

Access and Charging Control (Gx)

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.

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.

Abstract

This document describes the Access and Charging Control function provided by the Ericsson Service-Aware Policy Controller (SAPC) when Gx interface is used.



Contents

1	Access and Charging Control Introduction	1
2	Access and Charging Control Function	3
2.1	IP-CAN session Access Control	4
2.2	Service Access Control	5
2.3	Service Charging Control	14
2.4	Subscriber Charging Control	16
2.5	Content Filtering	16
2.6	Event Triggers	17
2.7	Multiple Gx Support	18
2.8	Presence Reporting Area	19
2.9	Diameter Race Condition Handling	21
3	Access and Charging Control Network Deployments	27
4	Access and Charging Control Traffic Cases	29
4.1	IP-CAN session Lifetime	29
4.2	Redirect Owing to non-authorized Static Service	41
4.3	One Time Redirect for Authorized Static Services	43
4.4	Service Authorization and Static Service Qualification Policies with Time of Day Conditions When the PCEF is Selected As Time Controller	45
4.5	Presence Reporting Area	48
4.6	PCC Rule Error Handling	51
4.7	Diameter Race Condition Handling	52
4.8	Access and Charging Control Error Handling	53
	Reference List	57





1 Access and Charging Control Introduction

This document describes the Access and Charging Control function provided by the SAPC when Gx interface is used.





2 Access and Charging Control Function

This function enables the SAPC to provide differentiated Access and Charging control per subscriber and service basis.

The services that the SAPC can handle through this function are the ones that can be identified through predefined filters statically defined either in the PCEF or in the SAPC. That is, services that do not require dynamic session negotiation. These last services require Dynamic PCC rules support in the SAPC, and they are described in *Dynamic Policy Control (Rx)*.

Access and Charging control is performed handling **PCC rules**. A PCC rule is a set of information including:

- Filters that enable the detection of traffic IP flows belonging to a service and allow the PCEF to block those packet flows that do not match with the filter.
- Charging data that allows the PCEF to apply different charging depending on the service.
- QoS information that allows the PCEF to apply different QoS characteristics depending on the service.

This function uses two different types of PCC rules:

- Static PCC rules: they are locally configured in GGSN/PDN GW or SASN and dynamically activated/deactivated from the SAPC. The information sent from the SAPC to the PCEF, by Gx interface, is the name of the PCC rules that should be installed/removed.
- Preconfigured PCC rules: they are configured in the SAPC and dynamically sent to GGSN/PDN GW. The information sent from the SAPC to GGSN/PDN GW, by Gx interface, includes the Service Data Flow filters (IPv4 or IPv6 or both) and charging data.

This function does not handle any QoS information as part of PCC rules. Refer to *Bearer QoS and Bandwidth Management* for a further description of QoS information handling performed by the SAPC.

PCC rules

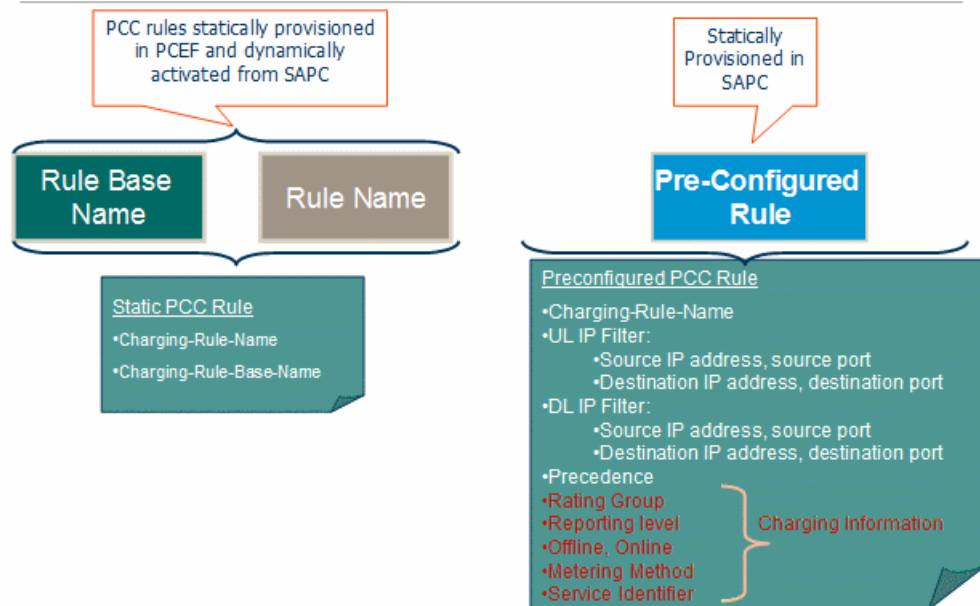


Figure 1 Static and Preconfigured PCC rule Data

The SAPC supports IP address overlapping scenarios:

- Handling different IP-CAN sessions within the same PCEF: Support to differentiate multiple IP-CAN sessions for the same subscriber having the same UE IP Address and PCEF but different APN.
- Handling of different IP-CAN sessions among different PCEFs sharing same range of IP addresses: Support to differentiate IP-CAN sessions for different subscribers having the same UE IP Address and APN but from different PCEF.

This function provides Ericsson proprietary enhancements to the standard 3GPP PCC Access and Charging control function, it includes, among others, rule Space management, IP-CAN session authorization, content filtering, and so on.

The function is supported in the following network scenarios:

- 3GPP accesses Including GPRS and EPS.
- Non-3GPP accesses for WLAN.

2.1 IP-CAN session Access Control

IP-CAN session Access Control is used to allow or reject IP-CAN session operations and allows the possibility to request the termination of the IP-CAN session.

The SAPC decides if the IP-CAN session is authorized or rejected evaluating IP-CAN Session Access Control policies, these policies can take into account



subscriber information, dynamic conditions and context information received (for example SGSN IP address, RAT, charging characteristics).

IP-CAN 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 IP-CAN session is authorized):

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

Therefore 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. Refer to Solving Policies Conflicts section in *Subscription and Policy Management*.

By default IP-CAN sessions are authorized, therefore in case there are no IP-CAN Session Access Control policies configured or the IP-CAN Session Access Control is not configured for the requesting PCEF, the IP-CAN session is authorized.

IP-CAN session Access Control is performed at:

- IP-CAN session establishment
- IP-CAN session reauthorization because of:
 - IP-CAN session modification.
 - Update subscriber data, refer to *Subscription and Policy Management*.
 - Changes owing to time conditions, refer to *Subscription and Policy Management*.
 - Changes owing to Fair Usage Control, refer to *Fair Usage Control*
- Events received from the Application Function (for further details, refer to *Dynamic Policy Control (Rx)*).

2.2 Service Access Control

Service Access Control determines the services that are authorized to run on a particular IP-CAN session.

Service Access Control decisions are based on policies (conditions) that can take into account the subscriber profile, time of day and network information received in the message. In addition, these policies can take into account usage information such as if the subscriber has surpassed the provisioned usage limit.

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

Service Access Control can purely follow 3GPP specifications, but can also be augmented with Ericsson Value Added function, depending on the information received from the PCEF about the support of each proprietary capability. Therefore, when working with the Ericsson Added Value function, there are some differences compared to the standard solution that are remarked in the corresponding section as “Ericsson Added Value”.

Service Access Control is performed at:

- IP-CAN session establishment.
- IP-CAN session reauthorization because of:
 - IP-CAN session modification.
 - Update subscriber data, refer to [Subscription and Policy Management](#).
 - Changes owing to time conditions, refer to [Subscription and Policy Management](#).
 - Changes owing to Fair Usage Control, refer to [Fair Usage Control](#)
- Events received from the Application Function (for further details, refer to [Dynamic Policy Control \(Rx\)](#)).

If the control is disabled for the requesting PCEF, the SAPC does not authorize any service for the subscriber.

Procedure to Determine the Authorized Services

The following procedure is used to determine the authorized services:

- Selection of Rule Space (Ericsson Added Value)
- Service Selection
- Service Authorization
- Static Services Qualification

2.2.1 Selection of Rule Space (Ericsson Added Value)

A Rule Space can be configured in the PCEF and it defines a set of local data for the subscriber, such as the set of static PCC rules that might be potentially assigned to the subscriber and certain local profiles, such as QoS profile, content filtering profile, which Bandwidth Limitation or Rating Group to apply to each service, and so on. These local profiles associated to the rule space are used by the PCEF when the SAPC does not return these profile data.



The operator may define different Rule Spaces but only one can be active. Once the Rule Space has been selected by the SAPC at IP session setup, it cannot be modified during IP session lifetime.

The selection of the applicable Rule Space is done in the following way:

- If the PCEF announces a rule space decision, this is the Rule Space selected.
- If the PCEF suggests a Rule Space, that means that it allows Rule Space negotiation if the corresponding capability is enabled. Then, the SAPC evaluates the configured policies for Rule Space selection, as output result it is obtained the applicable Rule Space.
- If there is no output result, the suggested Rule Space is the applicable one.

Static services can be grouped into Rule Spaces. Once the SAPC determines the applicable rule space, only the static services belonging to the selected rule space are considered in the following steps.

2.2.2 Service Selection

The services selected (static and preconfigured) are the final result of the following steps:

- The SAPC selects the list of services that belongs to the global Subscribed services list, the Subscribed-services list of the active groups the subscriber belongs to, and particular subscriber Subscribed-services list.

If the PCEF is configured in the SAPC as supporting preconfigured services, the preconfigured services are considered and their destination address of DL IP flow and source address of UL IP flow are filled with the UE IP address.

- Services in the blacklists of the active groups the subscriber belongs to, and also services in the particular subscriber blacklist are extracted out of the previous service selection.

This means that if a service is in the subscribed service list of a subscriber but it is in the blacklist of any of the active groups that the subscriber belongs to, the service is not authorized.

The following figure shows an example of how the SAPC performs the service selection:

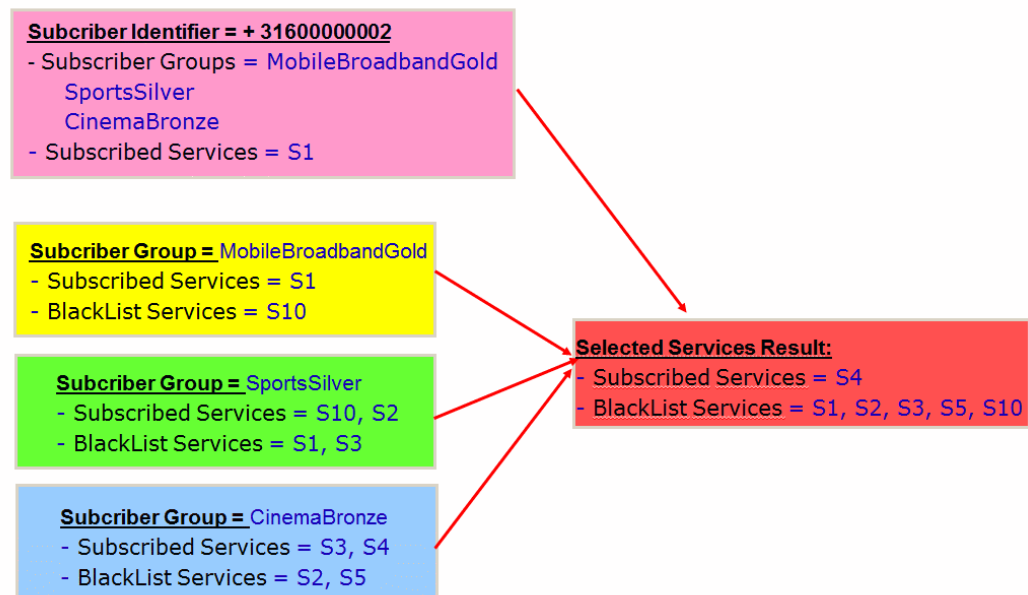


Figure 2 Example of Service Selection

Note: Priority of subscriber groups is not applicable in service selection (for more information about priority of subscriber groups, refer to *Subscription and Policy Management*).

2.2.3 Service Authorization

For each of the selected services in the former process, the SAPC evaluates the configured policy conditions for Service Authorization.

Service Authorization 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 service is authorized):

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

Therefore 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. Refer to Solving Policies Conflicts section in *Subscription and Policy Management*.

By default the selected services are authorized, therefore in case there are no Service Authorization policies configured for those services they are authorized.



It is possible to receive the UE time zone offset from the PCEF, if so, the time used in any calculation has to be corrected with this offset. When time zone information is not received, just the SAPC local time is considered.

Note: Time conditions are not considered in Service Authorization policies for dynamic services.

Service Authorization Policies without Time of Day Conditions or with Time of Day Conditions where PCRF controls time

The result of the evaluation process is:

- An authorization decision (that is, service authorized or not)
- If Static service is not authorized, a **reason of non-authorization (Ericsson Added Value)** when the enhanced service authorization control is negotiated.

Possible reasons of non-authorization can be: the service is in the blacklist, owing to roaming or owing to terminal capabilities, and so on. This information can be used by the PCEF, for example, to decide to redirect the subscriber to a self-provisioning portal.

If there are time of day conditions, the SAPC calculates an internal validity that is the minimum time and date conditions configured among all the evaluated rules. The SAPC triggers a new reauthorization when this time and date condition is reached. Refer to Policies based on Time of Day conditions section in [Subscription and Policy Management](#).

The following figure shows how this process is performed:

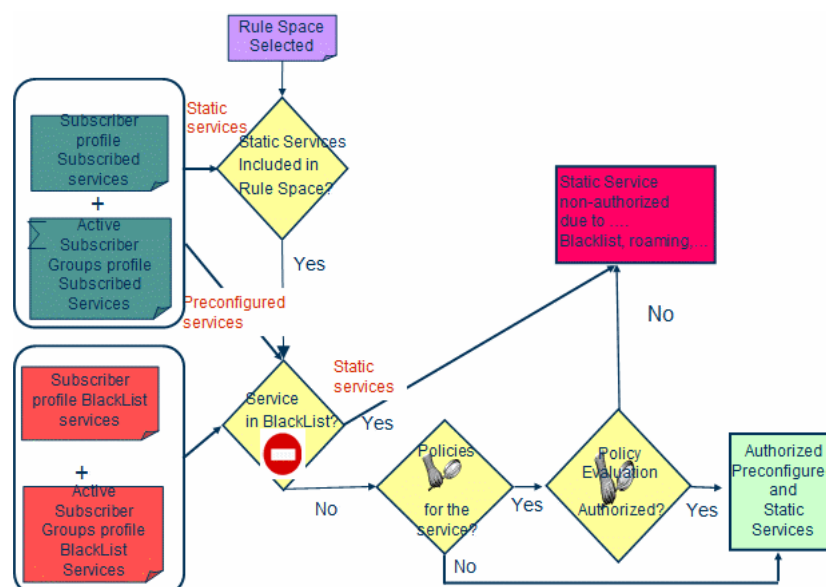


Figure 3 Service Authorization Process



Service Authorization Policies with Time of Day Conditions where the PCEF controls time

Service Authorization policies can be based on time conditions, so, the authorization decision is only applicable during a period.

In addition to the authorization decision, the SAPC determines the Revalidation time (this time indicates the PCEF when to reauthorize the service) and service activation/deactivation times.

If there are configured policies based on time conditions, the SAPC performs the following authorization process:

- 1 Determines if the service is authorized or not and the time when the authorization state should change (this time is the Validity Time)
- 2 Using the smallest validity time obtained in previous step and considering that currently it is this time, determines again if the service is authorized or not and the time when the authorization state should change.
- 3 The minimum validity time obtained in the second step is the Revalidation time, this time indicates to the PCEF when to reauthorize the service.

For those services not changing the authorization state as a result of second step:

- If the service is authorized but an authorization state change has been detected for the future, the SAPC installs the service with activation time equals to current time and deactivation time equals to its validity time obtained in the first step.
- If the service is authorized and no authorization state change has been detected for the future, the SAPC installs the service without activation and deactivation times.
- If the service is not authorized, it is not installed. If the service was authorized in previous request received from the PCEF, the SAPC will remove it if the service is not authorized again in the future (its validity time is infinite).

For those services changing the authorization state as a result of second step:

- If the service was authorized in first step and not authorized in second step, the SAPC installs the service with activation time equals to current time and deactivation time equals to its validity time obtained in the first step
- If the service was not authorized in first step and authorized in second step, the SAPC installs the service with activation time equals to its validity time obtained in first step and deactivation time equals to the validity time from second step.



2.2.3.1 One Time Redirect Control

One Time Redirection (OTR) allows to temporary redirect the desired HTTP/WAP traffic to a landing page to show some advertisements to the subscriber or notify to the subscriber about any operator desired information.

When the SAPC informs the PCEF that OTR should be applied for a certain authorized static service, the PCEF at reception of the first HTTP/WAP request of such service from the user redirects the request to the configured page and disarms the OTR for such service for the rest of the IP-CAN session lifetime. So that, the next time the PCEF receives an HTTP/WAP request from the user for the same service along the IP-CAN session lifetime, redirection is not applied unless the SAPC informs again to the PCEF to apply it.

The SAPC indicates the activation or deactivation of One-Time Redirect towards the PCEF per service basis (it is only applicable to authorized static services).

At IP-CAN session establishment, the SAPC decides for which authorized static services OTR should be applied with checking the list of services to redirect provisioned for the subscriber and the active groups the subscriber belongs to. If the static service is authorized and OTR is provisioned, then the SAPC informs the PCEF that OTR is active for such service.

At IP-CAN session modification, the SAPC provides OTR information to the PCEF only when there is a change regarding the previously OTR provided information, that is:

- when a static service changes from non-authorized to authorized and OTR is provisioned or
- when OTR has changed from not-provisioned to provisioned or the opposite way.

2.2.4 Static Services Qualification

A Static Service can be identified by several static service names in the PCEF, each static service name assigns different characteristics (for example qualifying the service with rating group, service bandwidth) to the service. As an example, this enables the PCEF to perform service throttling.

Only one static service name at the time is applicable to the service.

The following figure shows how different characteristics can be assigned to a static service in the PCEF:

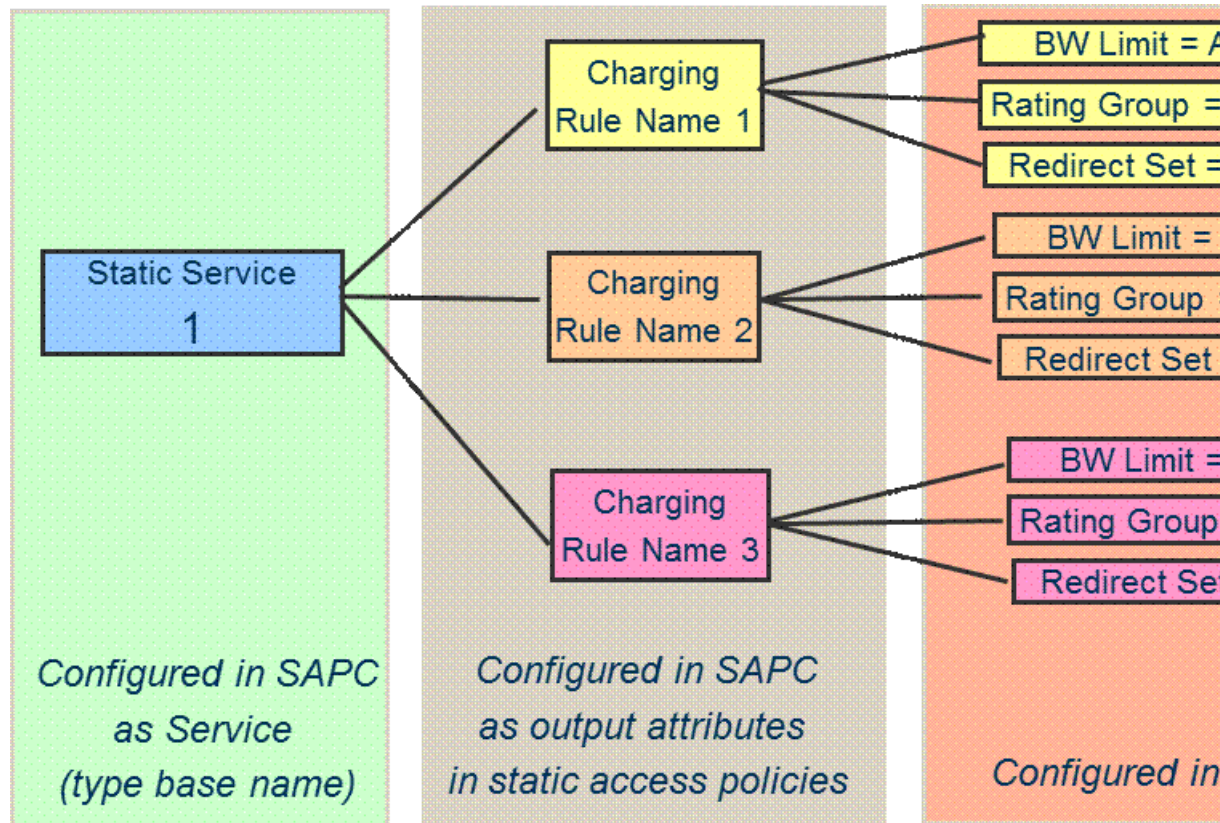


Figure 4 Example of Static Services Qualification

Static Services qualification policies can be applied by the SAPC to select which static service name is authorized and so to control the different set of service properties to be assigned by the PCEF. All properties configured for this static service name are configured in the PCEF.

For each static service authorized in the previous step, the SAPC evaluates the configured policies for static service qualification. The output result is the name of the qualified static service.

Static Services qualification policies are evaluated according to the following precedence allocation and applying permit overrides algorithm among them (if any policy evaluates to true, the static service is authorized):

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

Therefore 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. Refer to Solving Policies Conflicts section in *Subscription and Policy Management*.

If there are not configured static service qualification policies or policies are not fulfilled, the SAPC installs the service authorized in the previous step.

This option of using separately service authorization policies and static service qualification policies gives more flexibility and makes the configuration easier since it is possible to configure certain conditions for service authorization and different conditions to select the bandwidth, rating group, and so on. For example, authorize p2p service only if the subscriber is in his/her home network (with service authorization policies) and also select different bandwidth for p2p depending on time conditions (with static services qualification policies).

Static Service Qualification Policies with Time of Day Conditions

Static Service Qualification policies can be based on time conditions, so, the characteristics of the service (rating group, service bandwidth, and so on) is only applicable during a period.

- 1 Static Service Qualification policies with time of day conditions where the PCEF controls times.

Therefore, in addition to the PCC rule, the SAPC determines the Revalidation time (this time indicates the PCEF when to reauthorize the service) and service activation/deactivation times.

If there are configured static service qualification policies based on time conditions, the SAPC performs the following process:

- 1 Determines the static service name (Charging Rule Name) and the time when the static service name should change (this time is the Validity Time)
- 2 Using the smallest validity time obtained in the previous step and considering that currently it is this time, determines the static service name that is authorized and the time when the static service name is no longer authorized
- 3 The minimum validity time obtained in the second step is the Revalidation time, this time indicates to the PCEF when to reauthorize the service.

For those static service names obtained in both previous steps and no change in the static service names is detected for the future, the SAPC installs the static service name without activation nor deactivation times.

For those static service names obtained in both previous steps and in case a change in the static service names is detected for the future, the SAPC installs the static service name with activation time equals to current time and deactivation time equals to its validity time obtained in the first step.



For those static service names obtained in the first step and not obtained in the second one, the SAPC installs the static service name with activation time equals to current time and deactivation time equals to the validity time obtained in the first step.

For those static service names obtained in the second step, the SAPC installs the static service name with activation time equals to the validity time obtained in first step and deactivation time equals to the validity time from the second step.

- 2 Static Service Qualification policies with time of day conditions where PCRF controls times.

When PCRF is chosen as controller of time of day conditions, neither service activation/deactivation times or revalidation time are provided to the PCEF.

The SAPC calculates an internal validity that is the minimum time and date conditions configured among all the evaluated rules. The SAPC triggers a new reauthorization when this time and date condition is reached. Refer to Policies based on Time on Day Conditions section in [Subscription and Policy Management](#).

2.2.5 Notification of Errors in the Installation of Services

When a static or preconfigured service is not correctly installed or can no longer be maintained in the PCEF, it sends a notification towards the SAPC indicating that the corresponding PCC rules are not active, which means that the rules are removed (case of preconfigured) or deactivated (case of static) in the PCEF. The notification also includes a failure code that indicates the reason of the failure.

In such case, the SAPC also removes the PCC rules and performs policy evaluation ignoring the affected PCC rules, regardless of the failure code received.

The SAPC supports the notification of error for static, preconfigured, and dynamic PCC rules. For handling the notification of errors in the installation of dynamic PCC rules, refer to [Dynamic Policy Control \(Rx\)](#).

2.3 Service Charging Control

Service Charging Control allows SAPC to assign different charging data depending on service and subscriber basis.

2.3.1 Charging Control for Static Services with the PCEF

As it is explained in Static Services Qualification policies of Section 2.2 on page 5, each static service can be associated with several static service names in the PCEF, each name is associated with a certain set of properties, one of these properties can be the Rating Group of the static service.



The SAPC is able to select the static service name to be applied to the static service by evaluating the Static Services qualification policies, that can take into account subscriber information, dynamic conditions and context information received (for example SGSN IP address, RAT). By this way, the SAPC can control the rating to be applied to static services handled by the PCEF.

Static Services qualification policies are evaluated each time service access control is performed (see Section 2.2 on page 5).

2.3.2 Charging Control for Preconfigured Services with the GGSN/PDN GW

The SAPC is able to provide to the PCEF the following charging data applicable to authorized preconfigured services:

- Service identifier: Identifier of the service used for charging purposes.
- Rating-Group: Charging key for the service used for rating purposes.
- Reporting-Level: level on which the PCEF reports the usage.
- Metering-Method: defines if duration and/or volume should be metered for offline charging.
- Online/Offline: defines whether the Online and/or Offline should be enabled or disabled from the PCEF.

The SAPC selects the charging data to be applied to a service evaluating service charging policies according to the following precedence allocation:

- 1 Subject policy locator
- 2 Subject group policy locator. All the active subscriber groups are considered.
Therefore 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. Refer to Solving Policies Conflicts section in *Subscription and Policy Management*.

If there are not configured policies or the policies are not fulfilled, the SAPC obtains the charging profile provisioned for the service (Qualification data of service profile).

Service Charging Control is performed at:

- IP-CAN session establishment.
- IP-CAN session reauthorization because of:
 - IP-CAN session modification.



- Update subscriber data, refer to [Subscription and Policy Management](#).
- Changes owing to Fair Usage Control, refer to [Fair Usage Control](#)
- Events received from the Application Function (for further details, refer to [Dynamic Policy Control \(Rx\)](#)).

If Service Charging Control is not configured for the requested PCEF, no charging data are either selected or sent to the PCEF as part of the authorized services.

2.4 Subscriber Charging Control

Subscriber Charging Control allows SAPC to assign different charging data depending on the subscriber or subscriber group.

The SAPC is able to provide to the PCEF the following charging information applicable for a subscriber:

- **Charging Characteristics:** It is an **Ericsson Value Added** function, it can be used by the PCEF to select the user category and charging profile, to determine if credit control is to be used or not, or to select a particular charging server to be used when several servers are available, and so on.

It is an Ericsson Value Added function and its availability depends on the capabilities of the PCEF and the SAPC.

The PCEF can send to the SAPC the value provided from HLR and the SAPC can overwrite it in the PCEF.

- Default charging method: online or offline
- Primary and Secondary online and offline charging systems addresses.

The SAPC selects the charging data to be applied to a subscriber applying the mechanism for controls using both conditional (policies) and unconditional (static) qualification data explained in "Selection of Data to apply to the Subscriber" section in [Subscription and Policy Management](#).

Subscriber Charging Control is performed at:

- IP-CAN session establishment.

If Subscriber Charging Control is not configured for the requested PCEF, no subscriber charging data are either selected or sent to the PCEF for the IP-CAN session.

2.5 Content Filtering

The SAPC is able to provide the SASN/EPG with the applicable content filtering profile per subscriber (Ericsson Added Value). The SASN/EPG uses this profile to



decide whether to allow or not the subscriber to access to a specific URL content. Content filtering may be required because of different reasons such as parental control, black/white lists, censorship, lack of subscription, or any content rights restrictions.

The SAPC selects the Content Filtering profile to be applied to a subscriber applying the mechanism for controls using both conditional (policies) and unconditional (static) qualification data explained in "Selection of Data to apply to the Subscriber" section in [Subscription and Policy Management](#).

Content Filtering Control is performed at:

- IP-CAN session establishment.
- IP-CAN session reauthorization because of:
 - IP-CAN session modification.
 - Update subscriber data, refer to [Subscription and Policy Management](#).
 - Changes owing to time conditions, refer to [Subscription and Policy Management](#).
 - Changes owing to Fair Usage Control, refer to [Fair Usage Control](#)

If Content Filtering Control is not configured for the requested PCEF no content filtering data is either selected or sent to the PCEF for the IP-CAN session.

2.6 Event Triggers

Event triggers define events that cause the PCEF to request new access and charging decisions to the SAPC. Some of the possible events are:

- SGSN change
- PLMN change
- Radio Access Technology change
- IP-CAN type change
- Out of credit
- Reallocation of credit
- AN-GW change
- Tracking Area change
- E-UTRAN Cell change
- User location change

- Change of UE presence in Presence Reporting Area report

The SAPC performs the event trigger selection at:

- IP-CAN session establishment.
- IP-CAN session reauthorization because of:
 - IP-CAN session modification.
 - Update subscriber data, refer to [Subscription and Policy Management](#).
 - Time conditions configured in policies are reached. The SAPC only calculates an internal validity time from the time and date conditions configured in the last evaluated rule., refer to [Subscription and Policy Management](#).
 - Changes owing to Fair Usage Control, refer to [Fair Usage Control](#)

The SAPC obtains all event triggers statically provisioned at subscriber, active subscriber groups and global subscriber group.

Also, the SAPC evaluates Event Trigger Selection policies applicable to the subscriber, that is, policies associated to the subscriber, the active groups to which the subscriber belongs to and the global policies. Event Trigger Selection policies allow multiple result, so the event triggers of all rules within all the selected policies that evaluate to true are obtained.

The SAPC extends the event triggers from the dynamic selection to the event triggers from the static selection. All event triggers in the list are summed up ensuring that no event triggers are repeated since no precedence is applied between the event triggers at the subscriber, active subscriber group, or the SAPC level.

Whenever event triggers are changed, the SAPC provides a new complete list of subscribed event triggers. In case the SAPC selects no event trigger after performing Event Triggers Selection, the SAPC sends the Event-Trigger AVP set to the special value NO_EVENT_TRIGGERS.

2.7 Multiple Gx Support

The SAPC supports network scenarios where multiple PCEFs handle the same IP-CAN session for the same subscriber establishing multiple Gx sessions towards the SAPC. Multiple Gx support is an advanced feature offered by the SAPC that takes into account both events from bearers and DPI information to make the fine-tuned enforcement to the network.

In these scenarios, the SAPC consolidates the information received from all the multiple Gx sessions and is able to complement the information received from one Gx session with the information received from the others Gx sessions corresponding to the same IP-CAN session for the subscriber, that is, information



received from one Gx session can be used to enforce policies in the other Gx session.

2.8 Presence Reporting Area

The SAPC supports Presence Reporting Area (PRA) following 3GPP specifications.

A Presence Reporting Area is an area defined within 3GPP Packet Domain for the purposes of reporting UE presence within that area due to policy control. A PRA may consist in a set of neighbor or non-neighbor Tracking Areas, or eNBs, cells, etc.

With the PRA function, the SAPC monitors the location change when the UE enters or leaves the pre-defined area for policy control. This means that the PCEF only notifies the SAPC when the UE enters or leaves the PRA. The SAPC has to subscribe to the event trigger for the presence status of the UE (within or outside the PRA) to the PCEF.

This function reduces the frequency of sending location change information so that the amount of signalling in the network is reduced. It also simplifies some location based use cases, as policies can be defined in the SAPC based solely in the UE presence in or out of the PRA.

There are two types of PRA over Gx:

- UE-dedicated PRA

This is defined at subscriber level, and composed of a short list of TAs/RAs, or eNodeBs and/or cells/SAs in a PLMN. The element list is defined in the SAPC and sent towards the PCEF.

- Core Network pre-configured PRA

This is predefined in the SGSN-MME and composed of a short list of TAs/RAs, or eNodeBs and/or cells/SAs in a PLMN. The SAPC sends a PRA identifier to the PCEF to indicate the PRA predefined in the SGSN-MME.

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

- Subscriber profile,
- User location, for example users located in concert hall, stadium, festival,
- Device type,
- APN,
- Other data received through Gx interface

The PRA selection is performed only in the Gx session establishment. Only one PRA can be selected per Gx session.

The SAPC can request to start reporting the UE presence changes in a PRA by subscribing the event trigger `CHANGE_OF_UE_PRESENCE_IN_PRESENCE_REPORTING_AREA_REPORT`. To stop the reporting, the SAPC removes the event trigger.

The policy decisions based on PRA status can be performed in Gx session modification and reauthorization.

The SAPC selects the PRA applying the mechanism for controls using both conditional and unconditional qualification data explained in Selection of Data to apply to the subscriber section in Subscription and Policy Management.

The following figure shows how to use PRA for policy control in the UE Attach or PDN connectivity scenario:

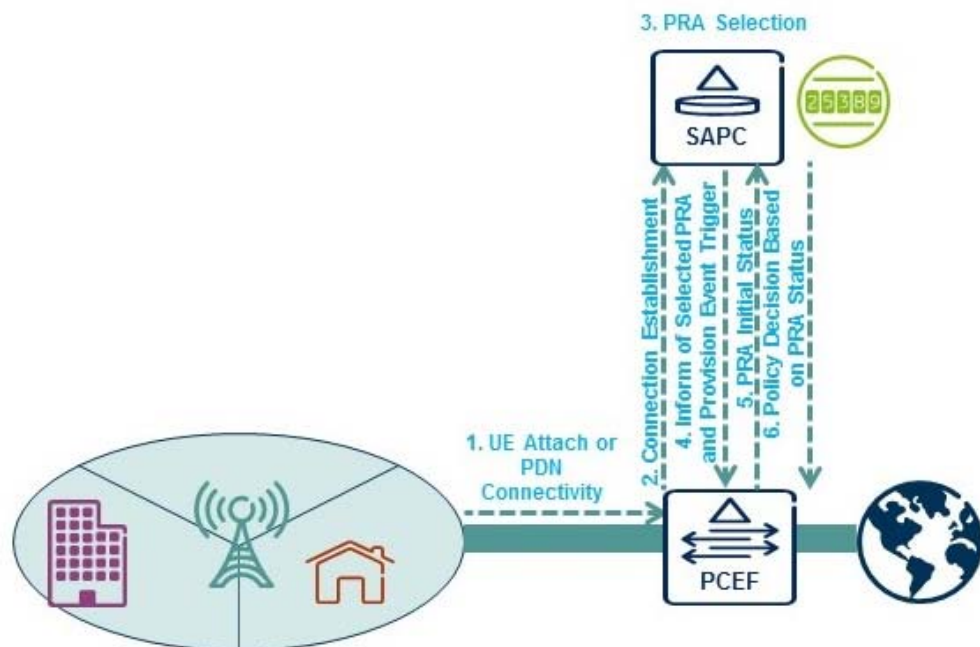


Figure 5 PRA over Gx

- 1-2: When a UE attaches to the network or connects to a PDN, the PCEF requests session establishment to the SAPC.
- 3: The SAPC performs PRA selection.
- 4: The SAPC answers the session establishment informing the PCEF of the selected PRA and event triggers.
- 5: If the event trigger is subscribed, the PCEF reports the PRA initial status to the SAPC. Otherwise, the PCEF does not report the PRA initial status.
- 6: The SAPC then makes policy decisions based on the PRA status. When the UE moves in or out of the PRA, the SAPC makes policy decisions based



on the PRA status change received from the PCEF, and updates the policy decision to the PCEF.

2.9 Diameter Race Condition Handling

The SAPC is able to handle diameter race conditions that may occur in the Gx and Ericsson Gx+ interfaces due to traffic events that happen concurrently or within a short time frame.

The solution involves two inter-related mechanisms:

- Handling of concurrent Gx Re-Authorization Request (RAR) and Credit-Control-Request (CCR) messages. This resolves situations where the state of an IP-CAN session is concurrently being modified from the PCEF and from the SAPC.
- Handling of concurrent SAPC-initiated reauthorizations. This resolves situations where the SAPC requires to perform multiple session reauthorizations within a short time period, in particular when the SAPC requires to send a new Gx RAR message before the previous Gx RAR message has been acknowledged.

2.9.1 Handling of Concurrent Gx RAR and CCR messages

The PCEF and the SAPC can initiate transactions that modify the state of the IP-CAN session independently (e.g. CCR from the PCEF and RAR from the SAPC) and potentially concurrently. Additionally, there may be diameter agents in between the PCEF and the SAPC that could cause messages to be delivered out of order. This can lead to race conditions that result in the wrong information maintained by the PCEF and/or the SAPC for the session.

Page 22 shows the typical message flow that results in a diameter race condition. From the point of view of the PCEF, the re-authorization request from the SAPC has occurred after the PCEF has initiated an IP-CAN session modification procedure; and so the RAR message cannot be safely handled until the ongoing procedure has been completed. However, from the point of view of the SAPC, the CCR-U message is received when there is a pending re-authorization request to be completed.

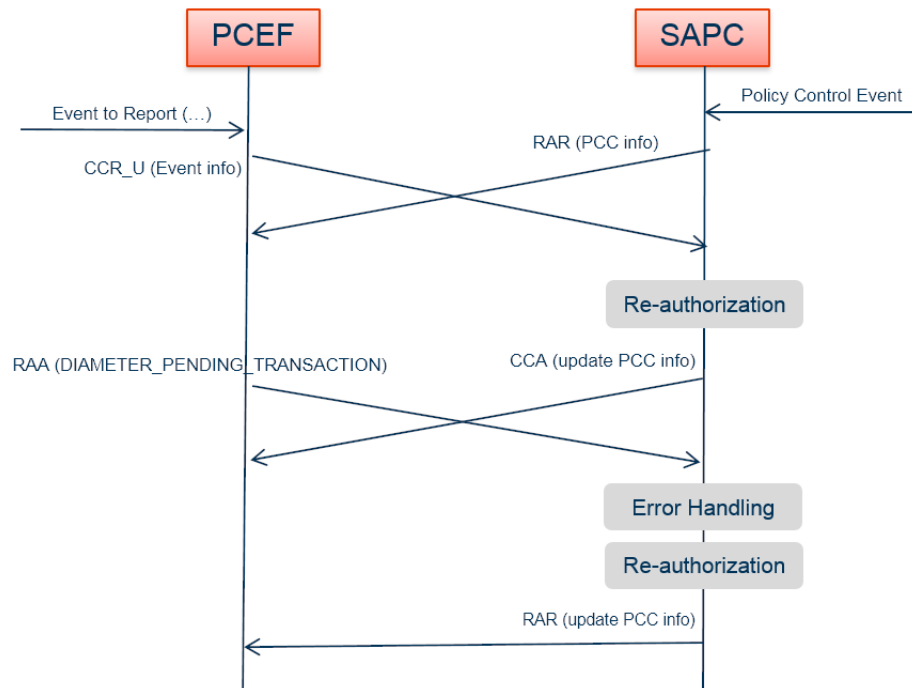


Figure 6 Diameter Race Condition

The procedure to handle this race condition situation is as follows:

- If the PCEF cannot handle the RAR message when there is an ongoing transaction on the session, the PCEF rejects the RAR message with diameter experimental result code of `DIAMETER_PENDING_TRANSACTION`, and keeps waiting for the reception of a Credit-Control-Answer (CCA) Update message from the SAPC.

Note: In legacy implementations, the PCEF may reject the RAR message with diameter result code of `DIAMETER_OUT_OF_SPACE` when a diameter race condition is detected. The SAPC can handle both protocol errors in the RAA message.

- When the SAPC receives a CCR-U message, the SAPC answers CCA-U as usual, even when there is an ongoing transaction on the session (i.e. a pending RAA message to be received).
- On the reception of Gx RAA message with result code `DIAMETER_PENDING_TRANSACTION`, the SAPC reauthorizes the session and sends a new RAR message to synchronize the policy information with the PCEF. The SAPC takes into account the information sent in the RAR that has been rejected, the current session state (that reflects the policy information that is currently being enforced in the PCEF) and the result of the new policy evaluation. With this information, the SAPC determines the valid policy information to be enforced in the PCEF. The policy information sent in the new RAR message consists of:
 - Policy information sent in the RAR message that was rejected but is still valid. For example, services that are still authorized in the IP-CAN



session, QoS information, etc. However, policy information sent in the RAR message that was rejected and is no longer valid, is not re-sent.

- New policy information as a result of new events that happen during the duration of the RAR/RAA transaction.

Therefore the new RAR message may contain the following policy information:

- PCC rule information to install and remove, including
 - Authorization state to specify the authorization state and reason for non-authorization for the charging rule names and charging rule base names
 - One time redirect control to specify one-time redirect is active or not for the charging rule names and charging rule base names
- Default bearer QoS information
- Event trigger information
- Content filtering profile to specify a local content filtering profile identifier in the Ericsson EPG
- Usage monitoring information
- Revalidation time

SAPC-initiated IP-CAN Session Termination

When the SAPC sends a request for session release (i.e. a RAR message with Session-Release-Cause AVP), the PCEF shall acknowledge the request immediately, wait for the current transaction to complete and perform the session termination procedure. However, if the PCEF returns an RAA with experimental result `DIAMETER_PENDING_TRANSACTION`, the SAPC re-attempts the RAR message with Session-Release-Cause AVP.

Maximum Number of Re-attempts

The SAPC implements a mechanism to limit the number of times to re-attempt the same request due to the reception of a `DIAMETER_PENDING_TRANSACTION` indication from the PCEF. This is to avoid infinite reattempting RARs. The maximum number of reattempts is a node configuration parameter set by Ericsson personnel (default value is 0); when reached, no further actions are taken.

Gx Feature Negotiation

Handling of diameter pending transactions is an optional feature that is negotiated during session establishment. However, the SAPC handles a race condition error received in the RAA message, regardless of whether the PCEF has indicated support of the optional feature in Gx CCR-I message or not.

Note: This is to enable inter-operability with legacy PCEFs that do not fully support the functionality according to the 3GPP standards.

2.9.2 Handling of Concurrent SAPC-initiated Reauthorizations

In certain network scenarios, the SAPC may need to perform multiple session reauthorizations within a short time period, triggered by either internal (e.g. time of day conditions) or external events (e.g. Sy events, AF events, subscriber profile change, etc.) that overlap in time. In this situation, the resulting RAR messages need to be sent to the PCEF sequentially, to avoid inconsistencies.

The SAPC does not send any new RAR message to the PCEF until the previous RAR has been acknowledged for the same IP-CAN session, or the maximum waiting time to receive the RAA message has been exceeded.

The procedure is as follows:

- Before performing a session reauthorization due to an internal or external trigger, the SAPC checks if there is a previous Gx RAR pending to be acknowledged for the same IP-CAN session.
 - If there is no pending RAA to be received, the SAPC performs the session reauthorization and sends the Gx RAR message.
 - If there is a pending RAA to be received, the SAPC starts a maximum waiting timer and delays sending the Gx RAR until the RAA is received or the timer expires.
- Other internal or external events that occur for the same IP-CAN session during the time period where the SAPC is waiting for acknowledgment of a RAR message, do not trigger a session reauthorization. Reauthorizations are delayed until the end of the time period or reception of the RAA message.
- When the timer expires, the SAPC performs the pending session reauthorization and sends a new RAR message including all the pending policy information to be communicated to the PCEF.
- If the RAA message is received while the maximum waiting timer is running, the SAPC stops the timer, performs a session re-authorization and sends the RAR message with all the pending policy information to be communicated to the PCEF. Also, if the RAA includes the result code `DIAMETER_PENDING_TRANSACTION`, the new RAR message also contains information about the policies that failed to be enforced in the PCEF, as described in Section 2.9.1 on page 21.
- If the SAPC receives a CCR-U message while the maximum waiting timer is running, the SAPC performs a session re-authorization depending on the event received in the CCR-U message, as usual. This reauthorization takes into account any other event received from sending the RAR message to reception of the CCR-U message. However, in this case the PCC rules that contain network location information cannot be sent in the CCA message (as this is not currently allowed in 3GPP standards), but are sent in a new



RAR message after reception of the acknowledgement of the previous RAR message or when the timer expires.

- If the IP-CAN session is terminated, the SAPC stops the maximum waiting timer and process the CCR-T message.

The maximum waiting time for reception of the RAA message is configured by Ericsson personnel (default value is 0).





3 Access and Charging Control Network Deployments

The SAPC can provide Access and Charging Control in the following network deployments:

- Ericsson EPG: through Ericsson Rel9 Gx+ onwards.
- Ericsson SASN, through Ericsson Rel9 Gx+
- Non-Ericsson PCEF, through standard 3GPP Gx (from Rel9 onwards).
- The SAPC also supports multiple PCEFs deployments.





4 Access and Charging Control Traffic Cases

This chapter explains the interfaces involved in Service Access and Charging Control.

For detailed description of each of the interfaces supported, the corresponding interface description should be consulted.

The precondition to all traffic cases is as follows:

- A diameter connection is already established between the SAPC and the PCEF.
- The PCEF is configured in the SAPC and all the required controls are enabled for the PCEF.
- The availability of this function in the SAPC is under license control, otherwise SAPC rejects any Gx message by answering with Result-Code DIAMETER_UNABLE_TO_COMPLY=5012.
- The number of simultaneous IP sessions has not reached the hard limit of the corresponding licensed IP sessions capacity, otherwise SAPC rejects any new IP session creation by answering with Result-Code DIAMETER_UNABLE_TO_COMPLY=5012.

4.1 IP-CAN session Lifetime

These traffic cases show the IP-CAN session life cycle: establishment, modification, and termination.

The following figure shows the Diameter messages exchanged in a communication between the PCEF and the SAPC:

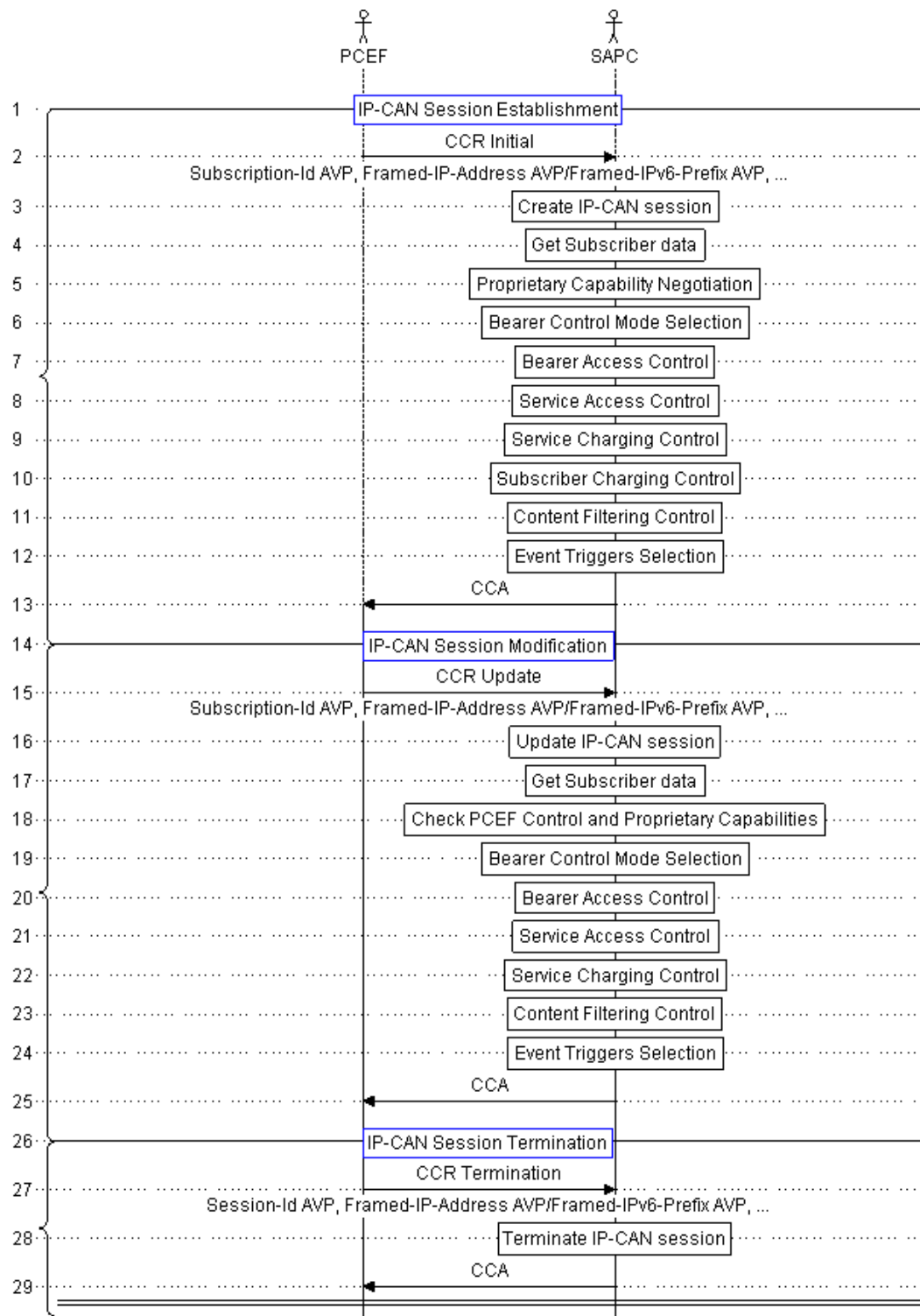


Figure 7



The following sections explain each of these steps showing the specifics for each Gx protocol binding.

4.1.1 Protocol Binding for Rel9 Gx/Gx+ onwards

Session-Id AVP is mandatory for all the messages in Gx protocol. Session-Id AVP is globally unique and univocally identifies an IP-CAN session.

The SAPC identifies the subscriber IP-CAN session using Framed-IP-Address AVP or Framed-IPv6-Prefix AVP together with Called-Station-Id AVP and Subscription-Id AVP.

Note: Ericsson added value: new AVPs and standard AVPs including any modification to include extra function are marked in **bold**.

However, Ericsson added value function is optional and the service can always be provided as defined in standard without using the proprietary AVPs or the modifications of the standard ones.

IP-CAN session establishment

- 2: The SAPC receives a Gx CCR-initial message from the PCEF indicating IP-CAN session establishment. The main information that the PCEF provides is:
 - **Gx-Capability-List AVP** may be provided indicating the offered proprietary functions. The following list indicates the possible values for the supported features:
 - Enhanced service authorization control: If set, the use of non-authorization codes is possible
 - RuleSpace negotiation: If set, the SAPC may be able to negotiate the Rule Space assigned to IP-CAN session.
 - Charging Characteristics retrieval: Set if the PCEF expects the SAPC to retrieve the Charging Characteristics specified for the subscriber and return it to the PCEF.
 - Support of Content Filtering Profile Identifier: When set the Content Filtering Profile id installation is supported.
 - Support of One Time Redirect: When set the One Time Redirect activation is supported.
 - **Rule-Space-Suggestion AVP** is used to indicate the rule space proposed by the client and changeable by the SAPC.
 - **Rule-Space-Decision AVP** is used to indicate the rule space that will be used by the client.

Note: If the Rule Space Negotiation is indicated in the Gx-Capability-List either Rule-Space-Suggestion AVP or Rule-Space-Decision AVP has to be sent by the client.

- Supported-Features AVP

The SAPC selects the protocol version to use according to the Supported-Features AVP value received.

- If the Supported-Features AVP is not present in the CCR-Initial message, the SAPC rejects the IP-CAN session establishment with the error code DIAMETER_MISSING_AVP (5005).
- Supported-Features AVP should have at least Rel9 (bit 1) or Rel10 (bit 3) set. If the PCEF requests session establishment with Gx interface Release 8 (only bit 0 set), the SAPC returns the error code DIAMETER_INVALID_AVP_VALUE (5004).

- IP-CAN-Type AVP

It indicates the type of Connectivity Access Network in which the user is connected:

- In a GRPS scenario, the received IP-CAN-Type is 3GPP-GPRS.
- In an EPS scenario, IP-CAN-Type is 3GPP-EPS.
- In WLAN scenarios, IP-CAN-Type is NON-3GPP-EPS

- Framed-IP-Address, Framed-IPv6-Prefix AVP or both, indicating UE IPv4 address and/or UE IPv6 prefix.

When both Framed-IP-Address and Framed-IPv6-Prefix AVPs are received, an IPv4v6 dual stack IP-CAN session is created.

- Subscription-Id is needed to fully support the enhanced service authorization function, IMSI, MSISDN, NAI, END_USER_PRIVATE (for example with a MAC address). Subscription-Id AVP can contain one or several traffic identities

- Called-Station-Id AVP (optional)

- RAT-Type AVP

Note: 3GPP-RAT-Type accepted for 3GPP-GPRS accesses owing to backward compatibility reasons.

- 3GPP-SGSN-MCC-MNC

- 3GPP-SGSN-Address or 3GPP-SGSN-IPv6-Address

- User location information (received within 3GPP-User-Location-Info or RAI).



- 3GPP-MS-TimeZone
 - User-Equipment-Info
 - Network-Request-Support
 - AN-GW-Address containing IPv4 or IPv6 addresses of the access node gateway
 - 3GPP-Charging-Characteristics
- 3: The SAPC creates an IP-CAN session state for this subscriber's request and this PCEF. When the UE IP-CAN session is controlled by several PCEFs, all the IP-CAN session states shall share the common network information.
- 4: The SAPC looks for the subscriber and subscriber group profile.

The SAPC maintains a mapping between the different subscriber traffic identities and the subscriber identifier. The SAPC looks for the corresponding subscriber id, based on the identity mapping information. The subscriber id obtained is used to access to the subscriber profile. If the SAPC does not find any mapping, it uses the traffic identity as key to find the subscriber profile.

Besides, the SAPC can be configured to select which of the traffic identities received in the Subscription-Id AVP should be used. If it is not configured, the first received Subscription-Id AVP is used. If it is desired to use NAI traffic identity, it should be received the first Subscription-Id AVP of the request message.

If subscriber is not found, refer to Subscribers not known by the SAPC in [Subscription and Policy Management](#).

- 5: The SAPC looks in the configuration data for the controls applicable for the requesting PCEF and also decides the proprietary capabilities to be applied towards the PCEF.

The SAPC capabilities decision is made taking into account the supported capabilities received from the PCEF and the corresponding controls to be applied towards the PCEF. If the capability is not supported by the PCEF or the control does not apply to the requesting PCEF, the SAPC decides that the proprietary capability is not allowed.

Gx-Capability-List AVP is set to:

- Enhanced service authorization control: capability (bit 0) set to '1' if this value is received from the PCEF and Service Access Control applies towards the PCEF.
- RuleSpace negotiation capability (bit 3) set to '1' if this value is received from the PCEF .

- Charging Characteristics capability (bit 4) set to '1' if this value is received from the PCEF and Subscriber Charging Control applies towards the PCEF.
- Content Filtering capability (bit 12) set to '1' if this value is received from the PCEF and Content Filtering Control applies towards the PCEF.
- One Time Redirect capability (bit 16) set to '1' if this value is received from the PCEF and Service Access Control applies towards the PCEF.

Each bit is set to '0' if any of its required conditions is not fulfilled.

This information is available during the IP-CAN session life. Next steps apply or not according to this information.

— 6: The SAPC performs Bearer Control Mode Selection

The SAPC performs Bearer Control Mode selection taking into account the information received from the PCEF. The SAPC sets Bearer-Control-Mode AVP to value:

- UE_ONLY (0), if Network-Request-Support AVP was received in CCR with value Network Request Not Supported, or if the Network-Request-Support AVP was not received.
- UE_NW (2), if Network-Request-Support AVP was received in CCR with value Network Request Supported.

— 7: The SAPC performs IP-CAN Session Access Control

The SAPC evaluates IP-CAN Session Access Control policies (see Section 2.1 on page 4). Result-Code AVP with a value indicating either success (IP-CAN session operation is authorized) or failure (IP-CAN session operation is not authorized) is included in the CCA.

The Result-Code DIAMETER_AUTHORIZATION_REJECTED (5003) is used to indicate that the IP-CAN session is not authorized. In that case, the IP-CAN session shall not be established.

— 8: The SAPC performs Service Access Control

The function Service Access Control (see Section 2.2 on page 5) is applied for the IP-CAN session. Service Access Control at IP-CAN session establishment is applied to static and preconfigured services.

The following data is obtained:

- **Rule-Space-Decision** AVP, if the SAPC has the capability to perform Rule Space Negotiation and the SAPC decides to overwrite the Rule-Space-Suggestion AVP received in the CCR.
- Charging-Rule-Install AVP including the PCC rules to install corresponding to the authorized PCC rules obtained as a result of the service



authorization process for static and preconfigured services and static services qualification process (see Section 2.2.4 on page 11). For **Ericsson Rel9 Gx+ onwards** the PCC rules corresponding to non-authorized static services are also included if the corresponding capabilities are received from the PCEF. Those static PCC rules sharing extra information regarding **Charging-Rule-Authorization** AVP, are grouped under the same Charging-Rule-Install instance.

- Charging-Rule-Name AVP
- Charging-Rule-Base-Name AVP

It is included if this PCC rule is authorized but static service qualification is not applied. For **Ericsson Rel9 Gx+ onwards** it can also be included if the PCC rule is not authorized.

- Charging-Rule-Definition AVP: this is only applicable to preconfigured services.
 - Include the Charging-Rule-Definition corresponding to the authorized preconfigured services

Note: **Precedence** of the preconfigured PCC rules is composed of a static part configured by the operator (optional) and a dynamic part calculated by the SAPC.

Dynamic part is calculated for preconfigured and dynamic PCC rules depending on the completeness of downlink filters.

- If the downlink filter of the PCC rule is defined with specific source IP, source and destination port, it has the higher precedence (lowest numeric value, 0).
- If some information is missing or incomplete in downlink filters, the precedence is smaller (higher numeric value), according to:
 - Source IP: increment +1 when IP is not defined; increment +2 if it is ANY
 - Source port: increment +1 if it is a list or range; increment +2 if it is ANY.
 - Destination port: increment + 1 if it is a list or range; Increment +2 if it is ANY.

Precedence for dynamic PCC Rules is higher than for static and preconfigured ones.

- Bearer Identifier AVP, it is included if it was received in CCR message

If Time of Day procedures are applicable and the PCEF is selected as time controller the following AVPs are also included:

- Rule-Activation-Time AVP indicating to the PCEF that it should set the PCC rules within this Charging-Rule-Install AVP active after this time.
- Rule-Deactivation-Time AVP indicating to the PCEF that it should set the PCC rules within this Charging-Rule-Install AVP inactive after this time.

For **Ericsson Rel9 Gx+ onwards** the static PCC rules include the authorization state:

— **Charging-Rule-Authorization AVP**

- **Authorization-State AVP** to specify the authorization state and reason for non-authorization for the Charging-Rule-Names and Charging-Rule-Base-Names provided in this Charging-Rule-Install AVP instance.

Note: For Ericsson Rel9 Gx+ onwards, non-authorization codes are not applicable if there are Time of Day conditions.

If Time of Day procedures are applicable and the PCEF is selected as time controller the following AVP is also included:

- Revalidation-Time AVP: It is used to indicate to the PCEF that before this given time, new PCC rules should be requested.
- 9: The SAPC performs Service Charging Control for preconfigured services. The resulting charging profile data are included in the PCC rule definition charging data:
 - Service-Identifier AVP
 - Rating-Group AVP
 - Reporting-Level AVP
 - Online AVP
 - Offline AVP
 - Metering-Method AVP
- 10: The SAPC performs Subscriber Charging Control, obtaining the following data:
 - Charging-Information AVP
 - Online AVP
 - Offline AVP



- **3GPP-Charging-Characteristics AVP.**
- 11: The SAPC performs Content Filtering Control for **Ericsson Rel9 Gx+ onwards**. If the Content Filtering capability is set to "1" in step 5, the SAPC gets the Content Filtering to the applied subscriber. For more information, see section 2.6.

If no Rule-Space-Id has been obtained after the rule-space negotiation process, `_ServiceDomain_` is used as Resource in Content Filtering policies.

- 12: The SAPC performs Event Triggers Selection, which selects the events that shall cause a re-request of PCC rules within the **Event-Trigger** AVP. The following values are applicable for this function:
 - **SGSN_CHANGE (0)** This value shall be used to indicate that upon the change of the serving SGSN PCC rules shall be requested.
 - **RAT_CHANGE (2)** This value shall be used to indicate that upon a RAT change PCC rules shall be requested.
 - **PLMN_CHANGE (4)** This value shall be used to indicate that upon a PLMN change PCC rules shall be requested.
 - **IP_CAN_CHANGE (7)** This value shall be used to indicate that upon an IP-CAN type change PCC rules shall be requested.
 - **RAI_CHANGE (12)** This value shall be used to indicate that upon a change in the RAI, PCC rules shall be requested.
 - **USER_LOCATION_CHANGE (13)** This value shall be used to indicate that upon a change in the user location (for GPRS or EPS scenarios), PCC rules shall be requested.
 - **OUT_OF_CREDIT (15)** This value shall be used to indicate that upon an out of credit-related event PCC rules shall be requested.
 - **REALLOCATION_OF_CREDIT (16)** This value shall be used to indicate that upon a reallocation of credit related event PCC rules shall be requested.
 - **REVALIDATION_TIMEOUT (17).** This value is downloaded to indicate that at revalidation time event new PCC rules should be requested.
 - **AN_GW_CHANGE (21)** This value shall be used to indicate that upon a change of the serving Access Node Gateway PCC rules shall be requested.
 - **UE_TIME_ZONE_CHANGE (25)** This value shall be used to indicate that upon a change to the time zone the UE is located in, PCC rules shall be requested.
 - **TAI_CHANGE (26)** This value shall be used to indicate that upon a change in the TAI PCC rules shall be requested.

- ECGI_CHANGE (27) This value shall be used to indicate that upon a change in the ECGI PCC rules shall be requested.
- 13: The CCA message is sent to the PCEF including the information previously computed (PCC rules installed, Charging data), Event triggers and Supported-Features AVP.

IP-CAN session modification

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

The CCR triggered by IP-CAN session modification only contains the new/modified parameters together with the associated event-triggers.

- 16: The SAPC updates the IP-CAN session state with the new information received. When the UE IP session is controlled by several PCEFs, the new network information shall be shared by all the IP-CAN session states. If the IP-CAN session does not exist, the SAPC rejects the request and answers with Diameter error code DIAMETER_UNKNOWN_SESSION_ID.
- 17: The SAPC looks for the subscriber and subscriber group profile. See Page 33.
- 18: The SAPC checks the controls and capabilities applicable for the requesting PCEF obtained in the IP-CAN session establishment. Next steps apply or not according to this information.
- 19: The SAPC performs Bearer Control Mode Selection

If requested by the PCEF, the SAPC performs Bearer Control Mode selection.

The SAPC performs Bearer Control Mode selection taking into account the information received from the PCEF. The SAPC includes Bearer-Control-Mode AVP only if Network-Request-Support was received in the CCR, and sets its value to:

- UE_ONLY (0), if Network-Request-Support AVP was received in CCR with value Network Request Not Supported.
- UE_NW (2), if Network-Request-Support AVP was received in CCR with value Network Request Supported.

Note: Network-Request-Support is an optional parameter that can be received anytime during session lifetime. If no value of Network-Request-Support is provided in the message, it is applied the previous value provided in the IP-CAN session.

- 20: The SAPC performs IP-CAN Session Access Control

Result-Code AVP with a value indicating either success (IP-CAN session operation is authorized) or failure (IP-CAN session operation is not authorized) is included in the CCA.



The Result-Code `DIAMETER_AUTHORIZATION_REJECTED` (5003) is used to indicate that the IP-CAN session is to be deactivated.

- 21: The SAPC performs Service Access Control for static, preconfigured, and dynamic services, obtaining the following results to be inserted in the CCA:
 - **Charging-Rule-Install** AVP that includes the authorized PCC rules obtained as a result of the service authorization process for static and preconfigured services, and static services qualification process which were not previously installed. In the PCC rules, the SAPC includes the IP flows for IPv4, IPv6 or both, according to the IP-CAN session that was initially established.

For **Ericsson Rel9 Gx+ onwards**, the non-authorized PCC rules corresponding to static services previously authorized are also included. Those static PCC rules sharing extra information regarding Charging-Rule-Authorization AVP are grouped under the same Charging-Rule-Install instance

- Charging-Rule-Name

- Charging-Rule-Base-Name

It is included if this PCC rule is authorized but static service qualification is not applied. For **Ericsson Rel9 Gx+ onwards** it can also be included if the PCC rule is not authorized.

- Charging-Rule-Definition including Flow-Status set to enabled. **Precedence** of the preconfigured PCC rules is composed of a static part configured by the operator (optional) and a dynamic part calculated by the SAPC. The dynamic part is calculated according to the completeness of the DL flows of the PCC rule. See description of how precedence is calculated in chapter Page 35.

- Bearer-Identifier

For **Ericsson Rel9 Gx+ onwards** the static PCC rules include the authorization state:

- **Charging-Rule-Authorization** including:

Authorization State to specify the authorization state and reason for non-authorization for the Charging-Rule-Names and Charging-Rule-Base-Names provided in this **Charging-Rule-Install** AVP instance.

If Time of Day procedures are applicable and the PCEF is selected as time controller the following two AVPs are also included in CCA:

- Rule-Activation-Time

- Rule-Deactivation-Time

- Charging-Rule-Remove AVP, including the PCC rules to be removed.

For standard 3GPP Gx Rel9 onwards those PCC rules of static, preconfigured, and dynamic services previously installed and not longer authorized and those PCC rules of static services previously installed with a different qualification (static access).

For **Ericsson Rel9 Gx+ onwards** those PCC rules of static services previously installed as non-authorized and now they are authorized with a given qualification are also removed.

- Charging-Rule-Name
- Charging-Rule-Base-Name

If Time of Day procedures are applicable and the PCEF is selected as time controller the following AVP is also included:

- Revalidation-Time AVP: It is used to indicate to the PCEF that before this given time, new PCC rules should be requested.
- 22: The SAPC performs Service Charging Control for preconfigured and dynamic services, the resulting charging profile data are included in the PCC rule definition charging data:
- Service-Identifier AVP
 - Rating-Group AVP
 - Reporting-Level AVP
 - Online AVP
 - Offline AVP
 - Metering-Method AVP
- 23: The SAPC performs Content Filtering Control for **Ericsson Rel9 Gx+ onwards**. If the resulting value for Content-Filtering-Profile-Id AVP is the same as the previously downloaded value, then the SAPC does not download it. If no value is obtained for Content-Filtering-Profile-Id and a different value was previously downloaded for the AVP then, it is downloaded with a value of 0xFFFFFFFF towards the PCEF.
- If no Rule-Space-Id has been obtained after the rule-space negotiation process, _ServiceDomain_ is used as Resource in Content Filtering policies.
- 24: The SAPC performs Event Trigger Selection. If the event triggers are changed, the SAPC includes the complete list of event triggers or the special NO_EVENT_TRIGGERS value if no event trigger is selected. If the event triggers are not changed, the Event-Trigger AVP is not included. For the values applicable for this function, see step 12 of Section 4.1.1 on page 31.
- 25: The CCA message is sent to the PCEF only including the new/modified Policy and Charging Control information.



IP-CAN session termination

- 27: The SAPC receives a CCR Termination from the PCEF indicating IP-CAN session termination, containing, at least, Session-Id AVPs.
- 28: The SAPC terminates the IP-CAN session for the requesting PCEF.
- 29: The SAPC sends a CCA message to the PCEF including the Result-Code AVP with value SUCCESS.

4.2 Redirect Owing to non-authorized Static Service

This traffic case shows how non-authorization code can be used by the EPG to redirect the subscriber to a web portal, so the subscriber can subscribe to the service if desired.

In this example, it is considered that HTTP-Streaming service is provisioned to the subscriber as static service but it is configured a Service Authorization policy that allows the usage of this service only if the subscriber is not roaming and in case roaming, such reason of non-authorization should be returned by the SAPC. Said non-authorization code triggers an HTTP redirection in EPG, so that the user is sent to a site where the user is informed about that HTTP-Streaming service is not available in roaming.

This traffic case can be performed using Ericsson Rel9 Gx+ onwards.

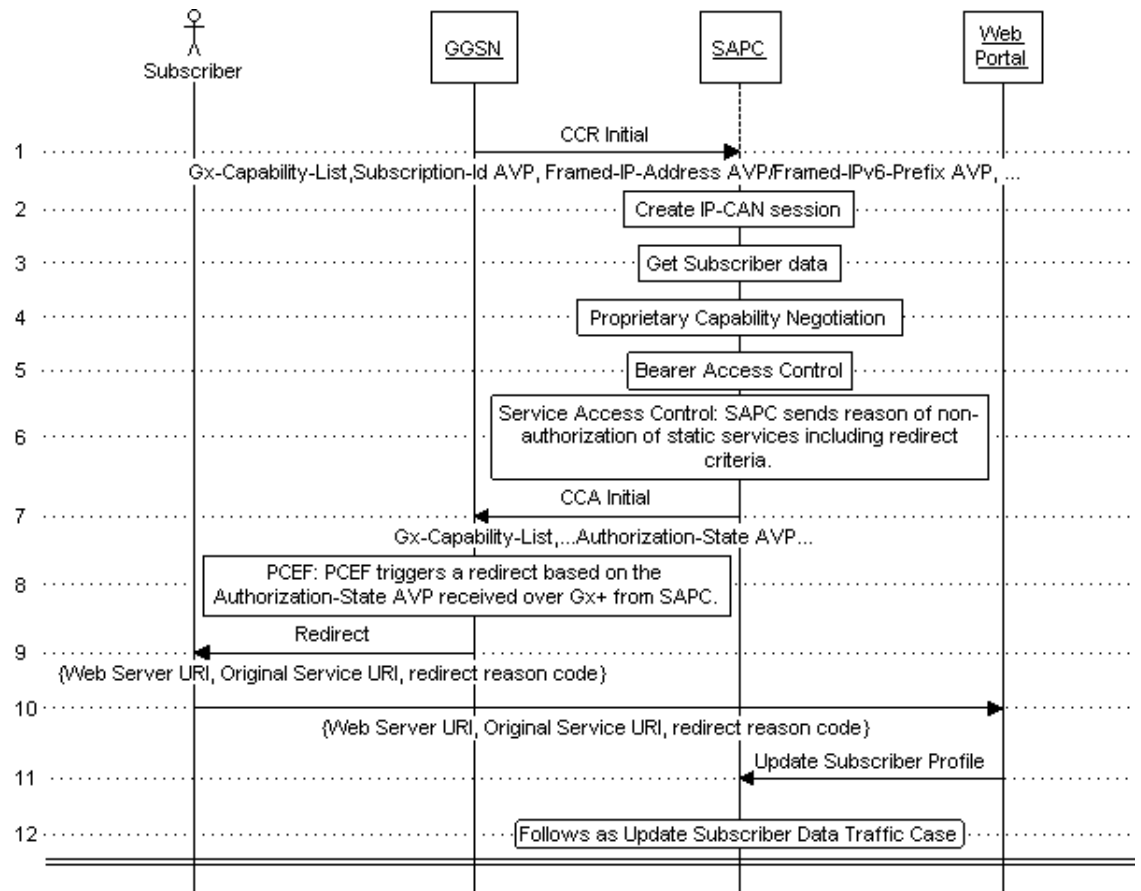


Figure 8 Redirect Owing to Non-authorized Static Service

— 1–6 IP-CAN session is established as explained in Section 4.1.1 on page 31.

- 4: **Gx-Capability-List AVP** with Enhanced service authorization control capability set should be received from EPG and Service Access Control should be applicable towards EPG.
- 6: The SAPC performs Service Access Control.

As the subscriber is roaming, result obtained from evaluation of service authorization policies to be inserted in CCA message is:

— Charging-Rule-Install AVP including the Charging-Rule-Name AVP configured for Chat service and **Charging-Rule-Authorization AVP** with **Authorization-State AVP** set to DENIED_ROAMING value.

— 7: The CCA message is sent to the EPG including the information previously computed, as explained in Section 4.1.1 on page 31.

— 8-10: When EPG detects traffic for HTTP-streaming, EPG triggers a redirection based on the reason for the service to be unauthorized obtained



from the SAPC. EPG can be configured with different redirect destinations based on the non-authorization reason.

User traffic is redirected to a portal that explains to the subscriber why the service is unauthorized and presents buying options to the subscriber.

- 11: The SAPC receives an Update Subscriber Profile requesting the provisioning of a new service offering for the subscriber.
- 12: Traffic case follows as Update Subscriber data Traffic case (refer to Subscription and Policy Management).

4.3 One Time Redirect for Authorized Static Services

This traffic case shows how One Time Redirect is performed for any authorized static service.

In this example, it is considered that HTTP-Streaming service is provisioned to the subscriber as static service and OTR is provisioned for this service.

This traffic case can only be performed using Ericsson Rel9 Gx+ onwards.

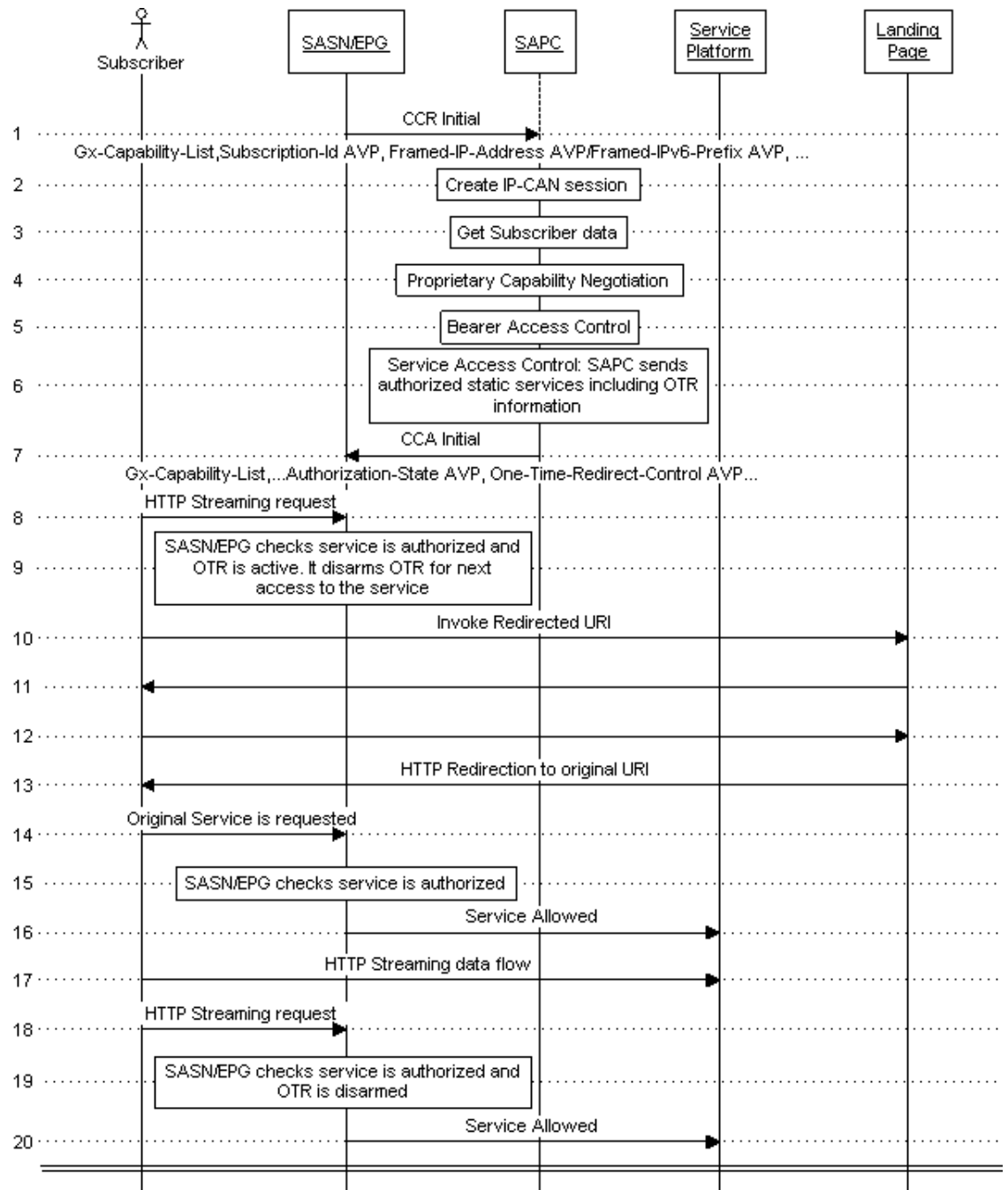


Figure 9 One Time Redirect for Authorized Static Services

— 1-6: IP-CAN session is established as explained in Section 4.1.1 on page 31

- 4: **Gx-Capability-List AVP** with One Time Redirect support capability set should be received from SASN/EPG and Service Access Control should be applicable towards SASN/EPG.



- 6: The SAPC performs Service Access Control.

Result obtained from evaluation of service authorization policies and OTR information is inserted in CCA message:

- Charging-Rule-Install AVP including the Charging-Rule-Name or Charging-Rule-Base-Name AVP configured for HTTP Streaming service and **Charging-Rule-Authorization AVP** with **Authorization-State AVP** set to 'Authorized' (0) value and **One-Time-Redirect-Control AVP** set to active (1) value.
- 7: The CCA message is sent to SASN/EPG including the information previously computed, as explained in Section 4.1.1 on page 31.
- 8: The subscriber requests a first HTTP Streaming service.
- 9: When SASN/EPG detects traffic for HTTP-streaming, it checks that the service is authorized and OTR is active, so it triggers a redirection and disarms OTR for the service.

SASN/EPG can be configured with different redirect destinations depending on the service.

- 10-17: Redirection is applied by the terminal and after the corresponding checks, the service is allowed and the subscriber can access to the service.
- 18: The subscriber requests HTTP Streaming service by second time.
- 19: SASN/EPG checks that this service is authorized and that OTR is disarmed for it.
- 20: The service is allowed after the corresponding checks in SASN/EPG and the user can access to the service. Redirection is not applied since it is not the first HTTP streaming request.

4.4 Service Authorization and Static Service Qualification Policies with Time of Day Conditions When the PCEF is Selected As Time Controller

Either the PCRF or the PCEF can be selected as time controllers when Time of Day conditions applies in Service Access Control.

These traffic cases show examples of Service Authorization and Static service qualification policies based on time conditions when the PCEF is the time controller.

4.4.1 Time of Day Conditions Applied Only to Service Authorization Policies

In this example it is considered that the following service authorization policies are configured for a subscriber:



- Service 1 (modeled as charging-rule-base-name-1) should be authorized from 10 a.m. to 17 p.m.
- Service 2 (modeled as charging-rule-name-2) should be authorized from 8 a.m. to 16 p.m. and from 20 p.m. to 22 p.m.

Static service qualification policies are not configured.

The SAPC performs the following authorization process when receiving a CCR message at 12 p.m.:

- 1 Determines if the service is authorized or not and the time when the authorization state should change (this time is the Validity Time)
 - Service 1 is authorized with a validity time = 17 p.m.
 - Service 2 is authorized with a validity time = 16 p.m.
- 2 Using the smallest validity time obtained in previous step (16 p.m.) and considering that currently it is this time (16 p.m.), the SAPC determines again if the service is authorized or not and the time when the authorization state should change:
 - Service 1 is authorized with a validity time = 17 p.m.
 - Service 2 is not authorized with a validity time = 20 p.m.
- 3 Finally, the SAPC includes the following information in CCA message:
 - Charging-Rule-Install AVP including:
 - Charging-Rule-Base-Name = 1
 - Rule-Activation-Time = 12 p.m.
 - Rule-Deactivation-Time = 17 p.m.
 - Charging-Rule-Install AVP including:
 - Charging-rule-name AVP = 2
 - Rule-Activation-Time = 12 p.m.
 - Rule-Deactivation-Time = 16 p.m.
 - Revalidation-Time = 17 p.m.

The SAPC sends to the PCEF the active services at the moment of receiving the request message and the next active service. It also sends the Revalidation time as the time the second service becomes inactive, so that, the PCEF should request reauthorization towards the SAPC to get the next active service.



4.4.2 Time of Day Conditions Applied to Service Authorization and Static Service Qualification Policies

In this example it is considered that the following policies are configured for a subscriber:

- Service 1 (modeled as charging-rule-base-name-1) should be authorized from 10 a.m. to 17 p.m.

In addition, different Bandwidth applies for the service depending on time (using static access qualification policies):

- Low Bandwidth (modeled as charging-rule-name-3) from 10 a.m. to 12.30 p.m. and 14 p.m. to 17 p.m.
 - High Bandwidth (modeled as charging-rule-name-4) from 12.30 p.m. to 14 p.m.
- Service 2 (modeled as charging-rule-name-2) should be authorized from 8 a.m. to 16 p.m. and from 20 p.m. to 22 p.m.

The SAPC performs the following process when receiving a CCR message at 12 p.m.:

- 1 Service Authorization policies are evaluated, it determines if the service is authorized or not and the time when the authorization state should change (this time is the Validity Time), obtaining:
 - Service 1 is authorized with a validity time = 17 p.m.

Static service qualification policies are evaluated, it determines the static service name (Charging Rule Name) and the time when the static service name should change:

 - Charging-rule-name-3 is obtained with a validity time = 12.30 p.m. - Service 2 is authorized with a validity time = 16 p.m.
- No Static Access policies are provisioned for this service.
- 2 Using the smallest validity time obtained in previous step (12.30 p.m.) and considering that currently it is this time (12.30 p.m.), the SAPC determines again if the service is authorized or not and the time when the authorization state should change:
 - Service 1 is authorized with a validity time = 17 p.m.

Static service qualification policies are evaluated:

 - Charging-rule-name-4 is obtained with a validity time = 14 p.m. - Service 2 is not authorized with a validity time = 16 p.m.
- 3 Finally, the SAPC includes the following information in CCA message:



- Charging-Rule-Install AVP including:
 - Charging-rule-name AVP = 3
 - Rule-Activation-Time = 12 p.m.
 - Rule-Deactivation-Time = 12.30 p.m.
- Charging-Rule-Install AVP including:
 - Charging-rule-name AVP = 4
 - Rule-Activation-Time = 12.30 p.m.
 - Rule-Deactivation-Time = 14 p.m.
- Charging-Rule-Install AVP including charging-rule-name AVP = 2
 - Rule-Activation-Time = 12 p.m.
 - Rule-Deactivation-Time = 16 p.m.
- Revalidation-Time = 14 p.m.

4.5 Presence Reporting Area

These traffic cases show the Gx session life cycle with the PRA function: establishment, modification, and termination.

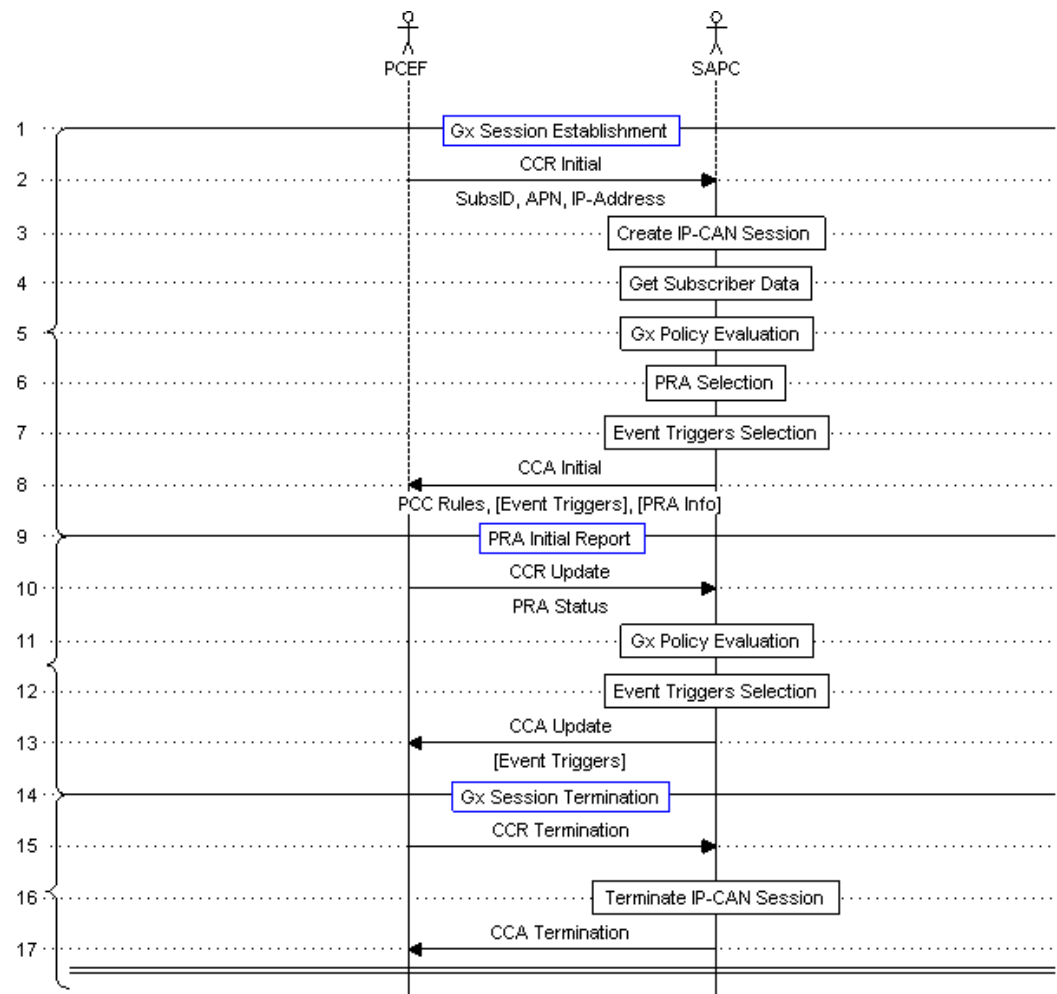


Figure 10 Gx Session Lifetime with PRA Over Gx Function

Gx session establishment

— 2: The SAPC receives a Gx CCR-initial message with the following AVPs:

- Framed-IP-Address, Framed-IPv6-Prefix AVP or both, indicating UE IPv4 address and/or UE IPv6 prefix.

When both Framed-IP-Address and Framed-IPv6-Prefix AVPs are received, an IPv4v6 dual stack session is created.

- Subscription-Id is needed to fully support the enhanced service authorization function. IMSI, MSISDN, and NAI could be received in this Gx context. Subscription-Id AVP can contain one or several traffic identities.
- Called-Station-Id AVP indicating the APN for the IP-CAN session.

- 3: The SAPC creates an IP-CAN session state for this subscriber's request and PCEF.
- 4: The SAPC looks for the subscriber and subscriber group profile. See step 4 of Section 4.1.1 on page 31.
- 5: The Gx policy controls are evaluated. See steps 5-11 of Section 4.1.1 on page 31.
- 6: The SAPC performs the PRA selection.
- 7: The SAPC performs the event triggers selection. The Event-Trigger value applicable for PRA is:
 - **CHANGE_OF_UE_PRESENCE_IN_PRESENCE_REPORTING_AREA_REPORT (48)**: This value is used to indicate when the user enters or leaves the PRA as indicated in the Presence-Reporting-Area-Information AVP.
- 8: The CCA message is sent to the PCEF including the information previously computed (Presence-Reporting-Area-Information AVP) and event triggers.

PRA initial report

- 10: If event trigger Presence-Reporting-Area was sent from the SAPC, the PCEF sends a CCR Update including the following information:
 - **Presence-Reporting-Area-Identifier AVP**: This indicates the PRA to which specific information refers.
 - **Presence-Reporting-Area-Status AVP**: This indicates the status of UE for the PRA. The possible values are:
 - IN_AREA (0)**: This value is used to indicate that the UE moved into the PRA.
 - OUT_OF_AREA (1)**: This value is used to indicate that the UE moved out of the PRA.
- 11: This step is the same as step 5. In this case Proprietary Capability Negotiation is not performed.
- 12: This step is the same as step 7.
- 13: The CCA-U message is sent to the PCEF including the information previously computed.

Gx session termination

- Idem as explained in Section 4.1.1 on page 31.



4.6 PCC Rule Error Handling

4.6.1 Protocol Binding for Rel9 Gx/Gx+ onwards Notification of Error in the Installation of PCC rules

This traffic case shows the notification of an error in the installation of PCC rules. It is valid for GPRS and EPS scenarios.

As an example of the Diameter messages exchange in a communication between the PCEF and the SAPC, see the following figure:

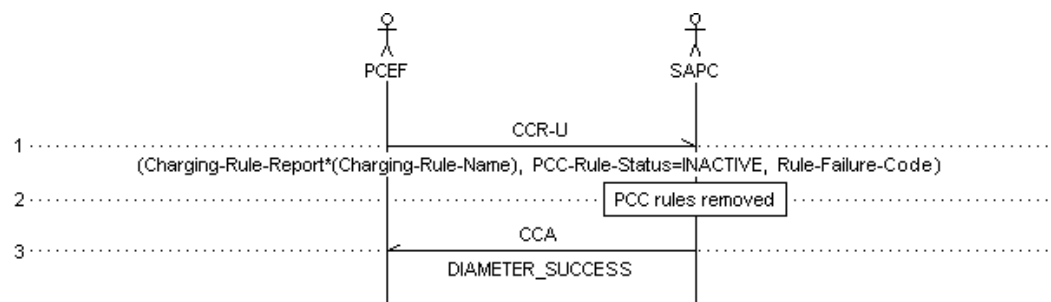


Figure 11 Notification of Error in the Installation of PCC rules

IP-CAN session modification

- 1: The SAPC receives a Gx CCR-update message from the PCEF indicating that the previous installation of PCC rules has failed. The main information that the PCEF provides is:

- Session-Id
- Charging-Rule-Report AVP

It indicates the status of the installation of PCC rules.

- Charging-Rule-Name

It indicates the PCC rules affected.

- Charging-Rule-Base-Name

It indicates the Charging-Rule-Names affected.

- PCC-Rule-Status

It contains the value INACTIVE to indicate an error in the installation of the PCC rules

- Rule-Failure-Code

It indicates the reason a PCC Rule is being reported.

- 2: The SAPC updates the session information (removing the PCC rules affected) and performs policy evaluation ignoring the affected PCC rules.
- 3: CCA message is sent to the PCEF to acknowledge the IP-CAN session modification.

If there are any dynamic PCC rules that are reported as inactive, the SAPC notifies the corresponding AF sessions, this is described in [Dynamic Policy Control \(Rx\)](#).

4.7 Diameter Race Condition Handling

The following traffic flow shows how the SAPC handles diameter race condition errors in an IP-CAN session.

The precondition is that the IP-CAN session has been established, and race conditions happen due to internal or external events.

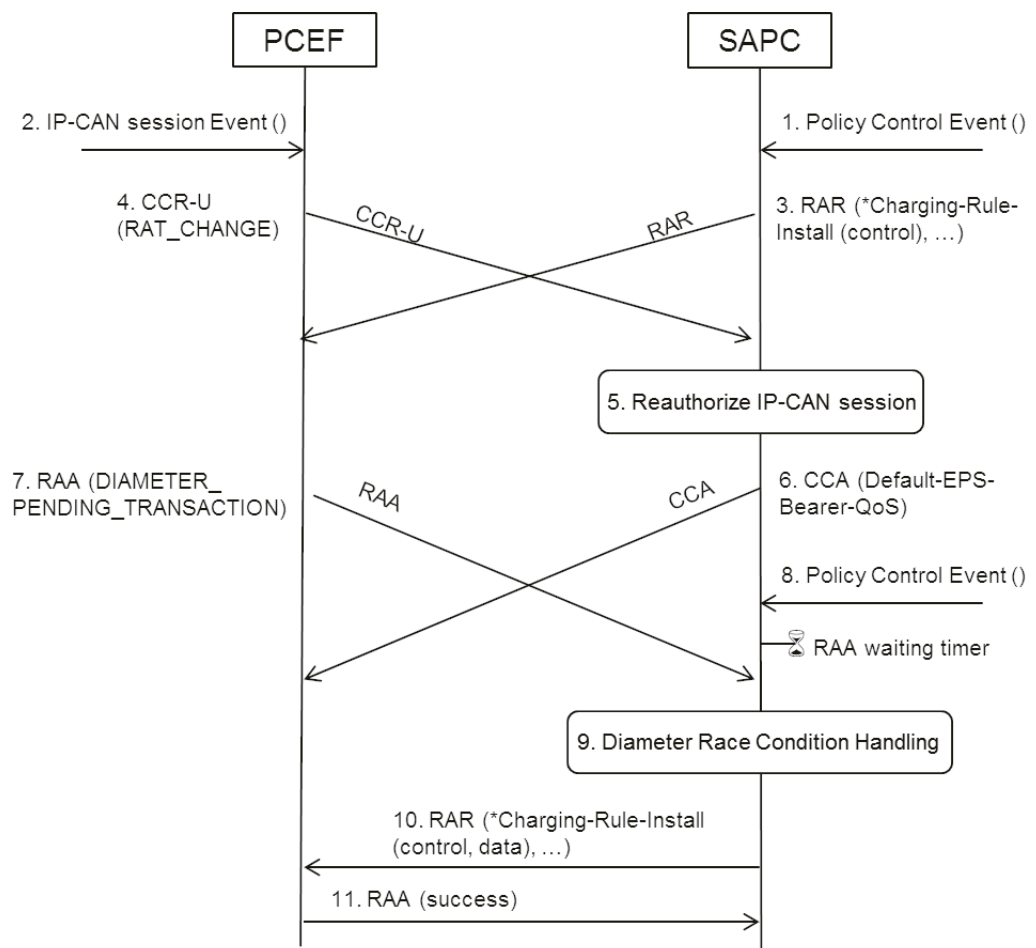


Figure 12 Diameter Race Condition Handling

- 1-2. The SAPC receives an internal or external trigger to re-evaluate PCC Rules and policy decision for an IP-CAN session. For example, the AF sends a



diameter AAR message to establish a new audio media service. And at the same time, the PCEF receives a request for IP-CAN session modification, for example due to a change in the RAT type.

- 3-4. The SAPC sends a RAR message to the PCEF that includes the PCC rule to be installed for the audio service. At the same time, the PCEF sends a CCR-U message to the SAPC indicating a change in the RAT Type.
- 5-6. The SAPC performs a reauthorization of the IP-CAN session and sends a CCA message to the PCEF including the updated policy control information. For example, the SAPC may update the default bearer QoS as a result of the RAT type change.
- 7. On reception of the RAR message when there is an ongoing transaction on the session, the PCEF returns a diameter RAA message with an Experimental-Result AVP including the Experimental-Result-Code AVP set to DIAMETER_PENDING_TRANSACTION (4144).
- 8. The SAPC receives an internal or external trigger to re-evaluate PCC Rules and policy decision for an IP-CAN session. For example, the AF sends a diameter AAR message to establish a new data media service. The SAPC detects that there is a pending RAA to be received for the same IP-CAN session, and starts a timer to wait for the RAA message. No Gx RAR message is sent to the PCEF at this point in time.
- 9. The SAPC receives an RAA message including the Experimental-Result-Code AVP set to DIAMETER_PENDING_TRANSACTION. If the configured maximum number of reattempts is not reached, the SAPC reauthorizes the IP-CAN session and determines the policy control information to be sent to the PCEF (for details see Section 2.9.1 on page 21).
- 10. The SAPC sends a re-attempting RAR message to the PCEF with the latest policy information. In this case, the SAPC includes the PCC rule to be installed for the audio service and also for the data service.

4.8 Access and Charging Control Error Handling

The SAPC may answer with the following error codes:



Table 1 Error Handling

Error Condition	Action	Code
The SAPC receives a CCR and the corresponding IP-CAN session is not authorized.	The SAPC returns a CCA indicating an error. No other information is included in the error message. In case of CCR-I, the Gx session is not established. In case of CCR-U, the PCEF shall send a new CCR-T immediately upon the reception of the CCA containing such error code.	Result-Code AVP set to DIAMETER_AUTHORIZATION_REJECTED (5003)
The SAPC receives a CCR-U/T for a diameter session not found in the SAPC	The SAPC returns a CCA indicating an error	Result-Code AVP set to DIAMETER_UNKNOWN_SESSION_ID (5002)
The SAPC receives a CCR-I for a subscriber not defined in DB and autoprovisioning and subscriber unknown features are disabled.	The SAPC returns a CCA indicating an error and the session is not established.	Result-Code AVP set to DIAMETER_USER_UNKNOWN (5030)
The SAPC receives a CCR request from a PCEF not configured in the SAPC	The SAPC returns a CCA indicating an error.	Result-Code AVP set to UNABLE_TO_COMPLY (5012)
The SAPC receives a CCR that cannot be complied owing to an internal error (for example, because of temporal DB error)	The SAPC returns a CCA indicating an error	Result-Code AVP set to UNABLE_TO_COMPLY (5012)
The SAPC receives a CCR with a mandatory parameter missed	The SAPC returns a CCA indicating an error including one or more Failed-AVP AVP containing the AVPs that caused the failure	Result-Code AVP set to DIAMETER_MISSING_AV P (5005)



Error Condition	Action	Code
The SAPC receives a CCR with an invalid AVP value	The SAPC returns a CCA indicating an error including one or more Failed-AVP AVP containing the AVPs that caused the failure	Result-Code AVP set to DIAMETER_INVALID_AV P_VALUE (5004)
The SAPC receives an IP-CAN session establishment request with Gx interface Release 7	The SAPC rejects the IP-CAN session establishment and returns a CCA indicating an error	Result-Code AVP set to DIAMETER_MISSING_AV P 5005
The SAPC receives an IP-CAN session establishment request with Gx interface Release 8	The SAPC rejects the IP-CAN session establishment and returns a CCA indicating an error	Result-Code AVP set to DIAMETER_INVALID_AV P_VALUE 5004
The SAPC receives an RAA message including the Experimental-Result-Code AVP set to DIAMETER_PENDING_TRANSACTION (4144) or DIAMETER_OUT_OF_SPACE (4002)	The SAPC reauthorizes the IP-CAN session and determines the policy information to send to the PCEF to resolve the error	





Reference List

Ericsson Documents

- [1] Bearer QoS and Bandwidth Management
- [2] Dynamic Policy Control (Rx)
- [3] Subscription and Policy Management

Standards

- [4] Policy and charging control architecture , 3GPP TS 23.203