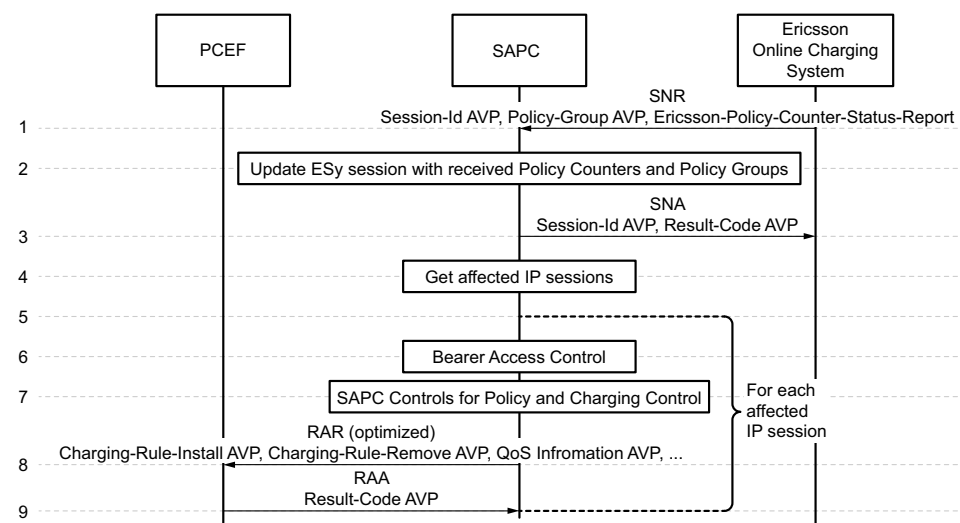


Figure 11 Counter Status Change, Bearer QoS Change

- 1: When the Ericsson Online Charging System detects that the status of a counter changes, the Ericsson Online Charging System sends an SNR message to the SAPC, pushing all the information available for the subscriber, that is, all the available Policy Groups, and all the Policy Counters.

In this example, the SAPC receives the Policy Group "MobileBroadbandBasic" and the Policy Counter "10€limitforMBB" with status "LimitSurpassed"

- 2: The SAPC gets the received Policy Groups and Policy Counters and updates the ESy session.
- 3: An SNA message is returned from the SAPC to the Ericsson Online Charging System.
- 4: The SAPC looks for the subscriber and ESy session related IP-CAN sessions.
- 5: For each affected IP-CAN session, the SAPC executes a session reauthorization process, considering the static and dynamic data bound to the Policy Groups and the status of the counters stored in the ESy session.



- 6: The SAPC performs SAPC controls. For Bearer Access QoS control, in this case, there is no policy defined.
- 7: When the result of the IP-CAN Session Access Control is authorized, all applicable controls are reevaluated. When evaluating Bearer QoS control, a policy defined for "MobileBroadbandBasic" Group with a condition that indicates that when the status of Policy Counter "10€limitMBB" is "LimitSurpassed" the Bearer QoS = 500 kbps comes true. The result of Bearer QoS control is a decrease of QoS to 500 Kbps.
- 8: A RAR is sent to the PCEF with only the new/modified information and with the AVP Re-Auth-Request-Type set to AUTHORIZE_ONLY:
- 9: A RAA including Result-Code AVP is returned by the PCEF.

4.2.3 Policy Group Update: Turbo Button Purchase

To describe this Use Case, it is being considered that the subscriber remains subscribed to the "Mobile Broadband Basic" Data Product though its limit has been surpassed.

To increase temporarily the QoS (for example, because the subscriber needs a high speed, high priority connection with his office), the subscriber decides to purchase a Turbo Button voucher that allows him to enjoy 1 Gbps QoS with high priority during 2 hours or up to 1 GB volume limit.

The steps described in the flow would be the same in case the subscriber unsubscribes to a provisioned Data Product.

The subscriber is involved in several IP-CAN sessions, and any of them might be controlled by different PCEFs.



4.2.3.1

New Policy Group Added

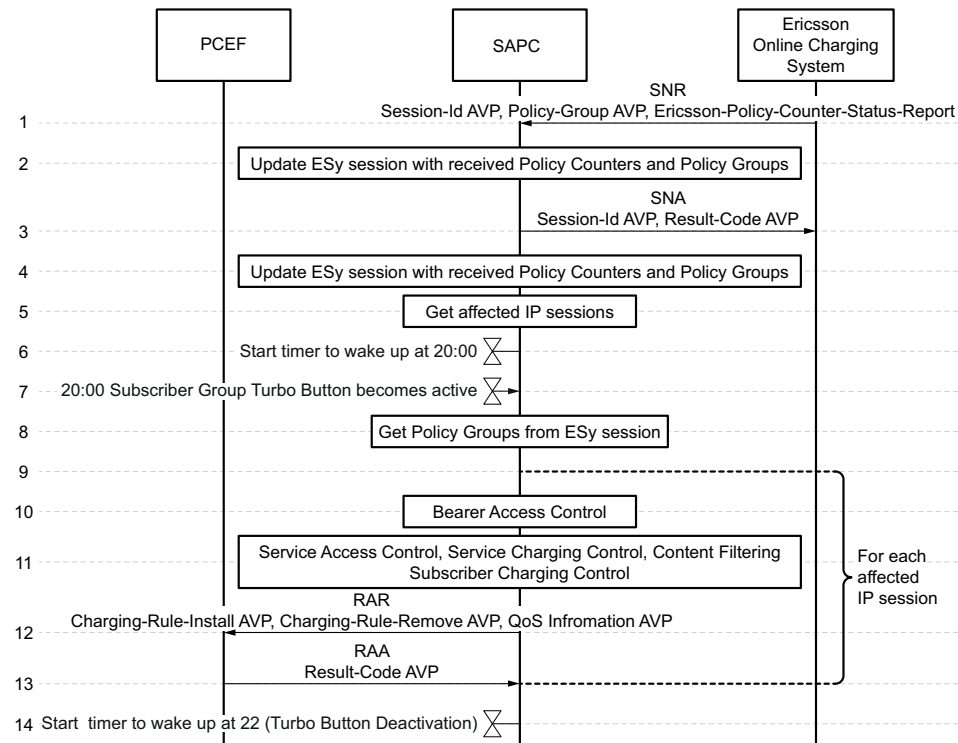


Figure 12 New Policy Group Added

- 1: When the Ericsson Online Charging System detects that a new Policy Group (and possibly new counters associated to this Policy Group) has been assigned to the subscriber, the Ericsson Online Charging System sends an SNR message to the SAPC, pushing all the information available for the subscriber, that is, the complete set of Policy Groups, and the complete set of Policy Counters.

Following the example, the following information is pushed to the SAPC: Policy Group "MobileBroadbandBasic" with Priority 2, Policy Group "Turbo" with Priority 1 and start date at 20:00 and end date at 22:00, Policy Counter "10€limitMBB" with status "LimitSurpassed" and Policy Counter "TurboStatus" with status "LimitNotSurpassed".

- 2: The SAPC gets the received Policy Groups and Policy Counters and updates the ESy session.
- 3: An SNA message is returned from the SAPC to the Ericsson Online Charging System.
- 4: The SAPC looks for the subscriber and ESy session related IP-CAN sessions and executes a reauthorization process. Since the Turbo package is not applicable yet, it is not needed to modify the data set in the PCEF.

- 5: The SAPC starts the internal timer to wake up at 20:00, the activation time of Turbo Button
- 6: Subscriber Group Turbo Button becomes active
- 7: The SAPC gets the Policy Groups from ESy session.
- 8: The SAPC looks for the subscriber and ESy session related IP-CAN sessions.
- 10: For each affected IP-CAN session, the SAPC executes first the IP-CAN Session Access Control. In this case, there is no policy defined, and the result is the session is authorized.
- 11: Then the SAPC executes a session reauthorization process, considering the Policy Groups and Policy Counters status stored in the ESy session.

When the SAPC applies the controls for Bearer QoS Control, first the SAPC evaluates which Group applies. For the configuration of the example, since the "Turbo" Group has higher priority than "MobileBroadbandBasic" Group, the SAPC evaluates the policies for the "Turbo" Group and the policies for "MobileBroadbandBB" are not evaluated. The policies for "Turbo" Group indicate that the Bearer QoS to apply is 1 Gbps when the status of Policy Counter "TurboStatus" is "LimitNotSurpassed".

- 12: A RAR is sent to the PCEF with only the new/modified information and with the AVP Re-Auth-Request-Type set to AUTHORIZE_ONLY:
- 13: A RAA including Result-Code is returned by the PCEF.
- 14: The SAPC starts a timer to control the time at which the Turbo package ends.

4.3 Operator Network Policies, Abusers Example

A network operator might be interested in controlling the use of network resources independently of the subscriber subscription to Data Products. In this example, the network operator has defined in the SAPC the Subscriber Group 'Abusers', which defines the conditions to apply to subscribers classified as abusers because of their accumulated usage historical data. This Subscriber Group, for example, defines policies that close the session at certain usage accumulation limit during the IP-CAN session, and downgrade the QoS of a particular service (for example, P2P) when certain daily usage accumulation limit is surpassed for this service. The Subscriber Group 'Abusers' is part of the subscriber profile stored in the SPR, and it is considered during IP-CAN session life cycle together with the Policy Groups and Policy Counters received from the EricssonOnline Charging System.

The realization of this Use Case relies on the feature **Fair Usage Control**. Fair Usage Control provides the capability to control the accumulated volume and/or time usage performed by a subscriber for a service or group of services during a period, for example, monthly, or during an IP-CAN session, and to take certain



actions whenever any of the usage limits configured for that subscriber is surpassed, such as QoS change, rating group change, or deny the access to a service, according to a policy decision

The following flow develops a use case where the session limit established for the IP-CAN session is reached, and as a consequence, the access is denied to the subscriber.

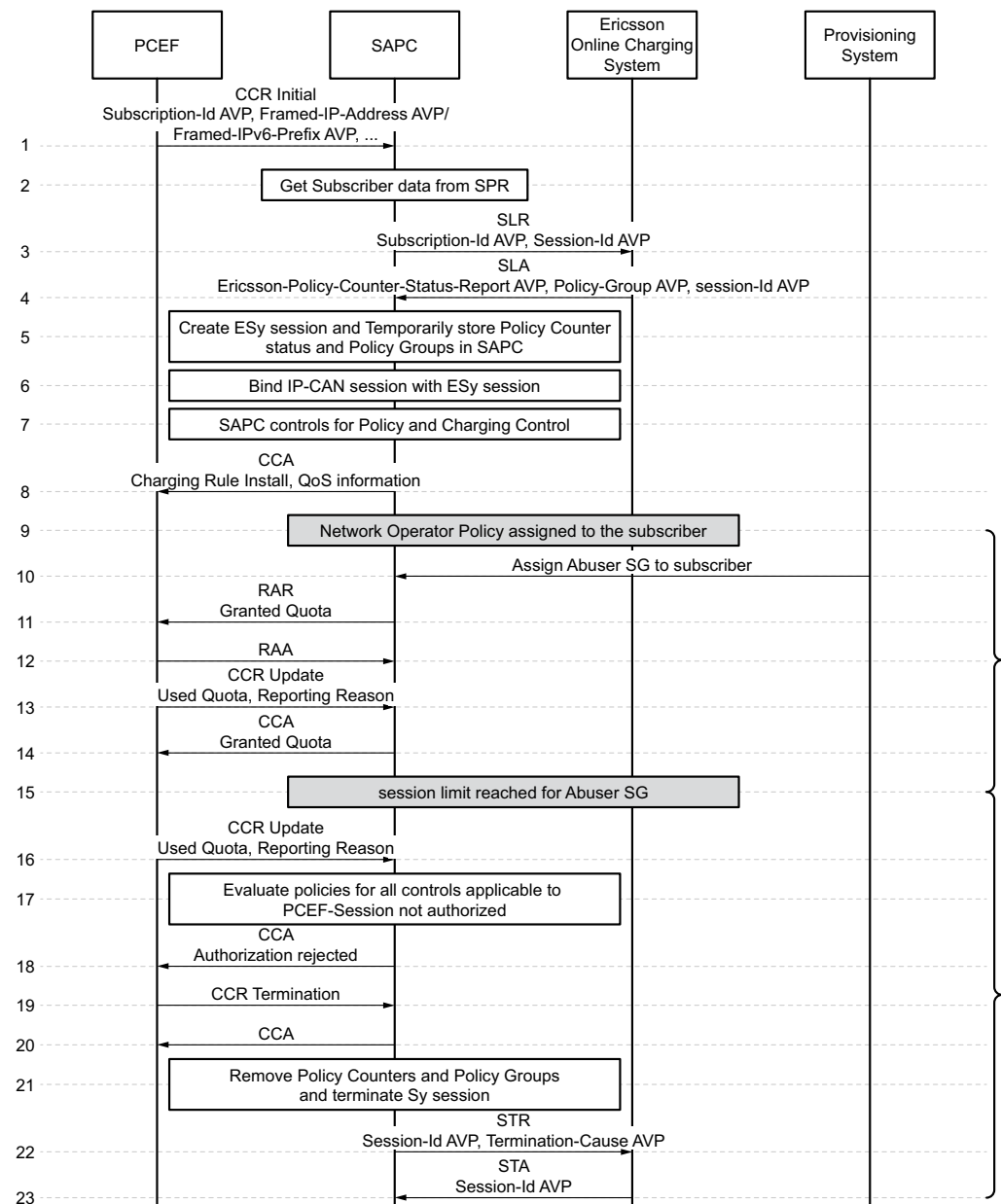


Figure 13 Network Operator Policies: IP-CAN session Termination

- 1–8 see [Use of Policy Counters and Policy Group Information during IP-CAN session Life Cycle](#) on page 21. In particular, for this use case it is considered



that the Policy Group "Flat Rate Unlimited" with Priority 2 is received from the Ericsson Online Charging System.

- 9: The subscriber is identified as a potential abuser by the mobile network operator. The mobile network operator decides to activate for this subscriber the network policies defined for subscribers classified as abusers.
- 10: An order to assign the Subscriber Group "Abusers" to the subscriber is received in the SAPC from the Provisioning System. The Priority 1 is assigned to this Subscriber Group, which is higher than the priority (2) of the Policy Group "Flat Rate Unlimited".
- 11: The SAPC reauthorizes all the active IP-CAN sessions of the subscriber. To activate reporting at "P2P" service level and at session level, a RAR message is sent to the PCEF including the assigned Quota.
- 12: The PCEF responds to the reauthorization message
- 13: When the subscriber consumes the assigned quota, the PCEF reports that the assigned Quota has been exhausted.
- 14: The SAPC assigns Quota to the subscriber for this session and responds the PCEF.

The process continues, with the PCEF reporting data consumed and the SAPC assigning new quota until at certain point in time, a report from the PCEF of the consumed Quota by the subscriber makes to reach the limit of allowed usage for the IP-CAN session:

- 16: The PCEF reports quota consumed by the subscriber. The SAPC detects that the limit established for data consumption during the IP-CAN session is reached.
- 17: The SAPC evaluates the different Policy controls to apply to the IP-CAN session. The result of evaluating IP-CAN Session Access Control policies is that the IP-CAN session operation is not authorized:

The SAPC gets the value of the policies from the active Subscriber Groups. In this case, the policies for the Group "Abusers" give a positive result when accumulated usage for the IP-CAN session is reached, indicating the IP-CAN session is not authorized.

- 18: A CCA message with Result-Code AVP DIAMETER_AUTHORIZATION_REJECTED =5003 is sent to the PCEF to indicate that the default IP-CAN session is to be deactivated.
- 19: The Enforcement Function sends a CCR Termination message.
- 20: The SAPC accepts the termination of the session.
- 21: Since there are no more IP-CAN sessions to the subscriber, the SAPC deletes the Policy Groups and Policy Counters temporarily stored in the ESy session.



- 22: The SAPC indicates to the Ericsson Online Charging System to terminate the ESy session for this subscriber.
- 23: The SAPC receives the ESy session termination confirmation from the Ericsson Online Charging System.

4.4 Connectivity with the Online Charging System

Routing of Diameter messages from a network element towards the right Diameter realm is based on standard Diameter realm-based routing (*Diameter Base Protocol - RFC 3588*).

The SAPC, to route SLR messages to the Online Charging System, uses pre-configured realm information. For the subsequent messages routed from the SAPC, the SAPC uses the Host Identifier included in the `Origin-Host` AVP and the Realm included in `Origin-Realm` AVP of the SLA message.

The next figure shows an example of how the realm information is considered in a typical deployment with the SAPC and a standard Online Charging System

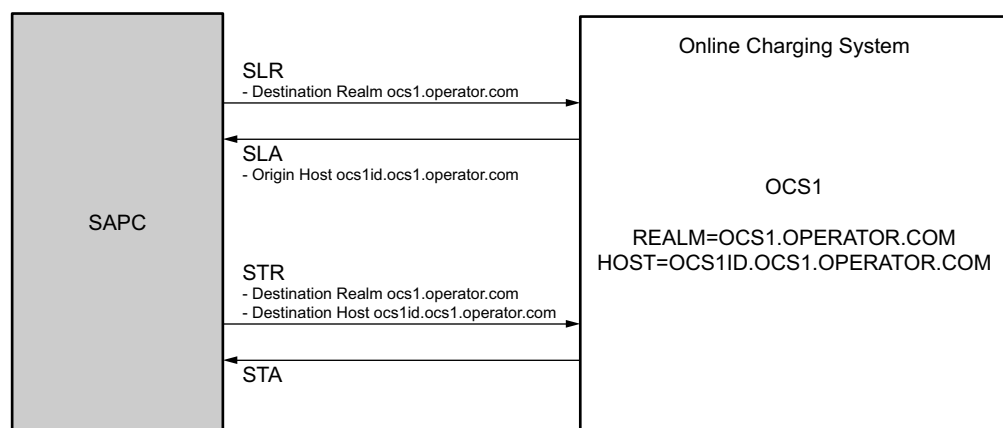


Figure 14 Messages Routing between the SAPC and a standard Online Charging System

The SAPC configures the Realm (OCS1.OPERATOR.COM) corresponding to the interfacing standard Online Charging System.

This Charging System can be assigned by default to the subscriber, can be explicitly provisioned to the subscriber, or can be selected by policies.

The routing of SLR/SLA, STR/STA messages occur as follows:

- SLR message is routed towards OCS1.OPERATOR.COM realm, using for example, a Diameter peer connection towards the OCS1 node (OCS1ID.OCS1.OPERATOR.COM).

- The OCS1 Diameter node receives the SLR message and terminates the Sy session. When composing the SLA message, the OCS1 Diameter node includes the `Origin-Host` AVP, that is, it includes `OCS1ID.OCS1.OPERATOR.COM`.
- The next request from the SAPC, STR, indicates the particular SDP realm for the subscriber (`OCS1.OPERATOR.COM`) in the `Destination-Realm` AVP and the OCS1 Diameter node identifier (`OCS1ID.OCS1.OPERATOR.COM`) in the `Destination-Host` AVP.

SNR messages are routed from the Online Charging System to the SAPC using both, SAPC Host Identity and SAPC realm provided by the SAPC to the Online Charging System in the `Origin-Host` AVP and `Origin-Realm` AVP included in the SLR message.

Routing to the Ericsson Online Charging System

Routing to the Ericsson Online Charging System differs from the previous explanation.

Figure 15 shows how the realm information is considered in a deployment with the SAPC and the Ericsson Online Charging System.

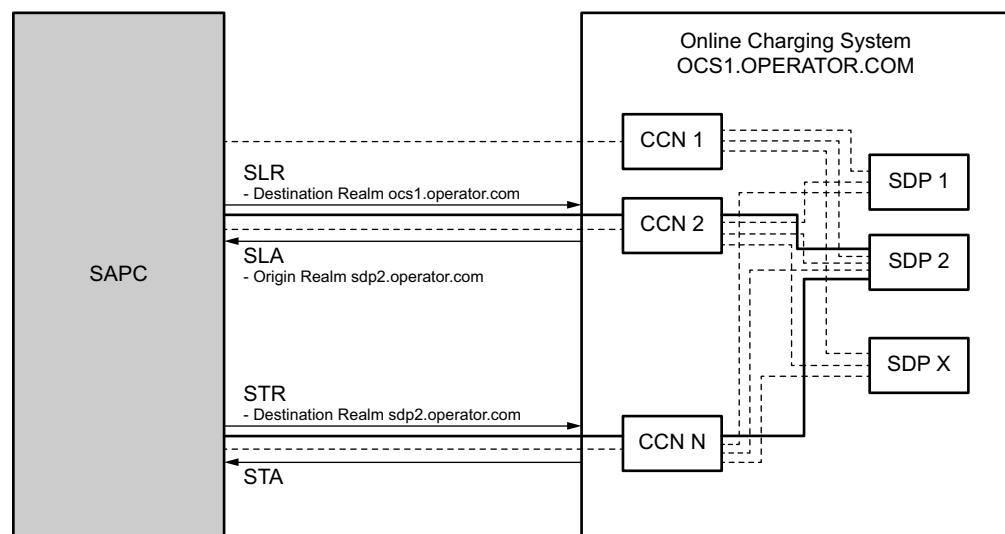


Figure 15 Messages Routing between the SAPC and the Ericsson Online Charging System

The SAPC configures the Realm (`OCS1.OPERATOR.COM`) corresponding to the interfacing Online Charging System.

This Charging System can be assigned by default to the subscriber, can be explicitly provisioned to the subscriber, or can be selected by policies.



The routing of SLR/SLA, STR/STA messages occur as follows:

- SLR message is routed towards OCS1.OPERATOR.COM realm, using a Diameter peer connection towards one of the CCN nodes, for example CCN2.
- CCN2, based on `Subscription-Id` AVP, determines the specific SDP realm where the SLR message has to be routed (for example SDP2.OPERATOR.COM) and forwards the request.
- An SDP Diameter node (selected based on load distribution logic) within the SDP-specific realm receives the SLR message and terminates the ESy session.
- SLA message includes the `Origin-Realm` AVP to indicate the SDP-specific realm applicable to the subscriber, that is, it includes SDP2.OPERATOR.COM. The message also includes the `Origin-Host` AVP of the SDP node answering the message.
- The next request from the SAPC, STR, indicates the particular SDP realm for the subscriber (SDP2.OPERATOR.COM) in the `Destination-Realm` AVP together with the `Origin-Host` AVP.
- STR message is routed towards SDP2.OPERATOR.COM using a Diameter peer connection defined in the Diameter routing table for SDP2.OPERATOR.COM, for example CCN N.
 - For the cases when an SDP node is down but the sessions are replicated in a different SDP node, SAPC is able to send the STR message to finish an Sy session towards the new active SDP node if at least one SNR message is received for that Sy session from the active SDP node.
- STR message is routed from CCN N to the appropriate SDP Diameter node based on the information indicated in the `Destination-Realm` AVP.

To route SNR messages, the Ericsson Online Charging System includes `Destination-Host` AVP and `Destination-Realm` AVP set to the values that the SAPC sent in SLR message `Origin-Host` AVP and `Origin-Realm` AVP.

4.5 Failure Handling

This section describes the Sy session or ESy session failure handling.



4.5.1

SLR Failure

Table 1 Error Handling

Error Condition	Action	Code
<p>An SLA message over Sy interface is received indicating no Policy Counter Identifier and has no Policy Counters available for the subscriber in the Online Charging System</p> <p>Experimental-Result AVP</p> <p>:DIAMETER_ERROR_NO_AVAILABLE_POLICY_COUNTERS</p>	<p>The SAPC does not create an Sy session and it logs the error.</p> <p>When the subscriber is provisioned in the SAPC, the SAPC answers the CCA according to the subscriber groups defined for the subscriber. If the subscriber is not populated in the SAPC, then the SAPC proceeds as defined in the 'unknown subscriber' profile if it applies (Subscription and Policy Management, otherwise, a DIAMETER_USER_UNKNOWN error is returned in the Gx response</p>	<p>Result-Code AVP set to success (code 2001) when the subscriber is populated or if not populated, the 'unknown subscriber' profile applies. Otherwise Result Code AVP is set to DIAMETER_USER_UNKNOWN (code 5030)</p>
<p>An SLA message is not received or it is received with an error, for example:</p> <p>Result-Code AVP:</p> <p>DIAMETER_USER_UNKNOWN</p> <p>DIAMETER_INVALID_AVP_VALUE</p> <p>DIAMETER_UNABLE_TO_DELIVER</p> <p>DIAMETER_TOO_BUSY</p> <p>DIAMETER_LOOP_DETECTED</p>	<p>The SAPC does not create the Sy session/ESy session and it logs the error.</p> <p>When the subscriber is provisioned in the SAPC, the SAPC answers the CCA according to the subscriber groups defined for the subscriber. If the subscriber is not populated in the SAPC, then the SAPC proceeds as defined in the 'unknown subscriber' profile if it applies (Subscription and Policy Management), otherwise, a DIAMETER_USER_UNKNOWN</p>	<p>Result-Code AVP set to success (code 2001) when the subscriber is populated or if not populated, the 'unknown subscriber' profile applies. Otherwise Result-Code AVP is set to DIAMETER_USER_UNKNOWN (code 5030)</p>



Error Condition	Action	Code
	NOWN error is returned in the Gx response	
An SLA message is received with DIAMETER_SUCCESS but AVPs have invalid value, are invalid, inconsistent, or missing	The SAPC accepts the answer and creates the Sy session/ESy session with the valid information received (empty if there is no valid information) and answers with a CCA according to the valid information received from the OCS, and - when the subscriber is provisioned in the SAPC - according to the subscriber groups defined for the subscriber if they apply.	Result-Code AVP set to success (code 2001)

4.5.2

SNR Failure

Table 2 Error Handling

Error Condition	Action	Code
An SNR message contains an unknown value in the Session-Id AVP	The SAPC logs the error and returns an error indicating the request cannot be handled because the indicated Sy session/ESy session is unknown	SNA Result-Code AVP is set to error DIAMETER_UNKNOWN_SESSION_ID, with error code 5002
An SNR message contains an AVP with Invalid value in its data portion. For example, Policy Group Activation Time occurs later than Policy Group DeactivationTime.	The Sy session/ESy session is updated with the values received without errors and the Gx sessions are reauthorized according to these values. The SAPC returns an error and indicate the AVPs that caused the failure.	SNA Result-Code AVP is set to error DIAMETER_INVALID_AVP_VALUE, with error code 5004. The Failed-AVP contains the AVP that caused the failure.
An SNR message is received and the SAPC detects an internal error that does not allow continuing	The SAPC logs the error and returns an error indicating that the request cannot be handled	SNA Result-Code AVP is set to error DIAMETER_UNABLE_TO_COMPLY



Error Condition	Action	Code
processing the request		

Other Diameter Base Protocol errors are handled according to RFC 3588 .

4.5.3

STR Failure

Table 3 Error Handling

Error Condition	Action	Code
An STA is not received or it is received with an error, for example: DIAMETER_UNKNOWNSessionID DIAMETER_UNABLETODELIVER DIAMETER_TOOBUSY DIAMETER_LOOPDETECTED	The SAPC logs the error and deletes the Sy session/ESy session	-
An STA is received with DIAMETER_SUCCESS but AVPs have invalid value, are invalid, inconsistent, or missing	The SAPC logs the error and deletes the Sy session/ESy session	-



5 Reference List

Ericsson Documents

1. Fair Usage Control
2. Subscription and Policy Management

Standards

1. Policy and Charging Control: Spending limit reporting over Sy reference point
- 3GPP TS 29.219
2. Diameter Base Protocol - RFC 3588