

Subscription and Policy Management

Ericsson Service-Aware Policy Controller

FACILITY DESCRIPTION

Copyright

© Ericsson España, S.A. 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	Subscription and Policy Management Introduction	1
2	Subscription and Policy Management Function	3
2.1	Subscription Management	4
2.1.1	Subscriber Management	4
2.1.1.1	Subscribers not known by the SAPC. Internal Repository	6
2.1.1.2	Subscribers not known by the SAPC. External Database	7
2.1.1.3	Removal of Subscribers	8
2.1.2	Subscriber Group Management	8
2.1.3	External Database	9
2.1.4	Reauthorization Because of Subscription Change	9
2.2	Handling of Multiple service offerings	10
2.2.1	Temporary Subscriber Groups	11
2.2.2	Handling of Subscriber Group Priority	13
2.3	Dynamic Group Selection Policies	13
2.4	Policy Management	14
2.4.1	Selecting Applicable Policies	15
2.4.2	Language Used in Policies	16
2.4.3	Policy Evaluation Process	17
2.4.3.1	Data Used for Policy Evaluation	17
2.4.3.2	Selection of Data to Apply to the Subscriber	18
2.4.3.3	Solving Policies Conflicts	19
2.4.4	Policies Based on Time of Day Conditions	20
2.5	Reauthorization Because of Time of Day Conditions	21
2.6	Header Enrichment	21
3	Subscription and Policy Management Traffic Cases	23
3.1	Update Subscriber Profile	23
3.2	Remove Subscriber Profile	24
3.2.1	Remove Subscriber Profile using standard Rel9 Gx/Gx+ onwards	25
3.2.2	Subscriber Profile defined in Ericsson OCS and SAPC. Remove Subscriber Profile only from SAPC	26
3.2.3	Disabled massive reauthorizations	27
3.2.4	Emergency Services	29
3.3	Subscriber Group activation/deactivation Because of Time Conditions	30
3.3.1	Subscriber Group activation/deactivation Because of Temporary Subscription using Rel9 Gx/Gx+ onwards.	30
3.3.2	Subscriber Group activation/deactivation Because of Static and Dynamic conditions using standard Rel9 Gx onwards or Ericsson Rel9 Gx+ onwards.	31



3.4	Policy Result Change Because of Time Conditions	33
3.5	Failure Handling	35
4	Restrictions	37
	Reference List	39



1 Subscription and Policy Management Introduction

This document describes subscription and policy management in the SAPC.





2 Subscription and Policy Management Function

The SAPC acts as a central policy node in the network and performs the following functions:

- Takes decisions about QoS, service access control, bandwidth limitation, usage accumulation, and so on, based on subscriber data and flexible policies (conditions) configured by the operator.
- Manages subscribers and subscriber groups to which it can apply these policies. Subscriber groups are a group of subscribers that have the same service offering. However, if operators want to apply an individual offer with particular data or conditions to a subscriber, operators can use subscriber data to apply individual offers.
- Takes decisions using its flexible policy engine that evaluates operator configured conditions, which use subscriber data, subscriber dynamic information, accumulated usage, time and date conditions, and so on.
- The SAPC can optionally use data stored in external repositories, such as the SPR, to evaluate the data in policy conditions, refer to [Database Access](#).

Subscriber data comprises of static and dynamic data:

- Static data is statically provisioned data to the subscriber and the subscriber groups to which the subscriber belongs.

Static subscription data is described in Section 2.1 on page 4.

- Dynamic data is data configured using policies and obtained by the policy engine.

Selecting and evaluating policies in the SAPC is described in Section 2.4 on page 14.

The following figure shows an overview of the subscriber data:

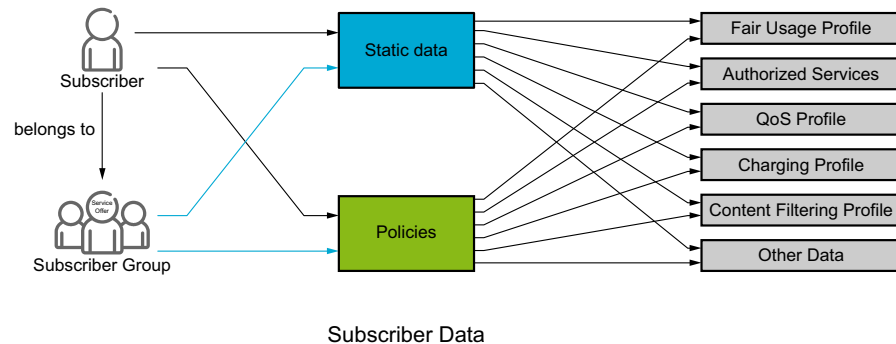


Figure 1 Subscriber Data Overview

For detailed information about how static and dynamic data are combined to build the final subscriber profile, see Section 2.4.3.2 on page 17.

2.1 Subscription Management

Subscription management function comprises of the following subfunctions:

- Subscriber management

Subscriber management provides specific data to the subscriber. Each subscriber can be associated with several service offerings that are managed using subscriber groups. Service offerings can be customized for a subscriber using the subscriber management function.

- Subscriber group management

Subscriber group management provides common data to a group of subscribers. Operators usually provide a set of service offerings to their subscribers that can be managed as subscriber groups in the SAPC. In this way, service offerings data can be provisioned only once.

Summarizing, if Subscriber group management provides common data to a group of subscribers, the Subscriber management provides specific data to a subscriber.

The effective data of a subscriber is a combination of subscriber data with the subscriber group data.

2.1.1 Subscriber Management

Each subscriber to which the SAPC should provide Policy Control capabilities should be defined in the SAPC internal database or external database (except if the SAPC performs autoprovisioning or Subscriber Unknown is used).

This subsection explains the main **static data** that can be provisioned to a subscriber. Static data can be provisioned when it is desired to provide any



additional or different data from the data configured for the subscriber groups to which the subscriber belongs to and these data do not depend on dynamic conditions.

The following are the main static parameters for a subscriber:

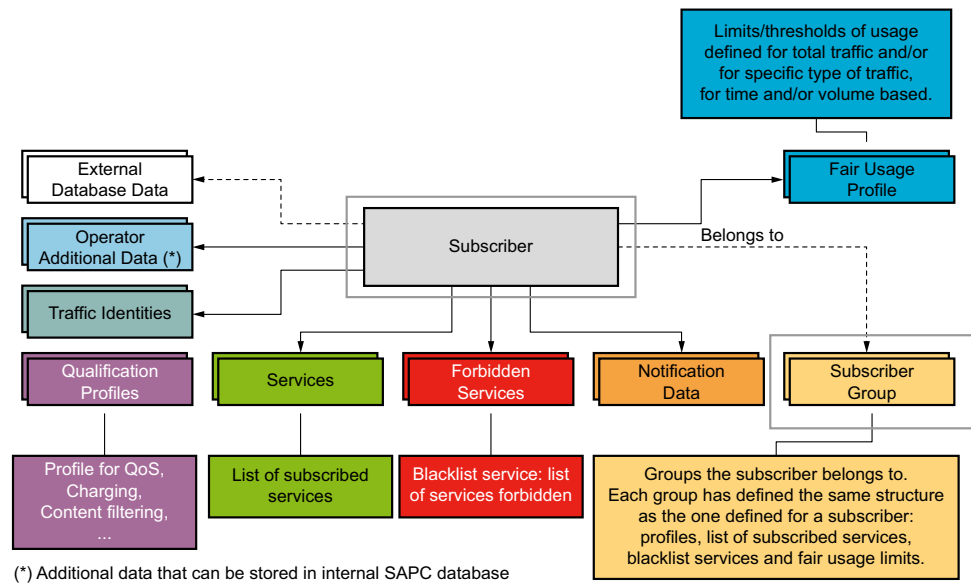


Figure 2 Subscriber Data

- Subscriber identifier is the administrative ID that it is used to identify the subscriber.
- Traffic identities are associated with a subscriber. Each subscriber can have several traffic identities, such as MSISDN, IMSI, and NAI. A subscriber traffic identifier is the identity sent in the requests by a traffic peer (GGSN/PDN-GW, AF, and so on.) to the SAPC. The SAPC maps different subscriber traffic identities to the subscriber identifiers. When the SAPC receives a request with a certain traffic identity, the SAPC looks for the corresponding subscriber ID, based on the identity mapping information. The subscriber ID obtained is used to access the subscriber profile. If the SAPC does not find any mapping, the SAPC uses the traffic identity as key to find the subscriber profile.
- Subscriber groups are the groups to which a subscriber belongs. This parameter is needed if the subscriber has a service offering that is common to many subscribers.

The association between a subscriber and subscriber groups can include:

- Subscriber group identifier
- A priority that the SAPC uses as a criteria to decide which subscriber group data to select, in case there is a conflict between the data from different subscriber groups

- Start date, or end date, or both for the subscriber group association

The SAPC also supports durations containing one or multiple sets of start date and end date for the subscriber group association. Each duration can contain start date, or end date, or both dates, or no date. For this type of association, start date or end date outside of the durations is not allowed.

For further information, see Section 2.2 on page 10.

- Subscribed services is the list of specific services associated with the subscriber.
- Blacklist services is the list of specific forbidden services associated with the subscriber.
- Subscriber qualification data is the data that characterizes the subscriber for each function the SAPC controls, such as QoS profile, charging profile, content filtering profile, header enrichment. They should be provisioned when these data does not depend on dynamic conditions.
- Notification data is the data needed to send notifications to the subscriber, such as the type of mechanism to be used and the receipt identity, which is where the notification is sent.
- Fair usage profile is the usage volume and/or time limits and set of data that specify usage accumulator characteristics. This data is needed if the operator wants to provide to the subscriber any fair usage data different from the data provided in the service offering applied to the subscriber group.
- Shared dataplan applicable to the subscriber: this data is used by Fair Usage Control function.

When any subscriber data is updated, the SAPC performs a reauthorization to check if any data should be added or removed and sent to the Enforcement Function, see Section 3.1 on page 23.

Additional Subscriber data

Subscriber data can be extended to be used in policy evaluation by defining Operator additional information. Any data stored in an external database can be used in policy evaluation.

2.1.1.1

Subscribers not known by the SAPC. Internal Repository

The SAPC can also provide policy control for subscribers that are not provisioned in a SAPC internal repository:

- Autoprovisioning function: A subscriber can be automatically provisioned in a SAPC internal repository when IP Session establishment is received from the Enforcement function.



- Subscriber Unknown: This is a special subscriber profile (default profile) that can be used for scenarios where subscriber differentiation is not needed, so it is not needed to provision the subscriber. Subscribers can share data profile.

The Subscriber Unknown profile can be applicable when both of the following conditions are true:

- The autoprovisioning policies evaluate to false, or when there are no autoprovisioning policies and
- The subscriber identity received in the traffic request is not found in the SAPC internal repository.

The following mutually exclusive steps are executed by the SAPC:

1. Autoprovisioning by dynamic assignment of a subscriber group to the automatically created subscriber:

Autoprovisioned policies are evaluated, and the result is the subscriber group profile to apply to the subscriber.

2. Autoprovisioning by static assignment of the default 'Autoprovisioned' subscriber group to the automatically created subscriber:

If autoprovisioning policies are not configured or not fulfilled, but 'Autoprovisioned' subscriber group profile is configured by the operator, the SAPC assigns the subscriber group profile to the subscriber.

3. If the above two conditions do not apply, autoprovisioning is not applied, and data from the Subscriber Unknown profile can be considered for processing the traffic request, if the profile is configured.

Note: If the subscriber group profile assigned to the autoprovisioned subscriber has any usage limit, the SAPC sends a reauthorization request message with the usage quota towards the Enforcement Function when the subscriber is automatically provisioned in the SAPC internal repository.

2.1.1.2

Subscribers not known by the SAPC. External Database

If the subscribers are provisioned in an external database:

- The autoprovisioning function cannot be applied.
- The Subscriber Unknown profile applies when the subscriber identity received in the traffic request is not found in the external database, the external database is down, or an error is received from the external database.

The Subscriber Unknown profile can be applicable, and can reside either in the SAPC internal repository or in an external database.



2.1.1.3 Removal of Subscribers

When a subscriber is removed by OAM and has an active IP-CAN session, the SAPC sends a reauthorization request message towards the Enforcement Function to terminate the session.

2.1.2 Subscriber Group Management

In the SAPC, service offerings can be managed as subscriber groups.

Using subscriber group management, operators can configure a common set of data for a group of subscribers simplifying the configuration. Each subscriber belonging to a subscriber group has the same set of data as other subscribers in the group.

A subscriber group consists of the following main **static data**:

- Subscriber group Identity: The identifier of the subscriber group.
- Subscribed Services: The list of services subscribed to by the group.
- Blacklist services: The list of services forbidden in the group.
- Subscriber Group Qualification data: The data associated with each function that the SAPC controls, such as QoS profile, Charging profile, Content Filtering profile, Header Enrichment. Subscriber Group Qualification data can be provisioned when the data does not depend on dynamic conditions.
- Notification data: This data is used if SMS is the desired mechanism to send the notifications to the subscribers of this group.
- Fair Usage profile: This is the usage volume limit, or time limit, or both to be applied to the service offering and set of data that specify usage accumulator characteristics.
- Default Priority: This is the priority assigned to the subscriber group, if it is not provisioned at subscriber level or shared dataplan level.

Note: Modifications to subscriber group data do not trigger a reauthorization of the subscribers belonging to that group.

Global Subscriber Group

The "Global Subscriber Group" is a special subscriber group, defined in the SAPC by default. The global subscriber group contains the default values to be applied to all the subscribers. Subscriber group priority and active period (explained in Section 2.2 on page 10) cannot be applied to the Global Subscriber Group, which has the lowest priority and applies forever (without temporary restrictions) unless there are dynamic group selection policies (explained in Section 2.3 on page 13) associated to it.



2.1.3 External Database

Subscriber data can be stored in external databases, or in the SAPC internal repository. For this purpose, Entity Data Sources must be defined inside the SAPC.

The following figure shows how the SAPC can use two external repositories:

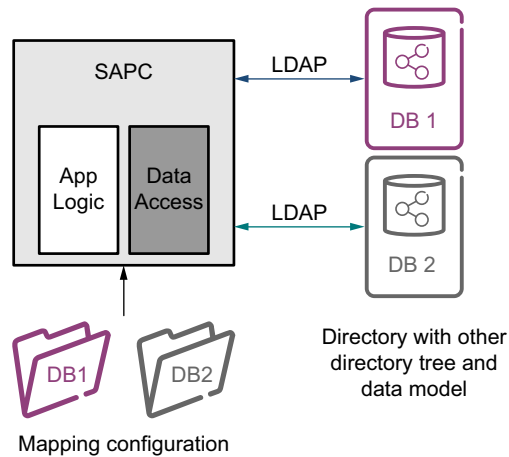


Figure 3 SAPC with external Database

The Entity Data Sources enable the retrieval of data from the corresponding repository and provide high flexibility for the SAPC to be integrated with different operator data models. The Entity Data Sources also enable the use of other data (apart of Subscriber data as requested by the SAPC data model) for policy evaluation.

The elements that form an Entity Data Source are the following:

- The name of an entity whose data is stored in one database or distributed across several databases.
- The location information about the database
- Information about how to obtain each field. The SAPC supports the following types of fields: constant fields, Entity Data Source field, and Entity Data Source reference fields, regarding another Entity Data Source

More information about usage of External Database function and Entity Data Sources configuration can be found in [Database Access](#).

2.1.4 Reauthorization Because of Subscription Change

The reauthorization because of Subscription Change allows the SAPC to update the IP session and thus provide new data to the Enforcement Function when a



subscription change affecting a single subscriber is ordered from the provisioning system.

The following subscription changes trigger a reauthorization process:

- A change in the set of Subscriber Groups associated to the subscriber. The removal and/or addition of a Subscriber Group to the subscriber subscription and the modification of the priority and/or the start and/or end date of a Subscriber Group initiate a subscriber reauthorization. The addition, removal, or modification of durations containing sets of start date and end date also initiates a subscriber reauthorization.
- A change in the set of Subscribed services and/or blacklist services assigned to a subscriber
- A change in the Subscriber Qualification data.
- A change in the Notification data
- A change in the Fair Usage profile assigned to the subscriber
- A change of the shared dataplan applicable to the subscriber.
- The addition, removal, or modification of traffic identifiers and the addition, removal, or modification of operator additional information defined for the subscriber
- The addition of a new subscriber, if there is an active IP-CAN session whose traffic identity is equal to the administration identifier defined for this new subscriber.
This happens when Subscriber Unknown profile is applied for a request and later the subscriber is provisioned with the administration identifier equal to the traffic identity received in previous request and IP-CAN session is still active.

There is a configuration option in the SAPC to disable the sending of reauthorization messages associated to subscription changes in case network traffic overload is too high. In this case, the new data are sent to the Enforcement Function when any message request is received from it.

2.2 Handling of Multiple service offerings

Each subscriber can be subscribed to multiple service offerings by associating the subscriber to several subscriber groups. This association can be characterized by:

- Subscriber group date and time

This implies subscription to the service offering only during a specific period.

- Subscriber group priority



The priority is used as criteria to decide which service offering to apply in case of conflict between different service offerings data. The SAPC considers that conflict can happen for the policy controls whose service offerings data is defined in the qualification data (for example Bearer QoS control, Charging control) and Fair Usage

Also, the SAPC supports dynamic selection of the statically associated groups, by using **Group Selection policies**, including operator configured conditions (see Section 2.3 on page 13).

The following figure shows an example in which a subscriber is subscribed to three service offerings with different priorities that overlap in time. The SAPC applies to the subscriber the active subscriber group data with higher priority along the IP session lifetime:

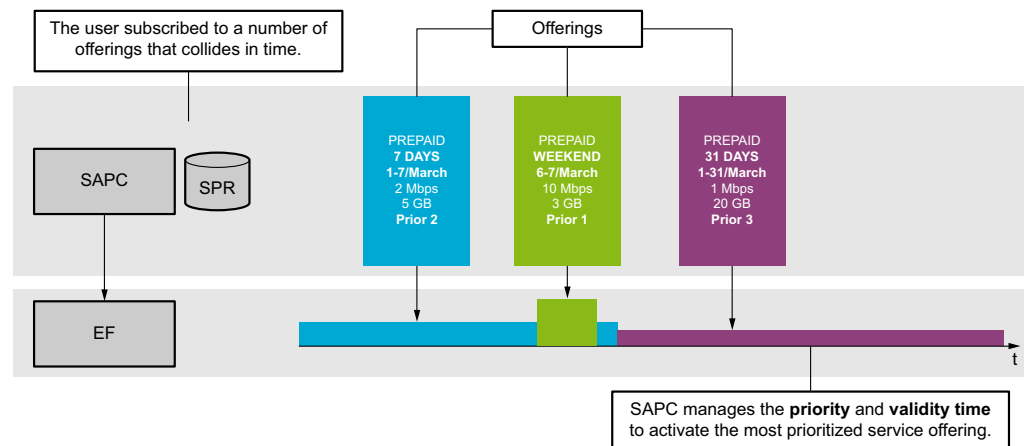


Figure 4 Multiple Service Offerings

2.2.1 Temporary Subscriber Groups

The SAPC enables subscribers to subscribe temporarily to a subscriber group, so the subscriber group data (static and dynamic) can be applied to the subscriber only when current time is between the provisioned start and end date. If the current date is not between start and end date, the subscriber group is inactive for the subscriber. Therefore, neither its static nor dynamic data are considered.

The SAPC also enables subscribers to subscribe multiple times to a subscriber group. For more information, see Stackable Dataplan in [Fair Usage Control](#). If the current date is not between any set of start and end date contained in the durations provisioned in the subscriber group association, the subscriber group is inactive for the subscriber.

If there is no date associated with the subscriber in the group subscription, it is considered that such group subscription can be applied without time restrictions. If only the end date is provisioned, then the subscriber group can be applied from

current date until the end date. If only the start date is provisioned, the subscriber group can be applied from the start date to unlimited date.

In addition to the temporary subscription through static data (provisioned start and/or end date), the SAPC supports dynamic selection of the subscribed groups, by using **Group Selection policies** including time of day policies (see Section 2.3 on page 13).

In PCC deployment, it is possible to receive the UE time zone offset from the Enforcement Function. If the SAPC is configured to accept it, the time used when the date or time of the subscriber group is evaluated is corrected with this offset. When time zone information is not received, or the SAPC is not configured to accept it, the SAPC uses its local time.

The following figure shows an example of a subscriber that belongs to two groups with different priority and the subscription to one of the groups is temporary:

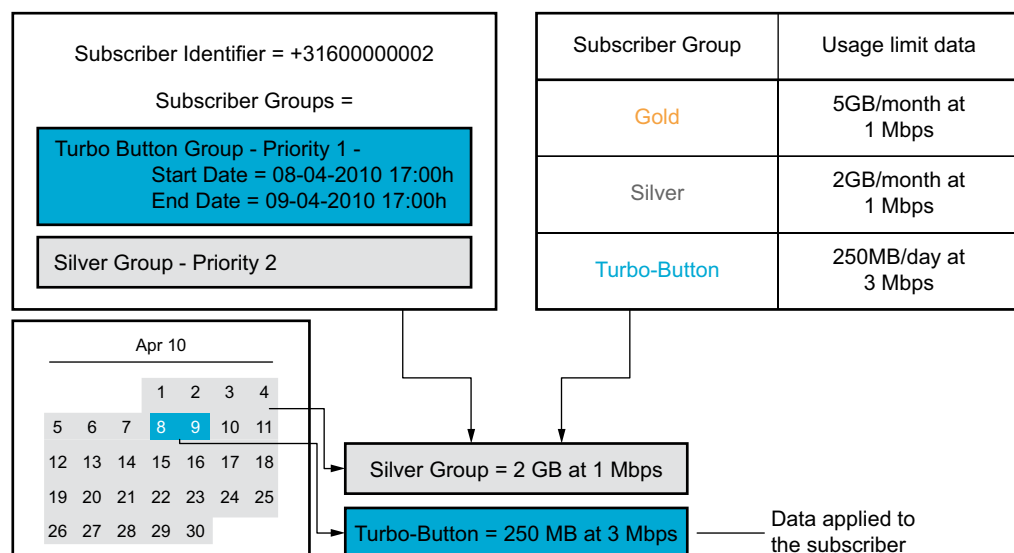


Figure 5 Example of Usage of Priority and Start/End Date for Subscriber Groups

In the example, data associated with the Turbo Button group is only applied from 8th of April at 17:00 to 9th of April to 17:00. Silver group data that has lower priority is applied the rest of the time.

The SAPC initiates a reauthorization towards the Enforcement Function when a subscriber group becomes active, and another reauthorization when the subscriber groups become inactive (see Section 3.3 on page 29).

See Section 2.5 on page 21 for more information about Time Trigger mechanism provided by the SAPC.



2.2.2 Handling of Subscriber Group Priority

It is possible to specify a priority per subscriber group to which the subscriber belongs. This priority specified is used as criteria to solve possible conflicts among the data of the different subscriber groups.

This priority can be specified at:

- Subscriber level.
- Subscriber group level, applicable for all the subscribers of the group. The SAPC considers it only when no priority is provisioned at subscriber level.

Subscriber groups without an assigned priority have the lowest priority.

The following figure shows an example of a subscriber that belongs to two groups with different priority whose data is in conflict:

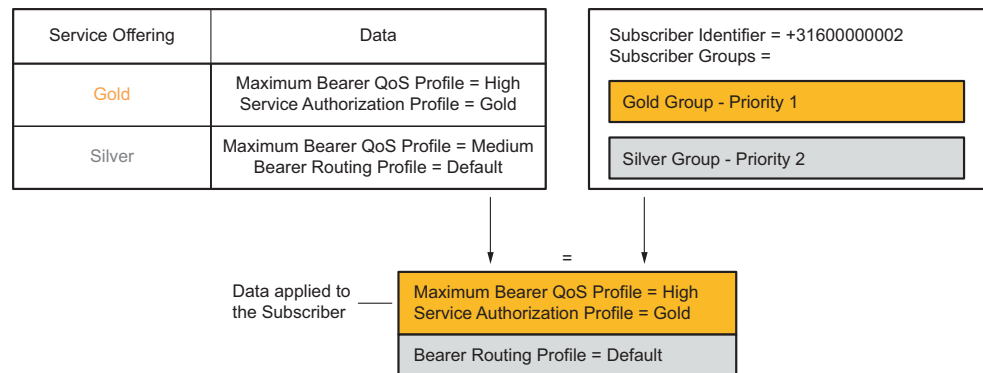


Figure 6 Example of Usage of Priority for Subscriber Groups

2.3 Dynamic Group Selection Policies

In addition to the association of a subscriber with a subscriber group, the SAPC supports dynamic selection of subscriber groups. Dynamic selection of subscriber groups is performed using group selection policies including operator configured conditions based on dynamic access information, accumulated usage, time and date conditions, and so on.

These policies are evaluated in the SAPC only for the list of groups associated with the subscriber, and when the current date is between the start date and the end date.

The evaluation of the previous policies results in the set of active subscriber groups, that is, the groups applicable to the subscriber. If no dynamic group selection policies are configured, the active subscriber groups are the associated with the subscriber, but in case of temporary subscriber groups, only if current date is between start and end date.

They can be defined globally or at subscriber level, but global level is recommended unless some authorization condition is required for a specific subscriber. Subscriber associated policies prevail over Global policies.

The following figure shows an example of a subscriber that belongs to two groups with different priority and the applicability of one of the groups depends both on static time conditions but also on dynamic access conditions:

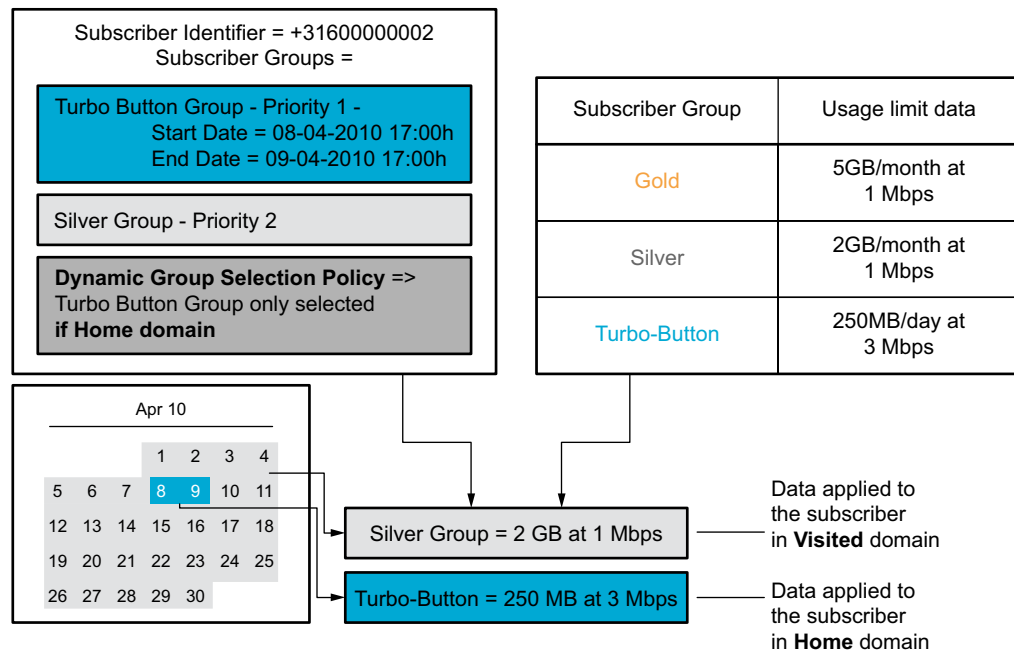


Figure 7 Example of Dynamic Group Selection Policies

In the example, data associated to Turbo Button group are only applied from 8th of April at 17:00 to 9th of April to 17:00 and if the user is in Home domain. Silver group data, has lower priority, are applied the rest of the time in case of Home domain and always when the user is roaming (Visited domain).

2.4 Policy Management

Policy management allows an operator to provide **dynamic data** to subscribers. Dynamic data is data that depends on certain conditions being fulfilled.

This model is based on XACML (Extensible Access Control Mark up Language).

The following subsections describe:

- How the SAPC selects suitable policies for a particular decision request
- The language that can be used in policies
- How policies are evaluated to provide dynamic data to the subscribers



- How policies based on time of day and date conditions are used

2.4.1 Selecting Applicable Policies

The operator has to specify a policy target when defining a policy in the SAPC. A policy target is the way to associate a requested resource with an applicable policy. The mapping between generic policy target attributes and the concepts that the SAPC handles is as follows:

- Subject, which is an actor whose attributes can be referenced by a condition. For example, a subject is mapped to a subscriber or subscriber group.
- Resource, which is data, service, or system component. For example, a resource can be an IP-CAN session for which an operation (for example, IP-CAN session creation/modification) is received or a service for which authorization is requested.
- Context, which is the environment to which the policy applies for. For example, Access or QoS.

The policies that are evaluated for a specific decision request are located from the whole set of policies defined in the SAPC, according to the policy target.

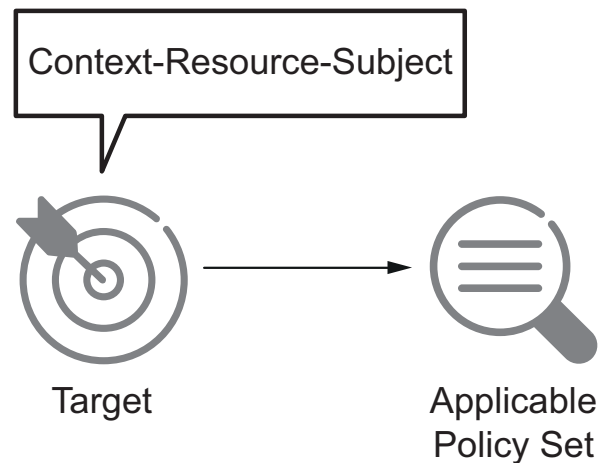


Figure 8 Locating Policies Target

When policies are defined in the SAPC, they can be assigned as follows:

- Globally to Resources (using so called global policy locators)
- For a Resource and Subject Group (using so called subject group policy locators)
- For a Resource and a Subject (using so called subject policy locators)

The next figure shows the links between Policies, Resources, and Subjects when policies are defined:

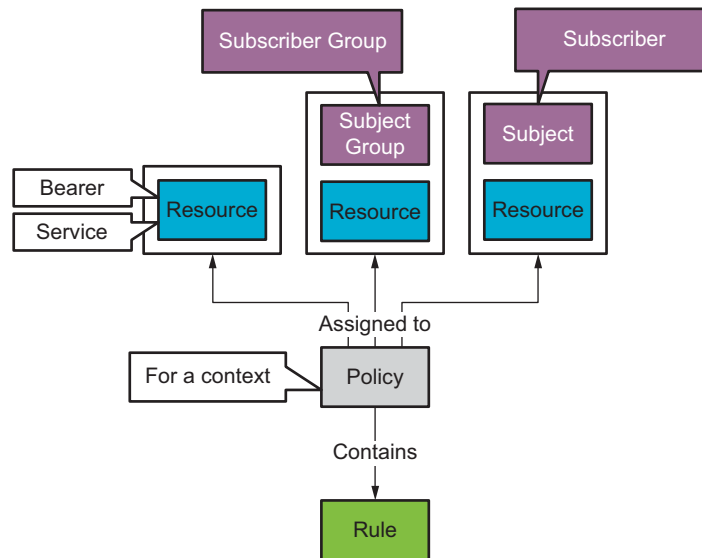


Figure 9 Policy Assignment for Context, Subject and Resource

When the SAPC receives a decision request, the SAPC performs a lookup on the SAPC policy repository selecting the following:

- The policies associated with the subscriber included in the request message, and
- The policies associated with the active groups to which the subscriber belongs, and
- The global policies for the applicable resources.

2.4.2 Language Used in Policies

The SAPC allows the operators to build the conditions to fulfill using:

- Formula operators, such as +, -, *, that allow combinations of different expressions.
- Expressions with tags (name representing a concept), time and date, and so on.
- Functions, such as included in a specified range, contains, and so on.



2.4.3 Policy Evaluation Process

To provide dynamic data to the subscribers, the SAPC evaluates the **business rules** contained in the applicable policies, by determining if the defined boolean conditions are fulfilled or not.

If the conditions are fulfilled, the associated data is assigned to the subscriber, such as bandwidth limitation, bearer QoS, authorized services.

Note: A condition always evaluates to false when the condition data to evaluate does not exist.

The time during the result is valid is also calculated (in case date and time conditions are configured), see Section 2.4.4 on page 20.

The following figure explains how the process evaluation is done in the SAPC once the applicable policies have been selected.

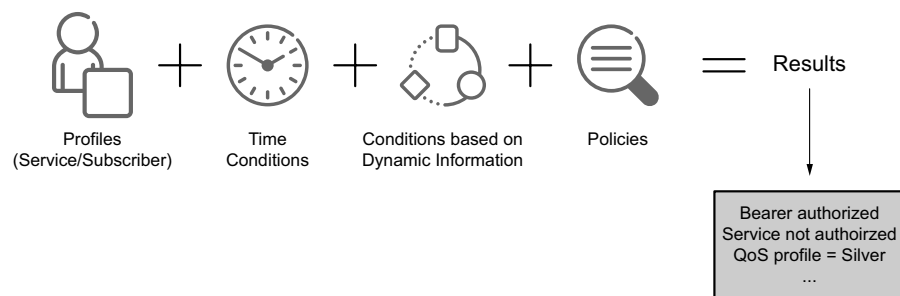


Figure 10 The SAPC Policy Evaluation

2.4.3.1 Data Used for Policy Evaluation

For policy evaluation, the SAPC can use the following set of data:

- Subscriber data: This information could be the subscriber category, subscriber age, and other operator-specific subscriber information. This information can be stored in the SAPC internal repository or in external SPRs.
- Time conditions such as current time and date when the policy evaluation is requested.
- Dynamic information such as usage information or information regarding the access network to which the subscriber is connected. This data is available from the incoming traffic messages. Examples of such data are the subscriber identity, the negotiated quality of service, the access type, subscriber location information (for example to determine if the subscriber is roaming), and subscriber equipment information.



2.4.3.2 Selection of Data to Apply to the Subscriber

The SAPC selects the data to be applied to a subscriber for those policy controls using both conditional (policies) and unconditional (static) qualification data (for example bearer QoS control) by applying the following mechanism:

- 1 Policies configured at subscriber level are evaluated.
- 2 If no result is obtained from the previous step, the SAPC gets the data unconditionally provisioned to the subscriber (such as static qualification data of Subscriber profile).
- 3 If no result is obtained from the previous step, policies configured for the active subscriber groups with the highest priority to which the subscriber belongs to are evaluated.

If there are several active subscriber groups with the same priority, and there are not Dynamic Group Selection policies configured to select only one of them, the subscriber group selected by the SAPC is unpredictable.

- 4 If no result is obtained from the previous step, the SAPC gets the data unconditionally provisioned (static profile) to the active subscriber group with the highest priority.

If there are several active subscriber groups with the same priority, and there are not Dynamic Group Selection policies configured to select only one of them, the subscriber group selected by the SAPC is unpredictable.

- 5 If no result is obtained from previous step, steps 3 and 4 are repeated for all active subscriber groups to which the subscriber belongs from highest to lowest priority (ending with Global Subscriber group), until a result is obtained.
- 6 If no result is obtained from the previous step, global policies are evaluated.

The SAPC selects the data to be applied to a subscriber for those policy controls not using unconditional qualification data (for example, Fair Usage control) applying the following mechanism:

- 1 If the same data is configured at subscriber and subscriber group level with different value, the value provisioned at subscriber level is selected.
- 2 If the same data is configured for several active subscriber groups with different value, the value associated with the active subscriber group with higher priority is selected for the subscriber.

If the same data with different value is configured for several subscriber groups having the same priority, then any group data is selected.

- 3 When there is no conflict between the different subscriber and subscriber groups data, all the data of each active subscriber group that the subscriber belongs to are selected.



- 4 Policies are evaluated for the selected data according to the following precedence allocation and applying permit overrides algorithm among them (if the policy evaluates to true, the result is true):

- a Subject policy locator
- b 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.

- c Global policy locator.

Note: For complete information about how data is selected for each policy control that the SAPC handles, see the corresponding Functional Description associated with such control.

2.4.3.3

Solving Policies Conflicts

A combining resolution mechanism is required because multiple policies can be applicable to a decision request, and because a single policy can contain multiple rules. The policies and the rules are always evaluated in order according to their configured Policy Order and Rule Order values. When several policies are evaluated, there are two working modes:

- Single result evaluation, where only one result for a resource is allowed (for example, bearer QoS, authorized service, charging profile). In this case, conflicting results can be obtained for the same resource (that is, one rule can say that the conditions for the resource evaluate to true and another rule say that the conditions for the resource evaluate to false). These conflicts are solved using the configured combination algorithms:

Rules combining algorithm

If conflicts arise between the results of rules belonging to the same policy, the algorithm configured in the policy solves the conflict. The possible algorithms are the following:

- Permit overrides: Evaluates the rules belonging to the policy in order starting with the rule with lower Rule Order value (higher priority) until any rule evaluates to true, then the result is true. Otherwise the result is false.
- Deny overrides: Evaluates the rules belonging to the policy in order starting with the rule with lower Rule Order value (higher priority) until any rule evaluates to false, then the result is false. Otherwise the result is true.

Policies combining algorithm

If conflicts arise between the results of policies belonging to the same policy locator, permit overrides algorithm always applies among them. The SAPC

evaluates the policies belonging to the same policy locator in order starting with the policy with lower Policy Order value until any policy evaluates to true. Then, the result is true, otherwise the result is false.

- Multiple result evaluation, where several results for a resource are allowed (for example, end-user notifications): The results of all rules within all the selected policies that evaluate to true are returned. In this case, the All permit algorithm is used.

2.4.4 Policies Based on Time of Day Conditions

The SAPC policies can evaluate conditions based on date and time. The SAPC obtains an internal validity (number of seconds) that is the minimum time and date conditions configured among all the evaluated rules, allowing the SAPC to detect the moment the policies should be evaluated again.

If a policy is composed of several rules, the SAPC considers the minimum validity value between all the time and date conditions evaluated in the rules.

Note: It is possible to receive the UE time zone offset from the Enforcement Function. If the UE time zone offset is used and the SAPC is configured to accept this time zone, the time used when these time conditions are evaluated is corrected with this offset. When the time zone information is not received, or the SAPC is not configured to accept it, only local time is used.

In case the time condition evaluation result changes during the IP session lifetime, the SAPC is able to provide the new information result to the Enforcement Function (for example, PCEF). The SAPC can provide the new information result to Enforcement function with:

- Triggering a reauthorization request message towards the Enforcement functions, at the moment the date or time condition is reached, to inform it about the new result.

This allows SAPC to provide time triggered policies to different controls such as Bearer QoS control, Bandwidth control, Service Access Control, Content Filtering .

- Sending a reauthorization request message after policy re-evaluation at the reception of the first interim message received once after the date or time condition is reached. This behavior applies only for DHCP/CLIPs
- Providing to the Enforcement functions in the authorization answer message the time at which it shall request reauthorization again since the answer provided should change then.

This method applies for Access Control policies.

See Section 2.5 on page 21 for more information about Time Trigger mechanism provided by the SAPC.



Note: For complete information about the policy controls that can evaluate conditions based on date and time, refer to the corresponding Functional Description associated with such control.

2.5 Reauthorization Because of Time of Day Conditions

Reauthorization because of time and date conditions allows the SAPC to provide:

- Temporary subscriber groups (see Section 2.2.1 on page 11)

Validity time is the time at which the temporary group becomes active or inactive.

- Policies with time conditions (see Section 2.4.4 on page 20)

Validity time is the time at which policy evaluation result changes.

The SAPC provides mechanisms to avoid massive sending of reauthorization messages due to Time Conditions, refer to [Overload Control](#) for more information.

2.6 Header Enrichment

The SAPC is able to send user-related information to be entered in the HTTP headers of a particular request to GGSN/PDN-GW so that the service can use this information in its internal logic. One typical application is to provide the third-party applications with a user alias so the MSISDN is not disclosed to third-party applications.

The SAPC allows the operator to define any alphanumeric string to be inserted in the HTTP header of a request, on a per subscriber or per subscriber group basis. It is sent towards GGSN/PDN-GW using Customer-Id AVP.





3 Subscription and Policy Management Traffic Cases

3.1 Update Subscriber Profile

The SAPC provides a REST interface for provisioning subscriber and subscriber group data in the internal repository. When the subscriber data is stored in an external database, the SAPC provides a Web Service interface to receive notifications about subscriber data updates.

This traffic case shows how the SAPC provides new data towards the Enforcement Function upon a subscription change that affects a single subscriber. Changes in Subscriber Group data do not trigger a reauthorization request. Changes in special subscriber profiles such as “Subscriber Unknown” do not trigger reauthorization requests.

Only the significant attributes for this traffic case are described in the following subchapters, for a detailed description of each of the interfaces supported it shall be consulted the corresponding interface description.

Update Subscriber data

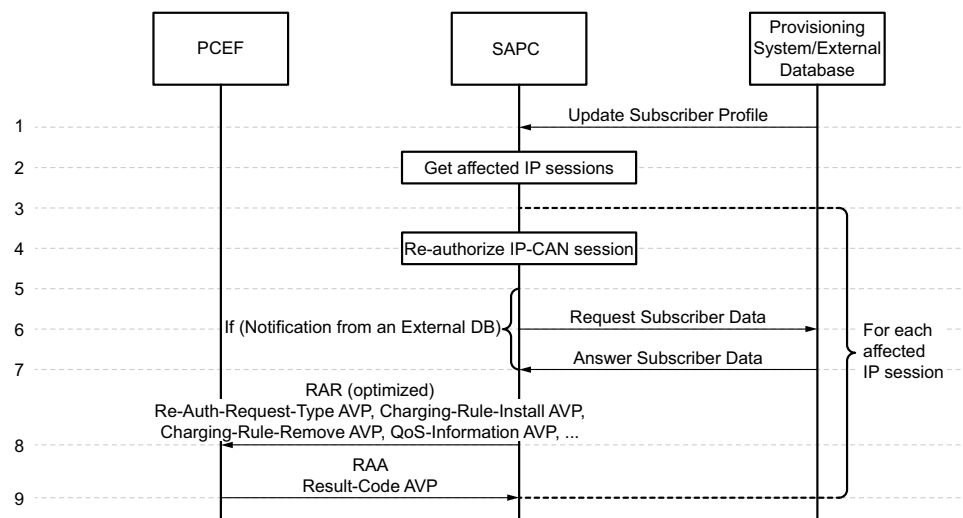


Figure 11 Update Subscriber Data using Rel9 Gx/Gx+ onwards

- 1: In the case of using the SAPC internal repository, the Provisioning System updates the data under the Subscriber profile using the REST interface. In the case of using an external database, the database notifies changes in the Subscriber profile through SOAP. In the latter case, the external database notification includes the identity of the affected subscriber.



- 2: The SAPC looks for the subscriber and related IP-CAN sessions.
- 3–8 For each affected IP-CAN session, the SAPC executes a session reauthorization process:
 - 5-7: In the case of a notification received from an external database through the Web Service interface,
 - 5: if the SAPC found a session for the subscriber, the SAPC requests the data to the external database through LDAP.
 - 6: The SAPC receives the response from the external database through LDAP
 - 8: The SAPC performs the reauthorization executing the controls enabled for the affected PCEF and a RAR is sent to PCEF with only the new/modified information and the Re-Auth-Request-Type AVP set to AUTHORIZE_ONLY.
Note: A RAR message is sent to the PCEF including Session-Release-Cause AVP set to UE_SUBSCRIPTION_REASON when:
 - the provisioning order or Web Service notification indicated the removal of a subscriber, or
 - the IP-CAN Session Access Control is enabled and the result is the non-authorization of the IP-CAN session.
 - 9: RAA including Result-Code is returned by the PCEF.
Note: If the RAA is the response to the RAR message sent indicating Session-Release-Cause AVP set to UE_SUBSCRIPTION_REASON, then the flow would continue and finish as follows:
 - 10: The SAPC receives a CCR Termination requesting IP-CAN session termination
 - 11: The SAPC removes the IP-CAN session and sends a CCA message to the PCEF including the Result-Code AVP with value DIAMETER_SUCCESS.

3.2 Remove Subscriber Profile

This section describes the traffic cases of the subscriber profile removal.



3.2.1

Remove Subscriber Profile using standard Rel9 Gx/Gx+ onwards

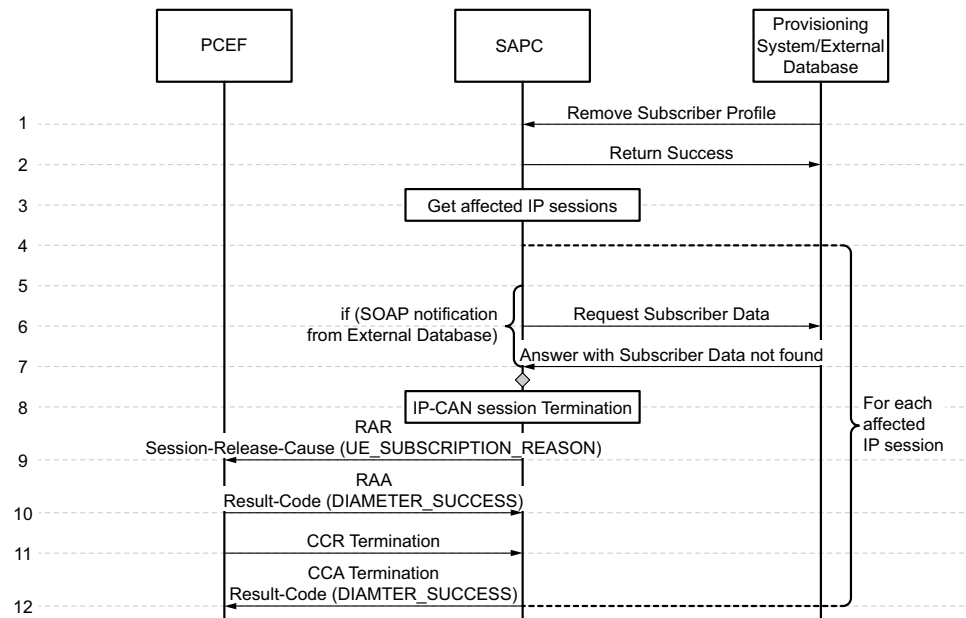


Figure 12 Remove Subscriber Profile

- 1: In the case of using the SAPC internal repository, the Provisioning System removes the Subscriber profile through REST interface. In the case of using an external repository, the database notifies removals of the Subscriber profile through SOAP.
- 2: The SAPC returns a success response (HTTP 200 OK in the case of SOAP or 204 (No Content) in the case of REST).
- 3: The SAPC looks for the IP-CAN sessions related to the subscriber.
- 4–12 For each affected IP-CAN session, the SAPC executes a session reauthorization process:
 - 5–7: In the case of a SOAP notification received from an external database:
 - 6: The SAPC requests the data to the external database through LDAP.
 - 7: The SAPC receives the LDAP response noSuchObject (32).
 - 8: The SAPC decides to terminate the IP-CAN session..
 - 9: The SAPC sends a RAR message to the PCEF including Session-Release-Cause AVP set to UE_SUBSCRIPTION_REASON.
 - 10: RAA including Result-Code AVP with value DIAMETER_SUCCESS is returned by the PCEF.

- 11: The SAPC receives a CCR Termination requesting IP-CAN session termination.
- 12: The SAPC removes the IP-CAN session and sends a CCA message to the PCEF including the Result-Code AVP with value DIAMETER_SUCCESS.

3.2.2

Subscriber Profile defined in Ericsson OCS and SAPC. Remove Subscriber Profile only from SAPC

The following traffic case occurs when the subscriber profile is defined in the SAPC and the policy groups information is also received from Ericsson Online Charging System. It is only applicable with the Ericsson Sy session.

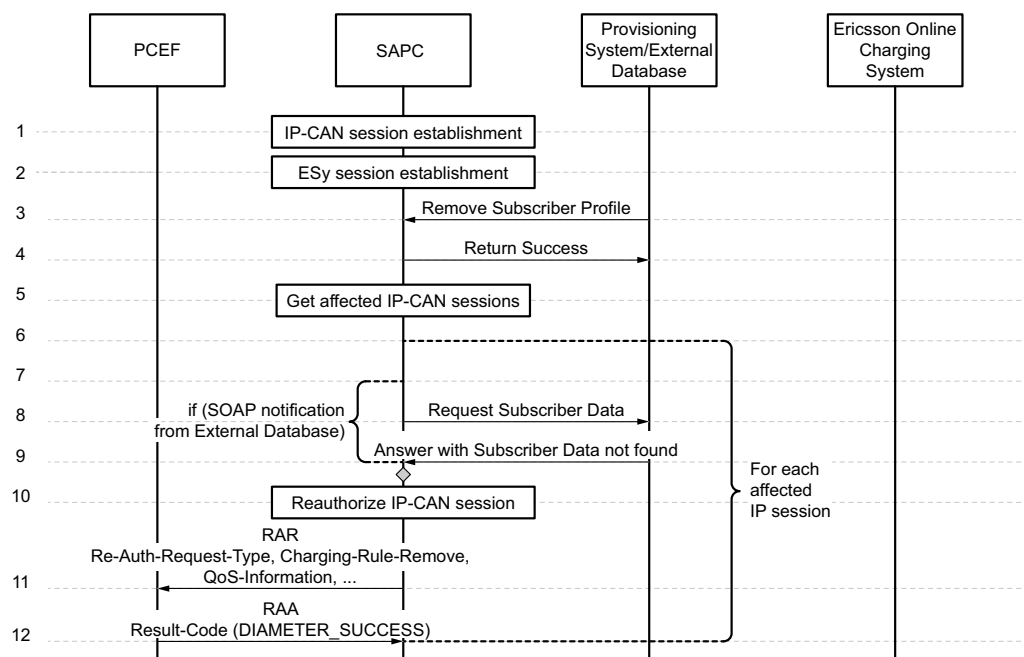


Figure 13 Remove Subscriber Profile in SAPC, still consider the Policy Groups from OCS

- 1-2: The precondition for this traffic case is that an Ericsson Sy session is associated to the active IP-CAN session and the Policy Counters and Policy Groups are already available in the SAPC. See [Integration with OCS for Monetary Spending Limit Reporting \(Sy\)](#) for further details.
- 3 In the case of using the SAPC internal repository, the Provisioning System removes the Subscriber profile through REST interface. In the case of using an external repository, the database notifies removals of the Subscriber profile through SOAP.
- 4: The SAPC returns a success response (HTTP 200 OK in the case of SOAP or 204 (No Content) in the case of REST).



- 5: The SAPC looks for the IP-CAN sessions related to the subscriber.
- 6–12 For each affected IP-CAN session, the SAPC executes a session reauthorization process:
 - 7-9: In the case of a SOAP notification received from an external database:
 - 8: The SAPC requests the data to the external database through LDAP.
 - 9: The SAPC receives the LDAP response `noSuchObject` (32).
 - 10: The SAPC reauthorizes the IP-CAN session. All applicable controls are reevaluated only considering the policy groups stored in the ESy session.
 - 11: The SAPC sends a RAR message to the PCEF, with only the new/modified information and with `Re-Auth-Request-Type` AVP set to `AUTHORIZE_ONLY`.
 - 12: RAA including `Result-Code` AVP with value `DIAMETER_SUCCESS` is returned by the PCEF.

3.2.3 Disabled massive reauthorizations

To prevent the network overload in case of massive subscriber profile removals, the attribute `enableReauthsOnSubsChange` in class `class AppConfig` is set to `false`. The RAR messages to terminate each IP-CAN session (see Section 3.2.1 on page 24 for details) are not sent to the PCEF and the SAPC removes the IP-CAN session at reception of next message from PCEF or SAPC-initiated reauthorization over the IP-CAN session. The following figure shows the SAPC behavior.

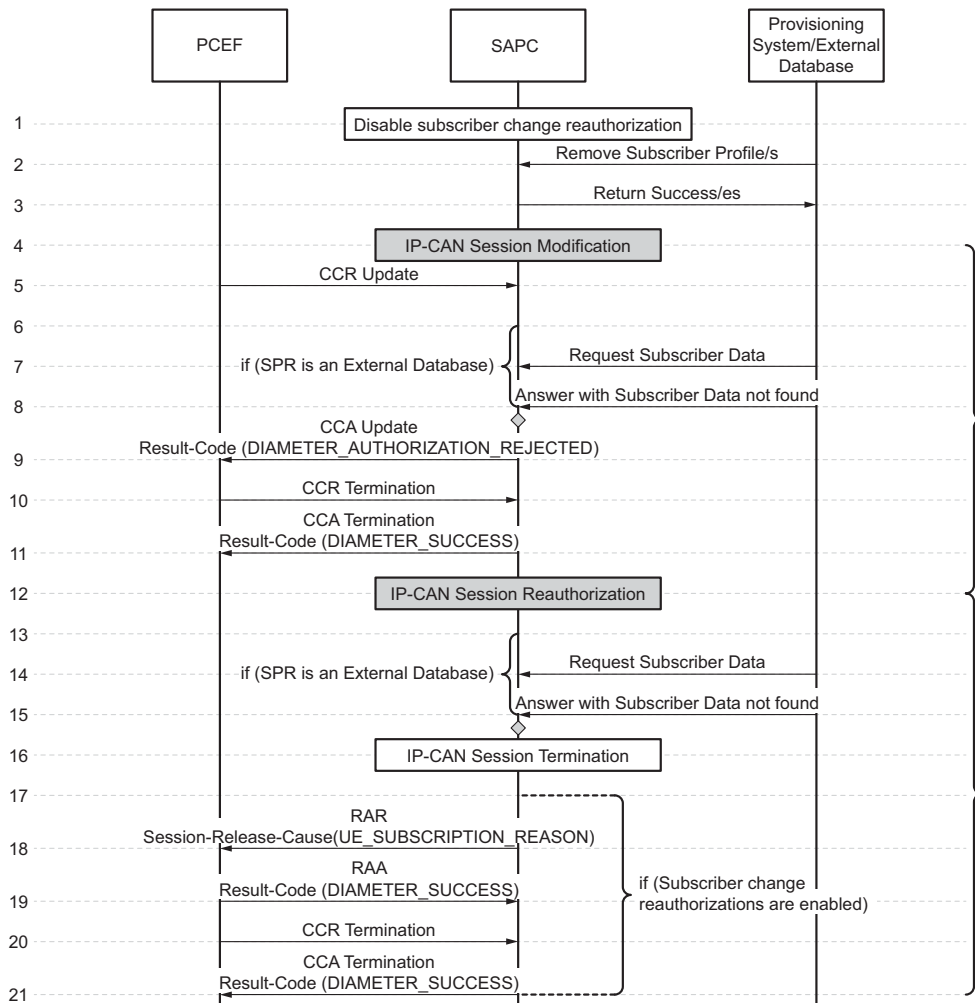


Figure 14 Remove Subscriber Profile when the massive reauthorizations are disabled.

- 1: The attribute enableReauthsOnSubsChange in class class AppConfig is set to false
- 2: The Subscriber Profiles are removed.
- 3: The SAPC returns a success response (HTTP 200 OK in the case of SOAP or 204 (No Content) in the case of REST). No RAR Termination messages are sent to the PCEF.
- 4-11: This use case represents the SAPC behavior on an IP-CAN Session modification request:
 - 5: The SAPC receives a CCR Update message from the PCEF indicating IP-CAN session modification.
 - 6-8: If the SPR is an external database:



- 7: The SAPC requests the data to the external database through LDAP.
- 8: The SAPC receives the LDAP response `noSuchObject` (32).
- 9: The SAPC identifies the IP-CAN session with one pending to be terminated. The Result-Code `DIAMETER_AUTHORIZATION_REJECTED` (5003) is used to indicate that the IP-CAN session is to be deactivated.
- 10: The SAPC receives a CCR Termination requesting IP-CAN session termination.
- 11: The SAPC removes the IP-CAN session and sends a CCA message to the PCEF including the Result-Code AVP with value `DIAMETER_SUCCESS`.
- 12-21: This use case represents the SAPC behavior on an IP-CAN Session reauthorization (for example due to time of day policies):
 - 13-15: If the SPR is an external database:
 - 14: The SAPC requests the data to the external database through LDAP.
 - 15: The SAPC receives the LDAP response `noSuchObject` (32).
 - 16: The SAPC identifies that the IP-CAN session is pending to be terminated. It sends a RAR message to the PCEF including Session-Release-Cause AVP set to `UE_SUBSCRIPTION_REASON`.
 - 17-21: If eventually, the attribute `enableReauthsOnSubsChange` is set again to `true`, to allow the sending of RAR messages to the PCEF:
 - 18: The SAPC sends a RAR message to the PCEF including Session-Release-Cause AVP set to `UE_SUBSCRIPTION_REASON`.
 - 19: RAA including Result-Code AVP with value `DIAMETER_SUCCESS` is returned by the PCEF.
 - 20: The SAPC receives a CCR Termination requesting IP-CAN session termination.
 - 21: The SAPC removes the IP-CAN session and sends a CCA message to the PCEF including the Result-Code AVP with value `DIAMETER_SUCCESS`.

3.2.4 Emergency Services

When the subscriber profile is removed but there is an associated emergency IP-CAN session (see [Emergency and Multimedia Priority Services](#)), the SAPC does not request to the PCEF the IP-CAN session termination.

3.3 Subscriber Group activation/deactivation Because of Time Conditions

This Traffic case shows how the SAPC requests a session reauthorization when a new subscriber group should become active during the IP-CAN session lifetime.

3.3.1 Subscriber Group activation/deactivation Because of Temporary Subscription using Rel9 Gx/Gx+ onwards.

In this traffic case it is considered a subscriber that is subscribed to two subscriber groups:

- Gold group, priority 0, from start-date 01-02-2010T20:00 to end-date 01-02-2010T22:00
- Normal group, priority 1

Priority 0 means higher priority than 1

Normal group does not include in its definition a start-date or an end-date, meaning that it is valid from the moment the subscription is created until the subscription is removed.

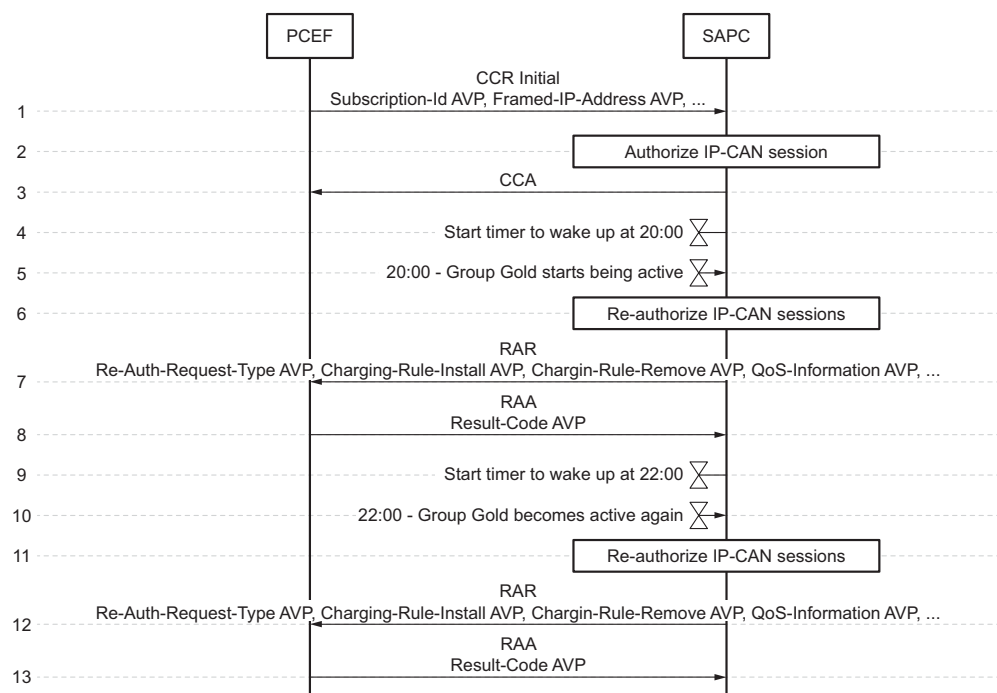


Figure 15 Subscriber group activation/deactivation Because of Time conditions in PCC deployment



1. At any time before 20:00, the SAPC receives a Gx CCR-initial message from the PCEF indicating IP session establishment.

The SAPC looks for the subscriber and subscriber group data. Since it is not between 20:00 and 22:00, subscriber group "Normal" is chosen.
2. The SAPC authorizes the IP session: it looks in the configuration data for the controls applicable for the requesting PCEF, decides the proprietary capabilities to be applied towards the PCEF and performs the applicable controls.
3. The information obtained in the previous steps is included in the CCA answer message.
4. In the example, the evaluation process detects that at 20:00 a re-evaluation shall be performed since Gold Group becomes active then; so the application sets up a timer
5. At 20:00, the SAPC automatically detects that the Time of Day condition to change to the subscriber group with higher priority is reached (20:00), then the traffic case continues as if any user profile data is updated according to the protocol binding described in Section 3.1 on page 23:
6. The SAPC looks for the subscriber and related IP sessions and for each affected IP session, the SAPC executes a session reauthorization process.
7. RAR is sent to the PCEF per affected IP-CAN session.
8. RAA including Result-Code is returned by the PCEF.
9. In the example, the evaluation process detects that at 22:00 a re-evaluation shall be performed since Gold Group becomes inactive again and Normal becomes active; so the application sets up a timer.
10. When 22:00 p.m. is reached, traffic case continues as if any user profile data is updated according to the protocol binding described in Section 3.1 on page 23.

3.3.2

Subscriber Group activation/deactivation Because of Static and Dynamic conditions using standard Rel9 Gx onwards or Ericsson Rel9 Gx+ onwards.

In this traffic case it is considered two subscribers associated to two subscriber groups:

- Gold group, priority 0, from start-date 01-03-2012 to end-date 01-03-2013
- Normal group, priority 1

Priority 0 means higher priority than 1

Also, Dynamic Group Selection policies are defined for Gold group:

- Gold group is only selected in Home domain, for all subscribers (Global Dynamic Group Selection policy).
- Gold Group is selected, for Subscriber_A, from 20:00 to 22:00 p.m. (Subscriber Dynamic Group Selection policy).

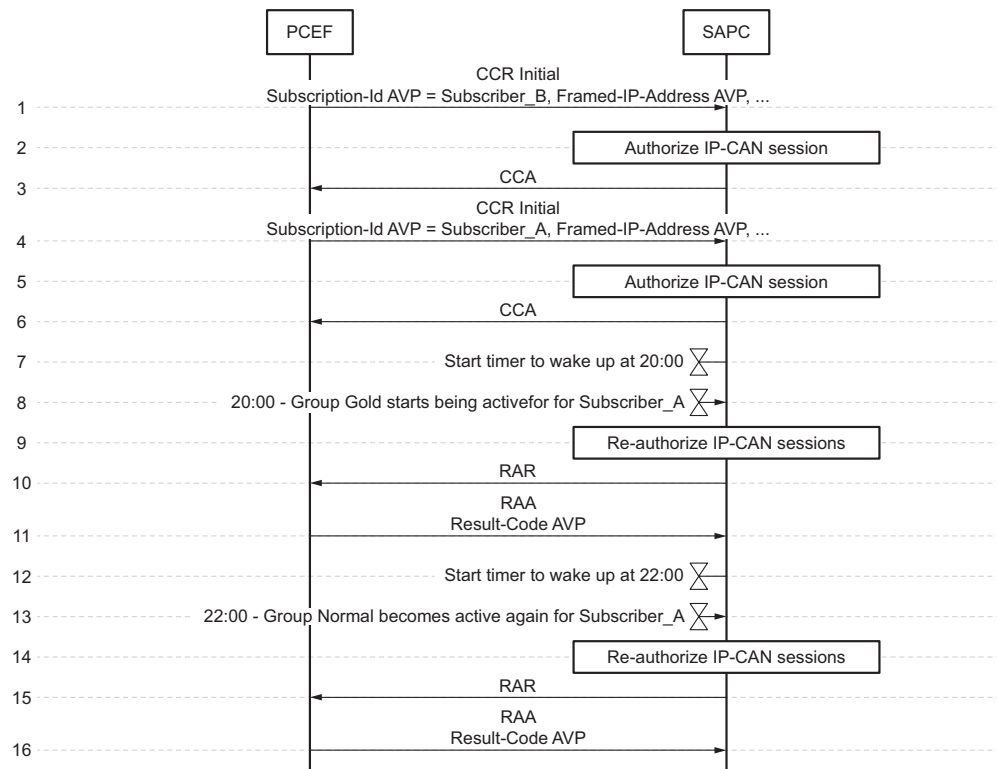


Figure 16 Subscriber group activation/deactivation Because of Static and Dynamic conditions in PCC deployment

1. The SAPC receives a Gx CCR-initial message from the PCEF indicating IP session establishment for Subscriber_B, indicating roaming (Visited domain).

The SAPC looks for the subscriber and subscriber group data. Since it is between 01-03-2012 and 01-03-2013 and the subscriber is roaming, subscriber group "Normal" is chosen.

2. The SAPC authorizes the IP session: it looks in the configuration data for the controls applicable for the requesting PCEF, decides the proprietary capabilities to be applied towards the PCEF and performs the applicable controls.
3. The information obtained in the previous steps is included in the CCA answer message.
4. The SAPC receives a Gx CCR-initial message from the PCEF indicating IP session establishment for Subscriber_A, indicating Home domain.



The SAPC looks for the subscriber and subscriber group data. Since it is between 01-03-2012 and 01-03-2013 but Time of Day is not between 20:00 and 22:00, although the subscriber is not roaming (Home domain), subscriber group "Normal" is chosen.

5. The SAPC authorizes the IP session: it looks in the configuration data for the controls applicable for the requesting PCEF, decides the proprietary capabilities to be applied towards the PCEF and performs the applicable controls.
6. The information obtained in the previous steps is included in the CCA answer message.
7. In the example, the evaluation process detects that at 20:00 a re-evaluation shall be performed, so the application sets up a timer
8. At 20:00, the SAPC automatically detects that the Time of Day condition to change to the subscriber group with higher priority is reached (20:00), then the traffic case continues as if any user profile data is updated according to the protocol binding described in Section 3.1 on page 23.

Gold Group becomes active for Subscriber_A, while for Subscriber_B Normal Group remains active.

9. The SAPC looks for the subscriber and related IP sessions and for each affected IP session, the SAPC executes a session reauthorization process, for Subscriber_A.
10. RAR is sent to the PCEF per affected IP session.
11. RAA including Result-Code is returned by the PCEF.
12. In the example, the evaluation process detects that at 22:00 a re-evaluation shall be performed since there are time-based policies associated to Gold Group; so the application sets up a timer.
13. When 22:00 p.m. is reached, traffic case continues as if any user profile data is updated according to the protocol binding described in Section 3.1 on page 23.

Normal Group becomes active for Subscriber_A (Gold Group becomes inactive). Gold Group continues inactive for Subscriber_B because of roaming reasons.

3.4 Policy Result Change Because of Time Conditions

This Traffic case shows how the SAPC requests a reauthorization to the Enforcement Function when a policy with Time of Day conditions changes the result during the IP-CAN session lifetime.

It is considered a policy associated to a subscriber with the following Time of Day conditions:

- Bearer QoS profile = High, from 18:00 to 23:00 p.m.

— Bearer QoS profile = Low, from 23:00 to 18:00 p.m.

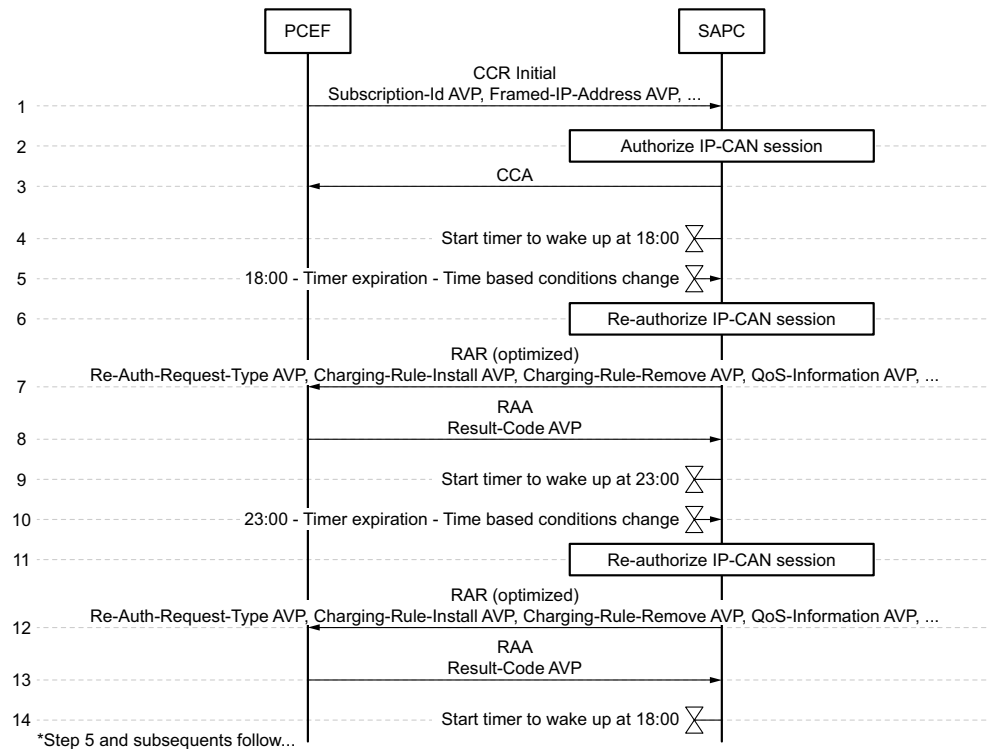


Figure 17 Policy result change Because of Time conditions in PCC deployment

1. The SAPC receives a Gx CCR-initial message from the PCEF indicating IP-CAN session establishment.
2. The SAPC authorizes the IP-CAN session: it looks in the configuration data for the controls applicable for the requesting the PCEF, decides the proprietary capabilities to be applied towards the PCEF and performs the applicable controls.

Since IP-CAN session is established at 17:00 p.m., Bearer QoS profile = Low is assigned

3. The information obtained in the previous step is included in the CCA answer message.
4. In the example, the evaluation process detects that at 18:00 a re-evaluation shall be performed since a time-based condition changes; so the application sets up a timer.
5. At 18:00, the timer expires
6. All the policies applicable to the PCEF are reevaluated. New Bearer QoS profile = High is assigned.



7. RAR message with modified information is sent to the PCEF.
8. RAA message is received from the PCEF.
9. In the example, the evaluation process detects that at 23:00 a re-evaluation shall be performed since a time-based condition changes; so the application sets up a timer.
10. At 23:00, the timer expires.
11. All the policies applicable to the PCEF are reevaluated. Bearer QoS profile = Low is assigned again
12. RAR message with modified information is sent to the PCEF.
13. RAA message is received from the PCEF.
14. In the example, the evaluation process detects that at 18:00 a re-evaluation shall be performed since a time-based condition changes; so the application sets up a timer.

Traffic case follows from step 5 onwards while the IP-CAN session is active.

3.5 Failure Handling

This section describes the Gx failures reported by the PCEF at the SAPC indication of IP session update because of Subscription Management or Time of Day Policies, or both.

Table 1 Error Handling

Gx Error Condition	Action
<p>After reauthorization because of Subscription Management or Time of Day Policies, the PCEF answers to the RAR sent by the SAPC with an RAA indicating either the user is not known in the PCEF or the session is not known in the PCEF</p> <p>Result-Code AVP:</p> <p>DIAMETER_USER_UNKNOWN</p> <p>DIAMETER_UNKNOWN_SESSION_ID</p>	<p>The SAPC deletes the affected Gx sessions</p> <p>When the Result-Code AVP indicates either DIAMETER_UNKNOWN_SESSION_ID or DIAMETER_USER_UNKNOWN, the SAPC deletes the session indicated in the request.</p>



Gx Error Condition	Action
<p>If a RAA message is received indicating the Diameter node is not reachable owing to request time-out or any error, as for exampleResult-Code AVP:</p> <p>DIAMETER_UNABLE_TO_DELIVER</p> <p>DIAMETER_TOO_BUSY</p> <p>DIAMETER_LOOP_DETECTED</p>	<p>The SAPC does not reattempt. The SAPC does not take any action and keeps the Gx session state generated by the subscription change or Time of Day event</p>
<p>RAA message is received with any other errors</p>	<p>The SAPC does not take any action and keeps Gx session state generated by the subscription change or Time of Day event.</p>



4 Restrictions

Because of Y2038 problem and NTP overflow, the SAPC does not support to handle dates beyond 6h 28m 16s UTC, 7 February 2036

Besides, Time of Day conditions are not applicable to the following Policies:

- Autoprovisioning
- End User Notifications
- Service QoS and Service Charging
- Online Charging System Selection





Reference List

- [1] Database Access
- [2] Emergency and Multimedia Priority Services
- [3] Integration with OCS for Monetary Spending Limit Reporting (Sy)
- [4] Overload Control