

Application Detection and Control based on ADC Rules (Sd)

Ericsson Service-Aware Policy Controller

Facility Description

Copyright

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

Disclaimer

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

Trademark List

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



Contents

1	Application Detection and Control Based on ADC Rules	1
	Introduction	1
1.1	Document Purpose and Scope	1
2	Application Detection and Control over Sd Function	2
2.1	TDF Overview	2
2.1.1	TDF Selection	2
2.1.1.1	Select TDF Conditionally	2
2.1.1.2	Select TDF Unconditionally	3
2.2	ADC over Sd Overview	3
2.3	Service Access Control in Sd	5
2.3.1	Service Selection	5
2.3.2	Service Authorization	5
2.3.3	Service Qualification	5
2.4	Application Detection Reporting	5
2.5	Dynamic Policy Control over Sd	7
2.5.1	Dynamic Policy Control over Sd Overview	7
2.5.2	Classification of Dynamic Services over Sd	8
2.5.3	Qualification of Dynamic Services over Sd	10
2.5.3.1	Allocation of QoS Information to Dynamic Services	11
2.5.3.2	Allocation of Charging Parameters to Dynamic Services	12
2.5.4	Dynamic PCC Rule Generation Based on Service Data Flow Received over Sd	12
2.6	IP-CAN Session Reauthorization	15
3	ADC Network Deployments over Sd	18
4	ADC Traffic Cases over the Sd Interface	19
4.1	Sd Session Life Cycle	19
4.1.1	Sd Session Establishment	19
4.1.2	Sd Session Modification	24
4.1.3	Sd Session Termination	26
4.2	QoS Control Based on Application Traffic Detection Upgrading Default Bearer	28
4.2.1	Session Establishment	28
4.2.2	Upgrade Default Bearer QoS at Application Start Detected	29
4.2.3	Downgrade Default Bearer QoS at Application Stop Detected	29
4.3	QoS Control Based on Application Traffic Detection Allocating Dedicated Bearer	30
4.3.1	Session Establishment	32



4.3.2	Download Dedicated Bearer at Application Start Detected	32
4.3.3	Remove Dedicated Bearer at Application Stop Detected	33
4.4	ADC over Sd Error Handling	33
4.4.1	Error Handling at Sd Session Establishment	33
4.4.2	Error Handling at Sd Session Modification	34
4.4.3	Error Handling at Sd Session Termination	34
4.4.4	Error Handling at Application Reporting	35
4.4.5	Error Handling at Dedicated Bearer Reported as Inactive by PCEF	36



1 Application Detection and Control Based on ADC Rules Introduction

1.1 Document Purpose and Scope

This document describes the Application Detection and Control (ADC) function provided by the SAPC over the Sd interface.

The Sd reference point is defined by 3GPP and is located between the Policy and Charging Rules Function (PCRF) and the Traffic Detection Function (TDF).



2 Application Detection and Control over Sd Function

2.1 TDF Overview

The TDF is a functional entity that performs application detection and enables the operator to have real-time and coordinated control over the services of the users. It is also responsible for the reporting of detected applications and describing their service data flow to the PCRF. The TDF detects the start and end of the respective service and notify the PCRF about it accordingly.

The TDF can be deployed in the network in the following ways:

- Collocated with the Policy and Charging Enforcement Function (PCEF) enhanced with ADC

The SAPC provides this solution over the Gx interface with Policy and Charging Control (PCC) rules. For more information, see [Application Detection and Control based on PCC rules \(Gx\)](#).

- Standalone

The SAPC provides this solution over the Sd interface with ADC rules. In this deployment, the SAPC and the PCEF must be coordinated so that the Sd session in the control plane and the subscriber data in the data plane go through the same TDF.

2.1.1 TDF Selection

A TDF selected to establish a new Sd session associated with the IP-CAN session can be received in the CCR-Initial message with the TDF-Information AVP. If the TDF-Information AVP is not provided, the SAPC selects the TDF based on the internal configuration.

Two different types of TDF selection can be provided:

- Select TDF conditionally (several TDFs per PCEF)
- Select TDF unconditionally (one TDF per PCEF)

2.1.1.1 Select TDF Conditionally

Multiple TDFs are handling the Sd sessions associated with the IP-CAN sessions established from a PGW. The SAPC selects a TDF associated with the PCEF based on the APN.

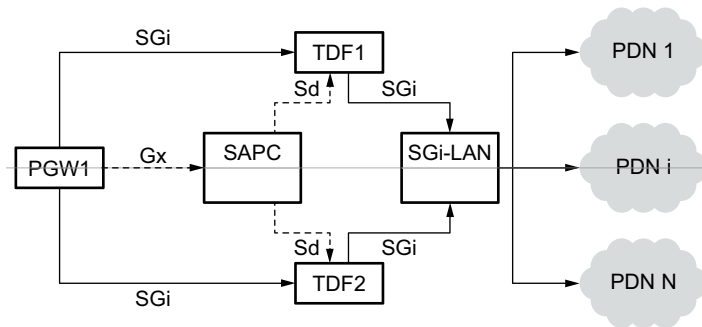


Figure 1 TDF Selection - Several TDFs per PCEF

2.1.1.2

Select TDF Unconditionally

One TDF is handling the Sd sessions associated with the IP-CAN sessions established from a PGW regardless the Access Point Name (APN).

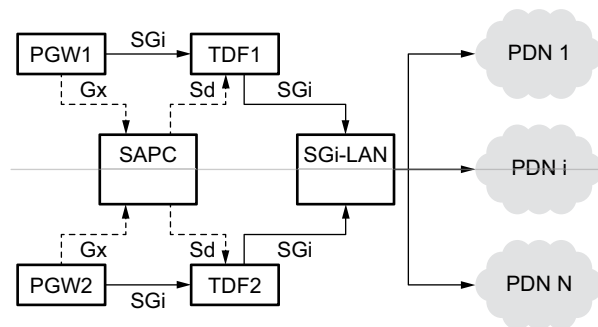


Figure 2 TDF Selection - One TDF per PCEF

2.2

ADC over Sd Overview

The SAPC that supports the ADC function over the Sd interface instructs the TDF to detect and report application start and stop events. Based on this report, the SAPC makes policy decisions and sends enforcement actions to the PCEF or the TDF, or both.

This function enables the operator to have real-time control over the services of the users. The operator can take the following immediate actions based on the application status:

- Change of service authorization
- Quality of Service (QoS) modification
- Bandwidth management
- Service charging control
- User notifications

QoS modification can be achieved by modifying the default or dedicated bearer QoS, or allocating dedicated resources.

The SAPC supports the activation of ADC rules in the TDF by using static ADC rules. These ADC rules can be used both for detection and enforcement. The type of the supported enforcement depends on the ADC rules defined in the TDF. The SAPC only activates or deactivates the ADC rules.

Figure 3 illustrates a high-level flow of the default bearer QoS upgrade based on notifications from the TDF. The TDF performs packet inspection on the data flow and detects when the user contacts a third-party content provider to start a video streaming service. The TDF informs the SAPC about the activation of the streaming service, and the SAPC adapts the QoS of the default bearer to guarantee the service delivery.

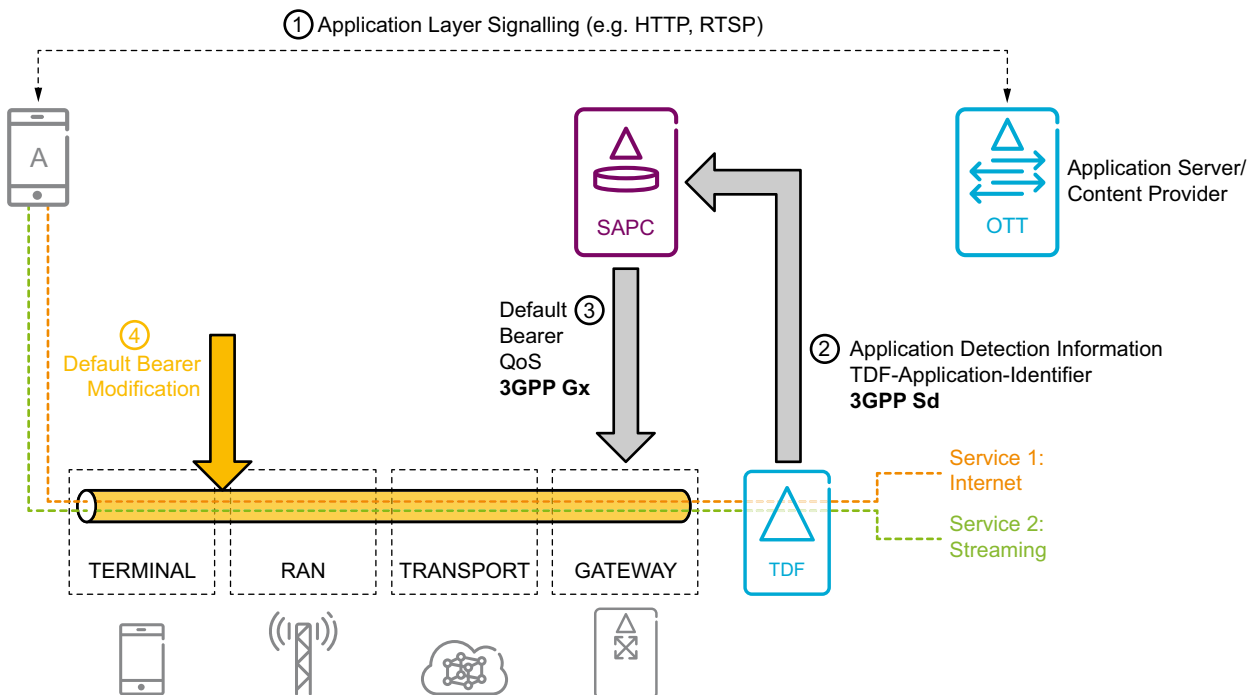


Figure 3 Default Bearer QoS Upgrade Based on Application Detection Start

First, the default bearer is established with the negotiated QoS, then:

1. The User Equipment (UE) starts the application traffic
2. The TDF detects and reports an application start event to the SAPC



3. The SAPC evaluates the QoS and sends new QoS to the GGSN (PGW)
4. The default bearer is updated with the new QoS

2.3 Service Access Control in Sd

The SAPC authorizes services as described in *Access and Charging Control (Gx)*.

The procedure to determine the authorized services in Sd includes service selection, service authorization, and service qualification.

When the authorized service contains ADC configuration, the SAPC authorizes ADC rules to be activated in the TDF for a particular Sd session.

Service Access Control in Sd contains a few restrictions in comparison with Gx. For more information, see the following sections:

- [Service Selection](#) on page 5
- [Service Authorization](#) on page 5
- [Service Qualification](#) on page 5

2.3.1 Service Selection

Service selection differentiates the services to be downloaded to the TDF from the services downloaded to the PCEF.

If an Sd session is established, the services that contain ADC rule configuration are exclusively downloaded to the TDF through the Sd interface.

2.3.2 Service Authorization

Regardless ADC rule configuration, there is no restriction on service authorization.

2.3.3 Service Qualification

For those services that contain ADC rule configuration, only static service qualification applies, as described in *Access and Charging Control (Gx)*.

2.4 Application Detection Reporting

The TDF performs application reporting if an Sd session is established for that purpose. The conditions for the SAPC to establish an Sd session for ADC towards the TDF associated with the PCEF that initiates the IP-CAN session are verified during the IP-CAN session establishment. These conditions are the following:



- There is no ADC support over the Gx interface

For more information, see *Application Detection and Control based on PCC rules (Gx)*.

- Authorized ADC rules are available for the IP-CAN session
- A valid Sd license is available
- TDF routing information is received over the Gx interface, within the initial Credit Control Request (CCR) message or pre-provisioned at the SAPC

If all these conditions apply, an Sd session is established. This Sd session includes the ADC rules which are used in the TDF that is associated with the PCEF for the purpose of application detection.

Once the Sd session is established, the TDF performs application reporting.

Note: The SAPC is subscribed to application start and stop event triggers.

The TDF reports the application status at application level or service data flow level, by sending the application start and stop events and application detection information to the SAPC.

If the reporting is at application level, the application detection information includes:

- A TDF application identifier, to refer to the corresponding application

If the reporting is at service data flow level, the application detection information includes:

- The TDF application identifier
- Flow information
- The TDF application instance identifier

Note: Each application may have several service data flows, and each TDF application instance identifier maps to an individual flow or a group of flows.

During the lifetime of an ADC rule, the SAPC expects that the application start and stop events are reported at the same level, that is either at application or service data flow level. The SAPC uses the TDF application identifier and TDF application instance identifiers received in the start and stop notifications reported by the TDF to keep track of the application traffic status.

Note: The TDF reports application status to the SAPC, even if the application traffic is discarded in the TDF.



2.5 Dynamic Policy Control over Sd

2.5.1 Dynamic Policy Control over Sd Overview

This section describes the Dynamic Policy Control over Sd function of the SAPC.

Additionally to the Dynamic Policy Control based on the Rx interface already supported in the SAPC, Dynamic Policy Control over the Sd interface provides PCC differentiated per subscriber for services that are dynamically activated. These services take into account the information received from the TDF over the Sd interface.

When a subscriber initiates an application and a TDF is in the data path from the subscriber to the data network, the TDF notifies the activation of the application using the Sd protocol to the SAPC. The SAPC makes classification and policy decisions. As a result, the SAPC generates policy control and charging information and sends the appropriate PCC rules to the PCEF, by using the PCRF-initiated IP-CAN session modification procedure.

This provides a mechanism for the TDF to adapt the service delivery in the transport plane to the required conditions dynamically, by installing the applicable PCC rules in the PCEF with the corresponding QoS and charging parameters.

Depending on network and UE capabilities, the default bearer can be used to transport the service, or a dedicated bearer can be established. If a dedicated bearer cannot be established, the default bearer is shared among all the services running on the IP-CAN session as shown in [Figure 3](#).

Dynamic Policy Control over Sd comprises the following functions:

- Classification (identification) of dynamic services
- Generation of dynamic PCC rules
- Allocation of QoS and charging parameters to the classified dynamic services
- Provisioning and removal of PCC rules to the PCEF

The application information provided by the TDF includes the application identifier. Optionally, it can also include additional information, such as the set of IP flows required to deliver the service, and the application instance identifier. This information is used by the SAPC to identify and qualify the dynamic services according to the configured policies and conditions. Dynamic PCC rules are only generated when the TDF provides information about the IP flows required to deliver the service.

[Figure 4](#) shows a high-level flow of the establishment of a dynamic service. In this case, the service delivery, for example Skype, requires the establishment of a dedicated bearer. During ADC, the TDF notifies the SAPC about the start of an application. The SAPC associates the received service data flows with an existing

IP-CAN session and creates a policy rule for the service, which triggers the PGW to create a new dedicated bearer.

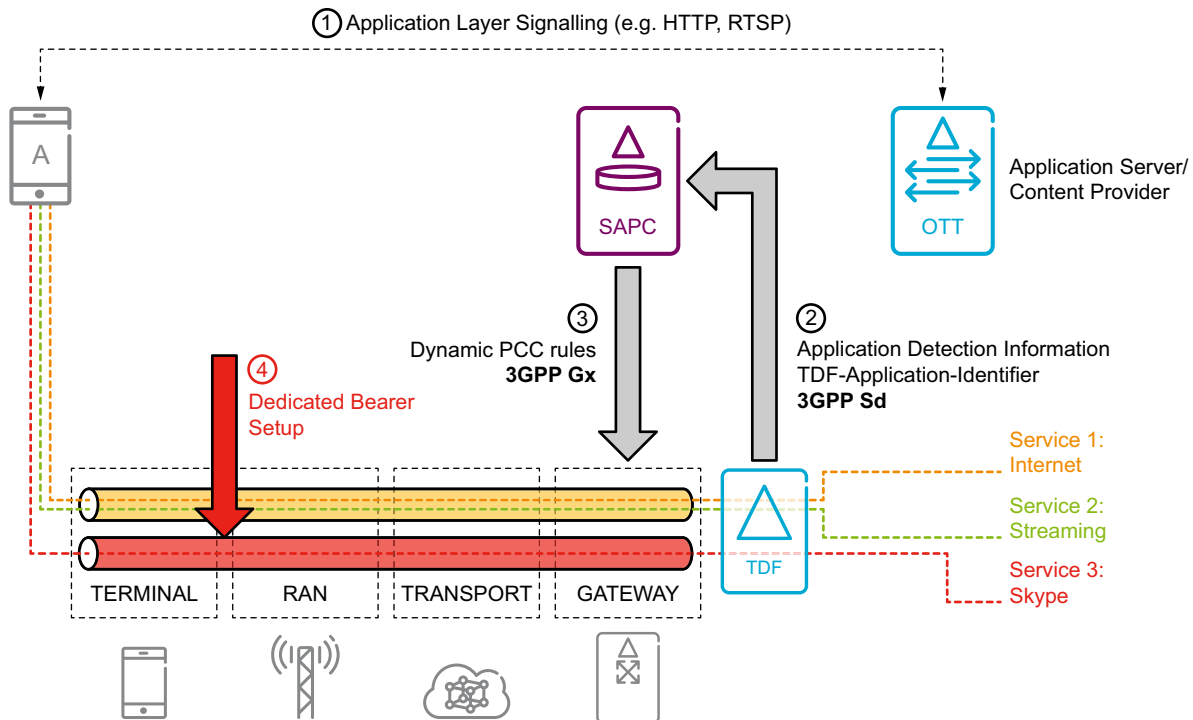


Figure 4 Sd Session Notification with Flow Information and Dedicated Bearer Setup

If a dedicated bearer cannot be established, the default bearer is shared among all the services running on the IP-CAN session.

2.5.2 Classification of Dynamic Services over Sd

This function determines the services that are dynamically activated in the PCEF based on information provided by the TDF through the Sd interface.

The TDF provides service information (application detection information) to the SAPC in the Credit Control Request-Update (CCR-U). The service data flows, when provided within the application detection information, are structured into a Flow-Information AVP in the CCR-U message. The SAPC uses this information to trigger the activation of one or more dynamic services, according to the configured conditions in the policies for dynamic service classification in Sd.

Dynamic service classification in Sd is performed at Sd session application reporting notification, including a START event, only if the TDF-Application-Instance-Identifier and Flow-Information AVPs are included in the Application-Detection-Information AVP.



Dynamic service classification is a global policy in the SAPC. It means that the policy is applied to all active subscribers and subscriber groups.

When a dynamic service is activated for an IP-CAN session based on information that is received over the Sd interface, it remains active until the SAPC receives a STOP notification, affecting the same IP-CAN session, for the corresponding TDF-Application-Id and TDF-Application-Instance-Identifier AVPs.

The following information received from the TDF can be evaluated to classify dynamic services in Sd:

- TDF application identifier
- TDF application instance identifier
- Flow information, including the IP address, the port or port range that is used to deliver the application service, which corresponds to the destination IP address or port of the uplink traffic or source IP address or port of the downlink traffic

The SAPC evaluates the policies for Dynamic Service Classification. The result of the service classification is the service identifier. The conditions (policy rules) to classify dynamic services are configured in the SAPC to match the application detection information received from the TDF. It is possible to classify one dynamic service per TDF-Application-Instance-Identifier AVP notified within the Application-Detection-Information AVP that is included in the CCR-U in the Sd session.

Figure 5 shows examples of service classification in Sd patterns and the associated dynamic service identifier.

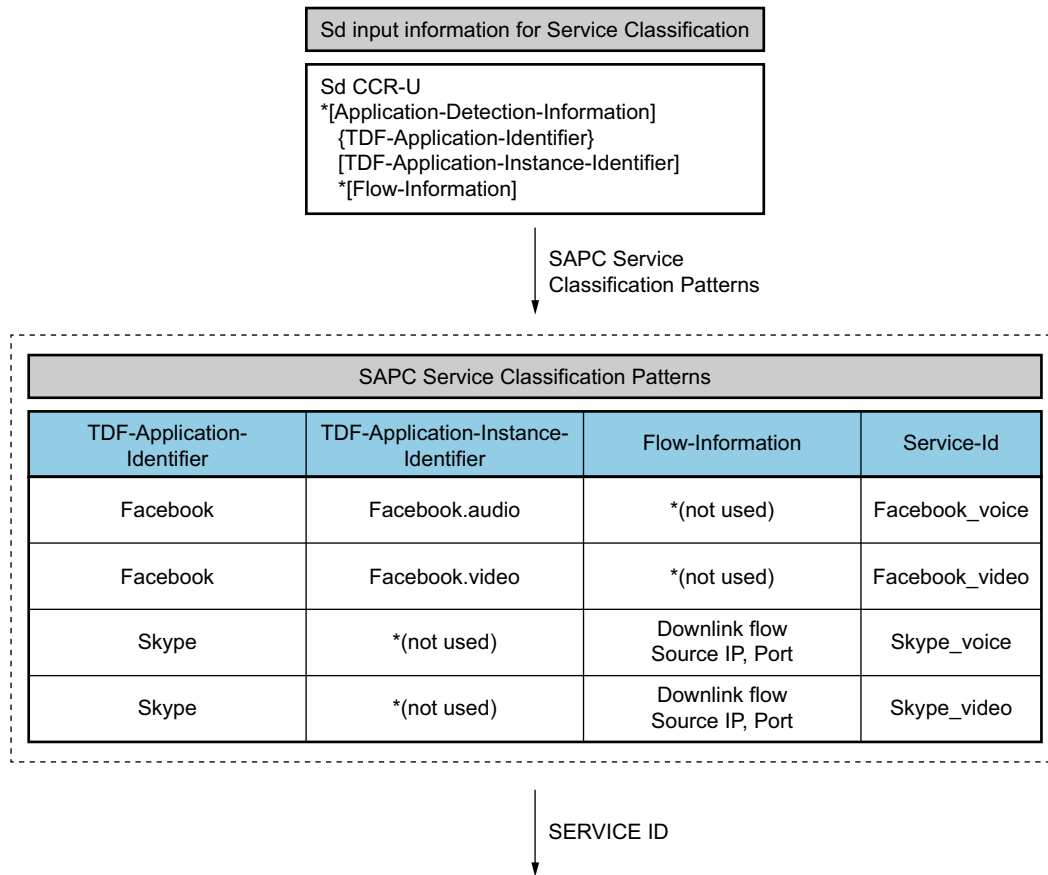


Figure 5 Service Classification in Sd Patterns and Associated Dynamic Service Identifiers

The output service identifier of the classification process is used as a reference to perform the subsequent service qualification.

If no policies are defined in the SAPC to match the information received in the CCR-U command and classify the relevant dynamic services, or some policies are defined but no result is obtained, the SAPC does not execute the subsequent service qualification and dynamic PCC rule generation.

The SAPC answers to the TDF successfully, regardless the result of the service classification.

2.5.3 Qualification of Dynamic Services over Sd

When the dynamic services are successfully classified, the SAPC determines the QoS information and the charging parameters associated with the dynamic PCC rules generated for the service.

Dynamic service qualification over the Sd interface is performed:



- When a new dynamic service is classified for a subscriber, as a result of the Sd session start event notification
- During IP-CAN session reauthorization, because of IP-CAN session modification or PCRF-initiated reauthorization

The output of the qualification of a dynamic service is a QoS profile and a charging profile that contain the authorized QoS and charging information for the dynamic PCC rule generated for the service.

For newly established dynamic services, this process, together with the dynamic PCC rule generation, results in new PCC rules sent to the PCEF in a Re-Authorization-Request (RAR) command.

For existing dynamic services, the SAPC re-evaluates the dynamic service qualification policies to detect changes. If the QoS or charging information differs from what was provisioned to the PCEF, the SAPC updates the existing PCC rules by sending a RAR command to the PCEF.

Dynamic services can be qualified with QoS or charging data, or both, either statically, using the `contentQosProfileId` and `contentChargingProfileId` attributes, or using policy conditions. The SAPC first evaluates the service qualification policies according to the following precedence allocation:

1. Subject policy locator
2. Subject group policy locator

Note: All active subscriber groups are considered.

3. Global policy locator

If there are conflicts among the rules within a policy, the result for the policy depends on the rule combining algorithm configured. For more information, see [Subscription and Policy Management](#).

If there are no applicable policies, or the policies are not fulfilled, the SAPC obtains the QoS and charging profile statically assigned to the dynamic service.

2.5.3.1

Allocation of QoS Information to Dynamic Services

The QoS information includes the following pieces of information:

- The QoS class identifier (authorized QoS class for the service data flow)
- The Allocation and Retention Priority (ARP) parameter
- Authorized bit rates for uplink and downlink

To get the QoS information associated with the dynamic service, the SAPC evaluates the QoS policies that apply to the service identifier that is obtained from the Dynamic Service Classification procedure. These policies can consider



subscriber information, access network information provided by the PCEF, and application detection information provided by the TDF.

The QoS information is assigned per service identifier.

If the QoS profiles obtained after the policy evaluation do not provide values for the QCI, MBR, or GBR, the SAPC omits these values in the dynamic PCC rule for this IP flow.

If there are no applicable policies, or the policies are not fulfilled, the SAPC obtains the QoS profile provisioned to the dynamic service (static qualification).

2.5.3.2 Allocation of Charging Parameters to Dynamic Services

The charging parameters define the following:

- Service Identifier
- Rating Group
- Reporting Level
- Metering Method
- Online charging interface enabled or not
- Offline charging interface enabled or not

To get the charging profile associated with a dynamic service, the SAPC evaluates the charging policies that apply to the service identifier obtained in the Dynamic Service Classification procedure. These policies can consider subscriber information, access network information provided by the PCEF, and application detection information provided by the TDF.

If the charging profile obtained after the policy evaluation does not provide any of the optional charging parameters, this information is omitted from the dynamic PCC rule.

If there are no applicable policies, or the policies are not fulfilled, the SAPC obtains the charging profile provisioned to the dynamic service (static qualification).

Finally, if the procedure cannot obtain a charging profile, no charging information is included in the dynamic PCC rule.

2.5.4 Dynamic PCC Rule Generation Based on Service Data Flow Received over Sd

The SAPC receives information about the initiated application through the Sd interface. If the flow information and application instance identifier are received,



the SAPC generates the PCC information in the form of PCC rules. These dynamic PCC rules are installed in the PCEF through the Gx protocol.

The SAPC can generate one dynamic PCC rule per application instance identifier received from the TDF. New dynamic PCC rules are generated when new dynamic services are established, that is when the TDF sends an application start notification.

Figure 6 shows the relation between the TDF service information received through the Sd interface and the PCC rule information that is generated by the SAPC and installed in the PCEF using the Gx interface.

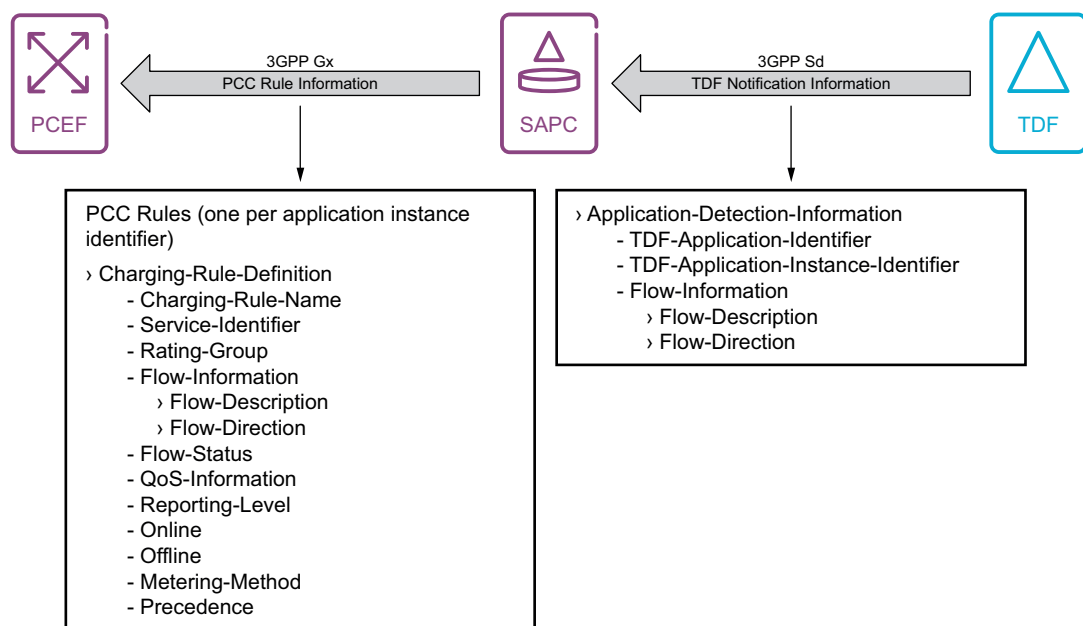


Figure 6 Information Received from the TDF and Provided to the PCEF

The information received from the TDF contains the following AVPs:

- TDF-Application-Identifier: refers to the application in the report sent to the PCRF
- TDF-Application-Instance-Identifier: refers to the instance of a specific application if service data flow descriptions are deducible and reported from the TDF to the SAPC
- Flow-Information:
 - Flow-Description: describes the uplink or downlink IP flows. It includes direction, source IPv4 address or IPv6 prefix, destination IPv4 address or IPv6 prefix, source port, destination port and protocol
 - Flow-Direction: describes the direction of the flows

The SAPC generates the corresponding dynamic PCC rule for each TDF-Application-Instance-Identifier AVP, and installs the corresponding PCC rule. The SAPC can generate one PCC rule per TDF-Application-Instance-Identifier AVP.

The SAPC generates each PCC rule containing the following information:

- PCC rule name: A unique identifier within the IP-CAN session provisioned in the Charging-Rule-Name AVP. The SAPC assigns a name to the PCC rules based on the TDF-Application-Identifier and the TDF-Application-Instance-Identifier values.
- Service data flow: This information identifies the uplink and downlink IP flows of a detected application.
 - Flow-Information AVP: the SAPC obtains the Flow-Information AVP from the information coming from the TDF.
 - Flow-Status AVP: it must be set to:
 - ENABLED_UPLINK (0): when the received flows only contain Flow-Direction AVPs with value upload (2)
 - ENABLED-DOWNLINK (1): when the received flows only contain Flow-Direction AVPs with value download (1)
 - ENABLED (2): when the received flows contain Flow-Direction AVPs with value upload (2) and download (1), or bidirectional (3)

Note: Flow-Status DISABLED (3) is not considered and REMOVED (4) is not applicable to the Gx interface.

- Precedence: the SAPC provides a value that belongs to the dynamic PCC rule precedence range. The SAPC calculates the precedence of the dynamic PCC rule beginning with the lowest numeric value of the precedence range according to the following criteria:
 - If the DL filter of the PCC rule is completed and defined with specific source and destination ports, the SAPC sets the precedence value to zero.
 - If some information of the DL filter is missing or incomplete, the precedence value is increased.
 - If the source or destination port is a list or a range, the precedence is increased by one.
 - If the source or destination port is missing, the precedence is increased by two.
 - If the source or destination IP is missing or is set to the keyword "any", the precedence is increased by one.



Note: If more than one Flow-Information AVPs are received, the precedence has to be calculated for each of them. The lowest precedence value obtained for the DOWNLINK and BIDIRECTIONAL flows must be used.

- QoS information: to generate the QoS information that applies to the PCC rule, the SAPC applies Dynamic Service Qualification.
- Charging Information: the SAPC obtains the Rating Group, Reporting Level, Metering Method, offline and online states, and the Service Identifier by applying Dynamic Service Qualification. Charging information includes the following:
 - Rating Group: it defines the charging key for the PCC rule, used for rating purposes.
 - Reporting Level: it defines the level on which the PCEF reports the usage for the related PCC rule. Reporting level can be at a combination of the service identifier and rating group, or at rating group level.
 - Metering Method: it defines what parameters are metered for offline charging. Metering method can be duration, volume, or both.
 - Offline: it defines whether the offline charging interface from the PCEF for the associated PCC rule is enabled.
 - Online: it defines whether the online charging interface from the PCEF for the associated PCC rule is enabled.
 - Service Identifier: The identity of the service or service component that the service data flow in a PCC rule relates to.

Note: Charging information must not be provided over the Gx interface for the dynamic PCC rule if TDF is already applying charging for the same traffic. The SAPC does not have information about the TDF configuration, therefore, this SAPC provisioning is the responsibility of the operator.

2.6 IP-CAN Session Reauthorization

In the SAPC, the establishment and termination of dynamic services over the Sd interface also trigger a re-evaluation of all previous policy decisions taken for the IP-CAN session. Examples of the application of session reauthorization owing to dynamic service establishment include the ability to apply Bearer QoS Control, Access and Charging Control, and Bandwidth Management to other services running in the IP-CAN session.

Session reauthorization owing to dynamic service establishment is useful, for example, in the following scenarios:

- For scenarios in which only the default bearer is supported, and a user application is started. In this case, the SAPC can downgrade the QoS of the

other services running on the default bearer, to accommodate the application service. Alternatively, the SAPC can upgrade the QoS of the default bearer to accommodate all services.

- For scenarios in which a TDF provides flow description to the SAPC. In this case, a dynamic PCC rule can be defined in the SAPC that is associated with the activation of a dynamic service. This PCC rule definition initiates the establishment of a dedicated bearer for the delivery of the service detected by the TDF.

The SAPC reauthorizes the IP-CAN session at TDF session notification, regardless the generation of dynamic PCC rules. The SAPC uses the TDF application identifier and TDF application instance identifiers received in the start and stop notifications reported by the TDF to keep track of application traffic status and uses this information to evaluate the applicable policies for the IP-CAN session to perform the following functions:

- IP-CAN Session Access Control
- Service Access Control
- Service Charging Control
- Bearer QoS Control
- Bandwidth Management

For more information, see the following documents:

- Access and Charging Control (Gx)
- Bearer QoS and Bandwidth Management

The conditions (policy rules) for the functions mentioned above are extended to apply policy decisions based on the establishment of a dynamic service over Sd as follows:

- Indication of dynamic service establishment

This function indicates if a dynamic service is running in the IP-CAN session, which means that the dynamic service was classified and generated successfully. This allows the SAPC, for example, to authorize and install static or preconfigured PCC rules depending on a given dynamic service running or not.

In addition to that, to calculate the QoS for the default bearer, the SAPC uses the Bearer QoS Control function extended with the Maximum QoS and Aggregated QoS for dynamic services functions to take policy decisions.

- Maximum QoS for dynamic services



This function returns a QoS profile composed of the highest value for every field in the QoS profile, out of the values received for each dynamic PCC rule running in the IP-CAN session (including dynamic services based on AF and TDF notifications through the Rx and Sd interfaces, respectively).

— Aggregated QoS for the dynamic services

This function returns a QoS profile composed of the sum of the throughput parameters (GBRs and MBRs), out of the values received for each dynamic PCC rule running in the IP-CAN session (including dynamic services based on AF and TDF notifications through the Rx and Sd interfaces, respectively), and selecting the highest value in the rest of the QoS parameters.



3 ADC Network Deployments over Sd

The SAPC can provide Application and Detection Control in the following network deployments:

- In the bearer plane (PCEF) side:
 - Ericsson EPG, through Ericsson Gx+ Rel9 onwards
 - Non-Ericsson PCEF, through standard Gx Rel9 onwards
- In the application plane (TDF) side:
 - Non-Ericsson TDF, through standard Sd Rel11 onwards



4 ADC Traffic Cases over the Sd Interface

This section explains the Sd interface which is involved in the ADC function based on TDF network deployment, and the traffic interactions between the network functions involved. For a detailed description of the Sd interface, see [Sd Interface Description](#).

The precondition to all traffic cases is that a diameter connection is already established between the SAPC and the PCEF, and between the SAPC and the TDF. In addition, support for dynamic PCC rules in the PCEF for the GGSN (PGW) and the following policy controls must be enabled in the PCEF:

- `dynamicServiceSupport` control is required for the SAPC to install dynamic services
- Bearer QoS Policy Control is required to allocate QoS information to dynamic services
- Service Charging Policy Control is required to allocate charging Information to dynamic services

The `Session-Id` is a mandatory AVP for all the messages in the Sd protocol, to identify a TDF session uniquely.

Precondition to all traffic cases:

- The availability of this function in the SAPC must be under license control, otherwise the SAPC does not initiate any Sd session establishment.

4.1 Sd Session Life Cycle

These traffic cases show the Sd session life cycle: establishment, modification, and termination.

4.1.1 Sd Session Establishment

Sd session establishment can be initiated at:

- IP-CAN session establishment
- IP-CAN session reauthorization due to a CCR-U received over the Gx interface
- IP-CAN session reauthorization due to a subscriber profile change, a Time of Day (ToD) condition, Rx or Sy events

[Figure 7](#) shows an example of Sd session establishment at IP-CAN session establishment.

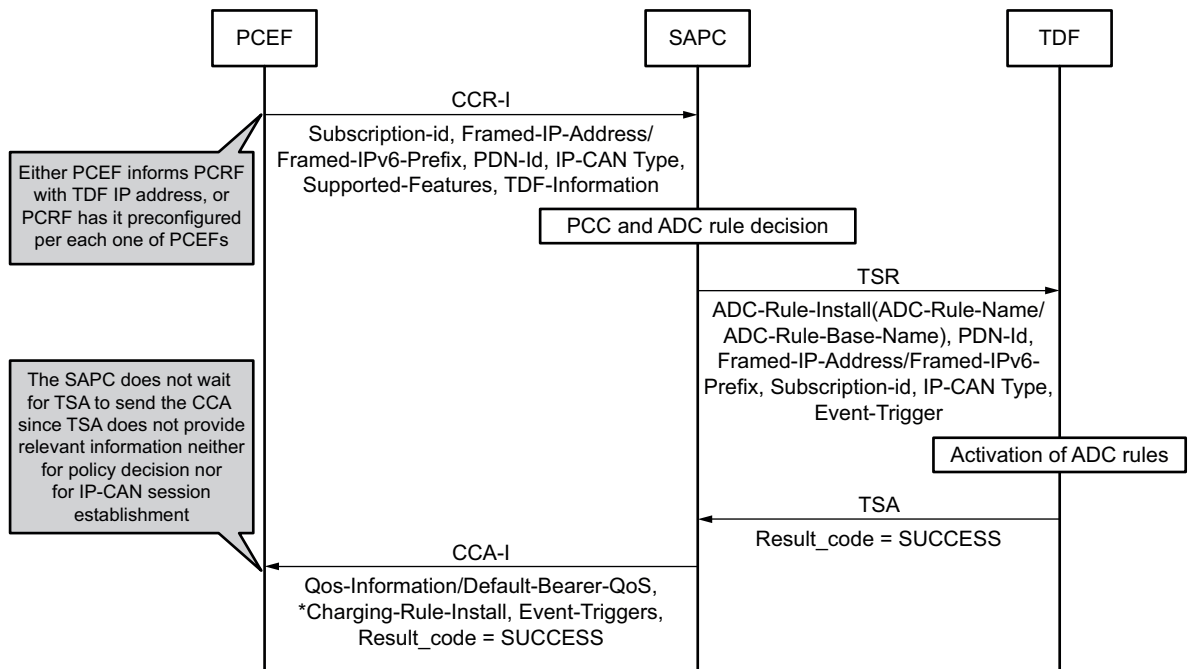


Figure 7 Sd Session Establishment at IP-CAN session establishment

- 1. The UE attaches to the network, and the PCEF receives a notification about this situation.
- 2. The PCEF sends a Credit Control Request-Initial (CCR-I) message to the SAPC with the ADC bit not set in the Supported-Features AVP. This message indicates that the PCEF does not support ADC. Optionally, it can also include the TDF-Information AVP containing information about the TDF that handles the application detection and reporting for that IP-CAN Session. The TDF-Information AVP includes the TDF-Destination-Realm and TDF-Destination-Host AVPs (both must be present) or the TDF-IP-Address AVP.
- 3. Based on the conditions described in [Application Detection Reporting](#) on page 5, the SAPC evaluates whether an Sd session has to be established with the TDF per corresponding IP-CAN session, during the IP-CAN session establishment. The Public Data Network (PDN) identifier, IP address, and the UE identity enable the identification of the IP-CAN session. The SAPC receives the TDF routing information either over the Gx interface in the previous step or it is pre-provisioned at the SAPC. A valid Sd license and the ADC support over the Gx interface are validated during IP-CAN session establishment.
- 4. The SAPC performs session authorization including the evaluation of Access and Charging Control.

The SAPC decides:



- To install preconfigured PCC rules and to activate static PCC rules to the PCEF
- To activate ADC rules to the TDF

Note: The Sd session is not established if there is an Sd session already established for the IP-CAN session. The association between the IP-CAN and Sd session is 1:1.

- 5. The SAPC sends a TDF Session Request (TSR) message to initiate an Sd session towards the TDF providing the ADC-Rule-Install AVP which includes the name of the ADC rules to activate within the ADC-Rule-Name or ADC-Rule-Base-Name AVPs; the Framed-IP-Address AVP, the Framed-Ipv6-Prefix AVP, or both, depending on the AVPs received over the Gx interface; the Called-Station-Id AVP, the User-Equipment-Info AVP if received over the Gx interface, and the Event-Triggers AVP including the APPLICATION_START and APPLICATION_STOP events.

Note: The SAPC does not support any features beyond the base functionality. As a result, the TSR command does not contain any Supported-Features AVP(s) and the TDF Session Answer (TSA) command does not include the Supported-Features AVP. In this case, both the TDF and the SAPC behave as specified in the Rel-11 version.

- 6. The TDF starts traffic detection.
- 7. The TDF sends a TSA to acknowledge the Sd session establishment and inform the SAPC about the outcome of the actions related to the decisions received in the TSR message. If the received result code is different from DIAMETER_SUCCESS, the Sd session will not be established.

Note: An Sd session is not established if the establishment of the associated IP-CAN session fails. In that case, the SAPC initiates an Sd session termination procedure for the affected Sd session.

- 8. The SAPC answers with a Credit Control Answer-Initial (CCA-I) message to the PCEF including the following AVPs:
 - Charging-Rule-Install AVP, including the Charging-Rule-Name or Charging-Rule-Base-Name AVPs for static PCC rules, and the Charging-Rule-Definition AVP for preconfigured PCC rules
 - The QoS-Information or Default-EPS-Bearer-QoS AVP with the QoS to apply to the default bearer

Note: The IP-CAN session is established regardless the outcome of the Sd establishment.

- 9. The PCEF applies the downloaded QoS parameters to the default bearer.

Figure 8 shows an example of Sd session establishment at IP-CAN session reauthorization due to a Gx CCR-U message.

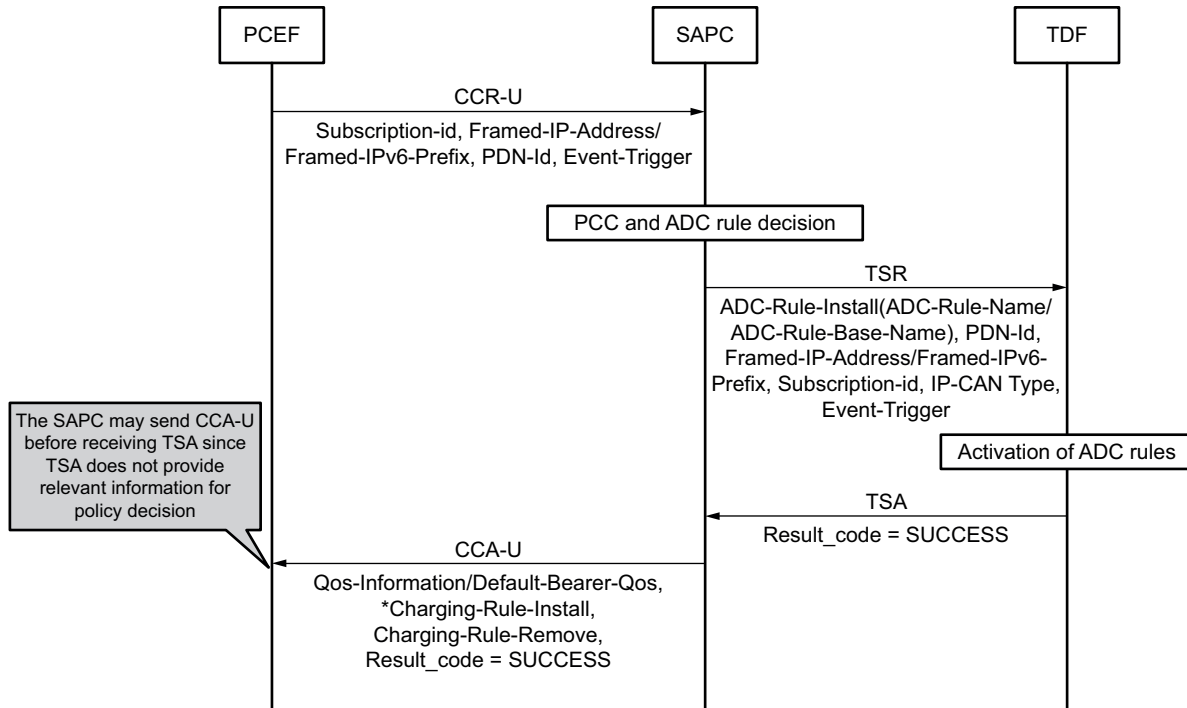


Figure 8 Sd Session Establishment at IP-CAN Session Reauthorization due to Gx CCR-U

During the IP-CAN session reauthorization, the SAPC may decide that an Sd session should be established with the TDF per corresponding IP-CAN session. No Sd session is established yet, because the SAPC did not send an Sd TSR message since there were no authorized ADC rules to be activated in the TDF. It can also happen that the SAPC did not receive the Sd TSA message or received it with an error.

- 1. The SAPC receives a CCR-U message from the PCEF indicating IP-CAN session modification. The CCR triggered by IP-CAN session modification only contains the new or modified parameters together with the associated event triggers.
- 2-6. These steps correspond to steps 4-8 in Figure 7.

Note: The TDF routing information is obtained during IP-CAN session establishment or it is preconfigured in the SAPC. Further details about Sd session establishment have been explained previously.

- 7. The SAPC sends a Credit Control Answer (CCA) message to the PCEF that includes the new or modified information only.

Figure 9 shows an example of Sd session establishment at IP-CAN session reauthorization due to subscriber change or SAPC events (ToD, Rx, or Sy).

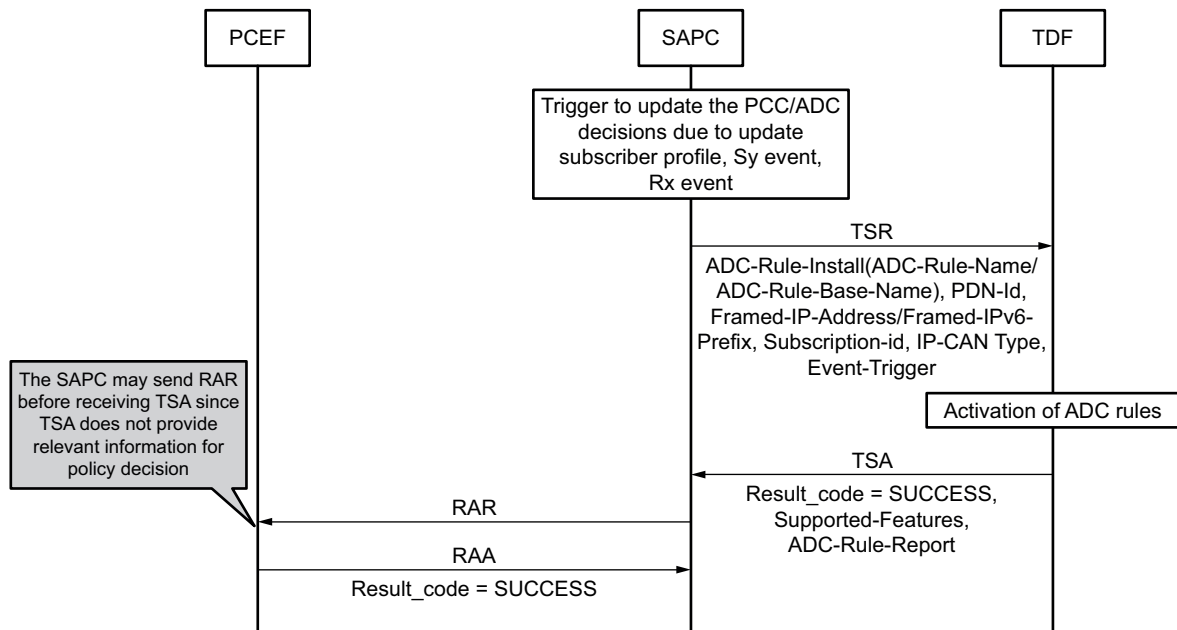


Figure 9 Sd Session Establishment at IP-CAN Session Reauthorization due to Subscriber Change or SAPC Events (ToD, Rx, Sy)

During the IP-CAN session establishment, the SAPC may decide that an Sd session should be established with the TDF per corresponding IP-CAN session.

No Sd session is established yet: the SAPC did not send an Sd TSR message since there were no authorized ADC rules to be activated in the TDF. It can also happen that the SAPC did not receive the Sd TSA message or received it with an error.

- 1. During the IP-CAN session reauthorization due to a subscriber change or SAPC events (ToD, Rx, or Sy), the SAPC may decide that an Sd session has to be established with the TDF per corresponding IP-CAN session.
- 2-6. These steps correspond to steps 4-8 in Figure 7.

Note: The TDF routing information is obtained during IP-CAN session establishment or it is preconfigured in the SAPC. Further details about Sd session establishment have been explained previously.

- 7. The SAPC sends a RAR message to the PCEF that includes the new or modified information only.
- 8. The PCEF sends a Re-Authorization Answer (RAA) message to the SAPC to acknowledge the Gx session reauthorization and inform the SAPC about the outcome of the actions related to the decisions received in the RAR message.

4.1.2 Sd Session Modification

Sd session modification can be initiated by the SAPC when a change in the ADC rules to be installed or removed in the TDF is detected:

- Triggered by a Gx CCR-Update
- Triggered by an internal event as a subscriber change or ToD event
- Triggered by another external event due to the Rx or Sy interfaces affecting the associated IP-CAN session

Figure 10 shows an example of Sd session modification due to a Gx CCR-U message.

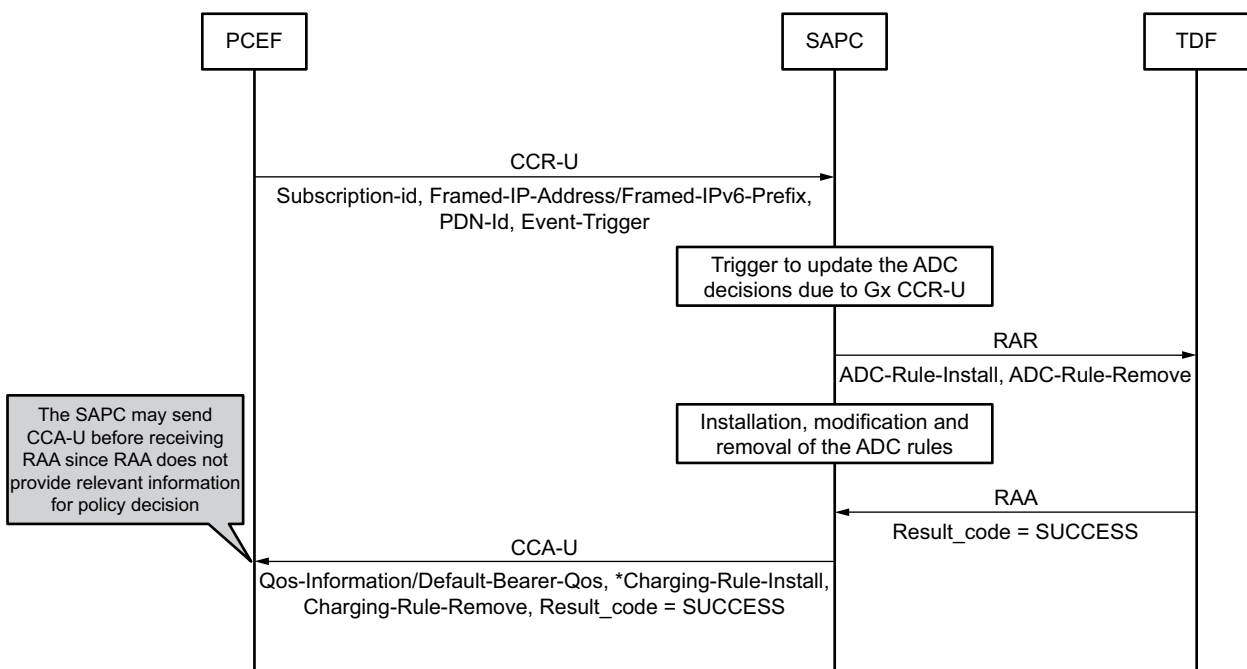


Figure 10 Sd Session Modification due to Gx CCR-U

- 1. The SAPC receives a CCR-U message from the PCEF, indicating IP-CAN session modification. The CCR message triggered by the IP-CAN session modification contains the new or modified parameters only and the event triggers that are associated with them.
- 2. The SAPC performs session authorization including the evaluation of Access and Charging Control.

The SAPC decides:

- To install or remove preconfigured PCC rules and to activate or deactivate static PCC rules to the PCEF



- To activate or deactivate ADC rules to the TDF
- 3. The SAPC sends a RAR to the TDF for the affected Sd session, providing the ADC-Rule-Install or ADC-Rule-Remove AVP that includes the name of the ADC rules to be activated or deactivated within the ADC-Rule-Name or ADC-Rule-Base-Name AVP.
- 4. The TDF activates or deactivates the ADC rules according the new ADC decisions provided.
- 5. The TDF sends an RAA message to the SAPC to acknowledge the Sd session establishment and to inform the SAPC about the outcome of the actions related to the decisions received in the RAR message.
- 6. The SAPC answers to the PCEF with a Credit Control Answer-Update (CCA-U) message, including the following AVPs:
 - Charging-Rule-Install AVP, including the Charging-Rule-Name or Charging-Rule-Base-Name AVP for static PCC rules, and the Charging-Rule-Definition AVP for preconfigured PCC rules
 - The QoS-Information or Default-EPS-Bearer-QoS AVP with the QoS to apply to the default bearer
- 7. The PCEF applies the downloaded QoS parameters to the default bearer.

Figure 11 shows an example of Sd session modification due to a SAPC trigger:

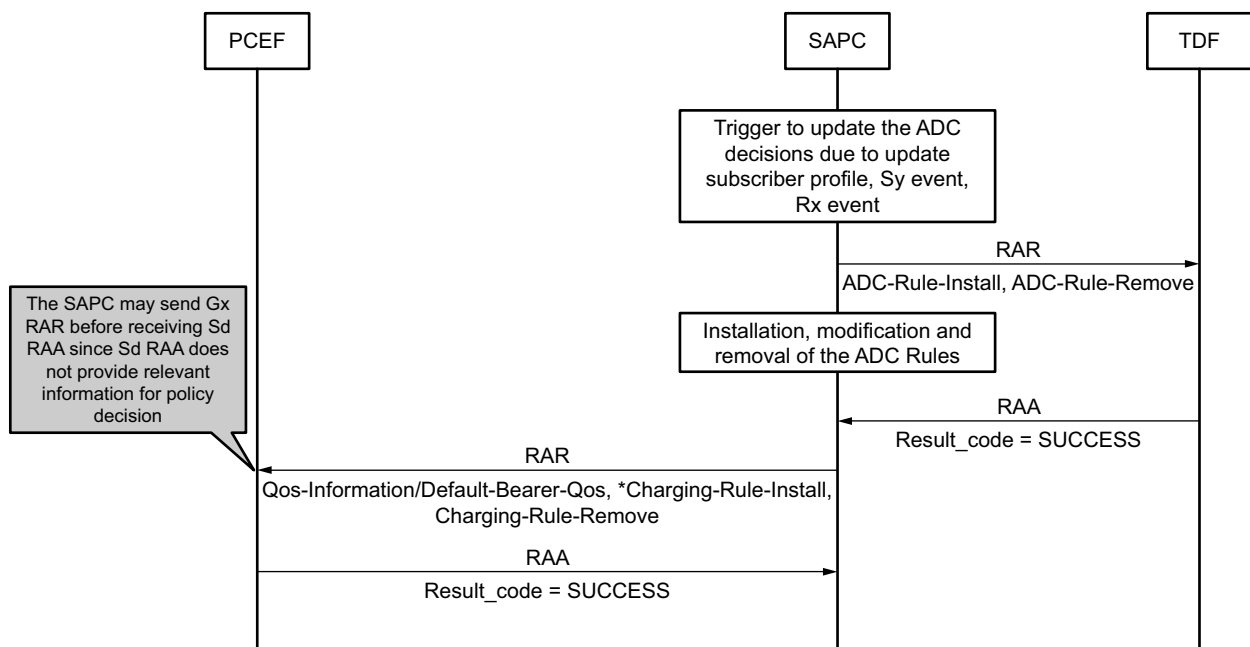


Figure 11 Sd Session Modification due to Subscriber Change or SAPC Events (ToD, Rx, Sy)



- 1. The SAPC receives a trigger to update the ADC rule. This trigger can be a subscriber profile configuration change, for example. The trigger provokes the reauthorization of Sd and Gx sessions. The possible triggers are:
 - The subscriber profile is updated, including changes due to ToD conditions
 - Events received from the AF over the Rx interface
 - Events received from the OCS over the Sy interface
- 2. The SAPC sends a RAR to the TDF for the affected Sd session, providing the ADC-Rule-Install or ADC-Rule-Remove AVP that includes the name of the ADC rules to activate or deactivate within the ADC-Rule-Name or ADC-Rule-Base-Name AVP.
- 3. The TDF activates or deactivates the ADC rules according the new ADC decisions provided.
- 4. The TDF sends an RAA message to acknowledge the Sd session reauthorization and informs the SAPC about the outcome of the actions related to the decisions received in the RAR message.
- 5. The SAPC sends a RAR message to the PCEF that includes the new or modified information.
- 6. The PCEF sends an RAA message to acknowledge the Gx session reauthorization and informs the SAPC about the outcome of the actions related to the decisions received the RAR message.

4.1.3 Sd Session Termination

Session termination is initiated at the request of the PCRF. It happens when the corresponding IP-CAN session is terminated due to the regular IP-CAN session termination, basic clean-up, or massive clean-up when the PCEF is restarted.

Figure 12 shows an example of the Sd session termination traffic case.

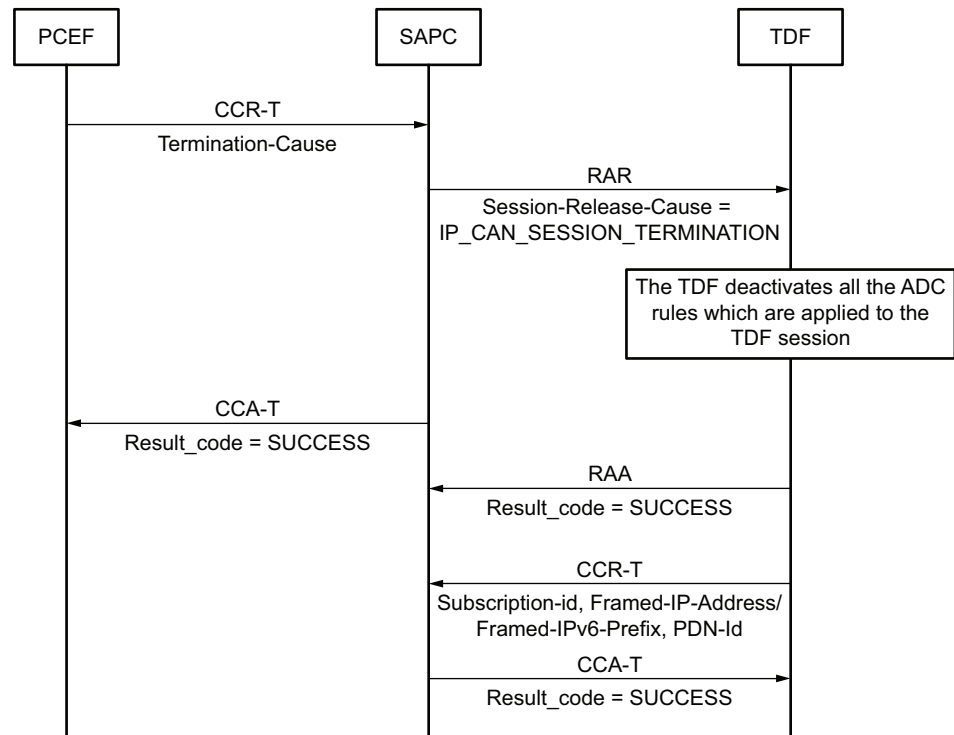


Figure 12 Sd Session Termination

- 1. The PCEF sends a CCR-T message to the SAPC, indicating the IP-CAN session termination.
- 2. The SAPC sends a RAR message to the TDF for the affected Sd session, requesting the termination of the TDF session that is associated with the incoming Gx session Session-Release-Cause AVP (IP_CAN_SESSION_TERMINATION (3) value
- 3. The SAPC removes the information related to the terminated IP-CAN Session and informs the PCEF that the SAPC terminated the handling of the IP-CAN session.
- 4. The TDF deactivates all the ADC Rules which are applied to the TDF session.
- 5. The TDF sends an RAA message to acknowledge the RAR message.
- 6. The TDF sends a CCR-T message to the SAPC, indicating the TDF session termination.
- 7. The SAPC acknowledges the TDF session termination by sending a CCA to the TDF.

Note: The IP-CAN session termination acknowledgement can be sent before initiating Sd session termination.

4.2 QoS Control Based on Application Traffic Detection Upgrading Default Bearer

Based on the notifications received over the Sd interface, the SAPC determines the QoS information to provide for the default bearer, in scenarios where the network or the UE does not support dedicated bearers.

Figure 13 shows an example of default bearer QoS control based on Sd application detection notification.

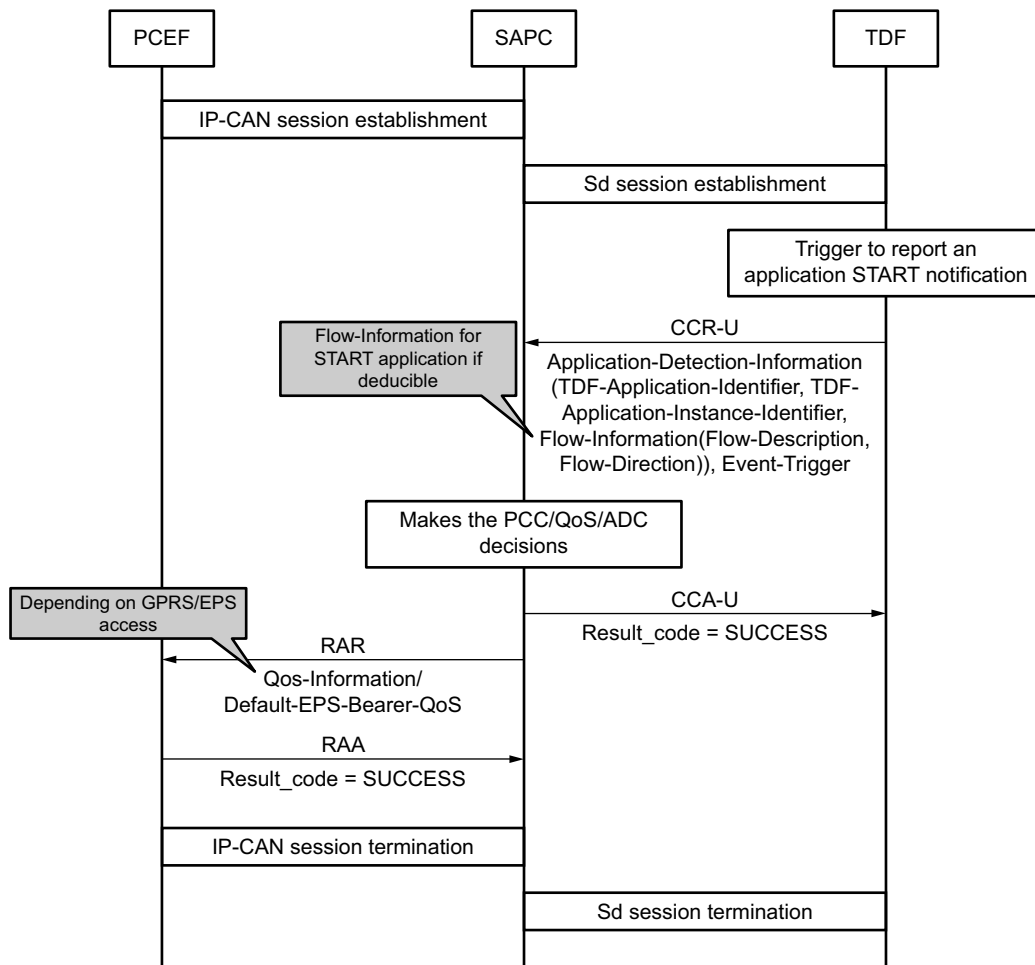


Figure 13 Default Bearer QoS Control Based on Sd Application Detection Notification

4.2.1 Session Establishment

See [Sd Session Establishment](#) on page 19.



4.2.2 Upgrade Default Bearer QoS at Application Start Detected

- 1. The subscriber starts application traffic that is to be detected by the ADC rule.
- 2. The TDF reports the application traffic start event by sending a CCR-U message including the following AVPs:
 - Event-Triggers AVP, including the APPLICATION_START event
 - Application-Detection-Information AVP, including the TDF-Application-Identifier AVP
- Note:** When the service data flow descriptions are deducible, the Application-Detection-Information AVP also includes the Flow-Information and TDF-Application-Instance-Identifier AVPs for the detected application.
- 3. The SAPC performs session binding. As a result, the SAPC identifies the IP-CAN session the current Sd session is related to. The SAPC reauthorizes the Sd and Gx sessions, and, as a result, the QoS for the default bearer is upgraded.
- 4. If, based on the received information, the Sd session needs to be updated because of policy evaluation, the SAPC answers to the TDF with a CCA-U message, including a new ADC-Rule-Install or ADC-Rule-Remove AVP.
- 5. The TDF stores the information received in the Diameter CCA-U message and activates or deactivates the ADC rules according the new ADC decisions provided.
- 6. The SAPC sends a RAR message to the PCEF for the affected IP-CAN session.
- 7. The PCEF answers to the SAPC with an RAA message.

4.2.3 Downgrade Default Bearer QoS at Application Stop Detected

- 1. The subscriber stops the application traffic detected by the ADC rule.
- 2. The TDF reports the application stop event using a CCR-U message including the following AVPs:
 - Event-Triggers AVP, including the APPLICATION_STOP event
 - Application-Detection-Information AVP, including the TDF-Application-Identifier AVP
- Note:** If an application start event is received with the TDF-Application-Instance-Identifier AVP, the corresponding stop event has to include the TDF-Application-Instance-Identifier AVP also.

- 3. The SAPC reevaluates the data to be applied to the subscriber. As a result, the QoS for the default bearer is downgraded.
- 4. If, based on the received information, the Sd session needs to be updated as a result of policy evaluation, the SAPC answers to the TDF with a CCA-U message, including a new ADC-Rule-Install or ADC-Rule-Remove AVP.
- 5. The TDF stores the information received in the Diameter CCA-U message and activates or deactivates the ADC rules according to the new ADC decisions provided.
- 6. The SAPC sends a RAR message to the PCEF for the affected IP-CAN session.
- 7. The PCEF answers to the SAPC with an RAA message.

4.3 QoS Control Based on Application Traffic Detection Allocating Dedicated Bearer

If the TDF sends a CCR-U start notification, including the Flow-Information and TDF-Application-Instance-Identifier AVPs, the SAPC classifies, qualifies, and generates a new dynamic PCC rule from that information. The new dynamic PCC rule is installed in the PCEF through the Gx protocol.

Once dedicated bearers are established in the PCEF based on start notifications received over the Sd interface, the SAPC may request the PCEF to update or terminate these dedicated bearers based on the information received over the Gx interface. Such information can be the location information, for example.

Upon receiving a Gx CCR-U message, the services associated with the subscriber are reauthorized. These services include dynamic services as well. As a result, qualification policies can update the QoS or charging profile.

If an APPLICATION_STOP notification is received, the corresponding PCC rule that was previously installed in the PCEF has to be removed.

Figure 14 shows an example of dedicated bearer QoS control based on Sd application detection notification.

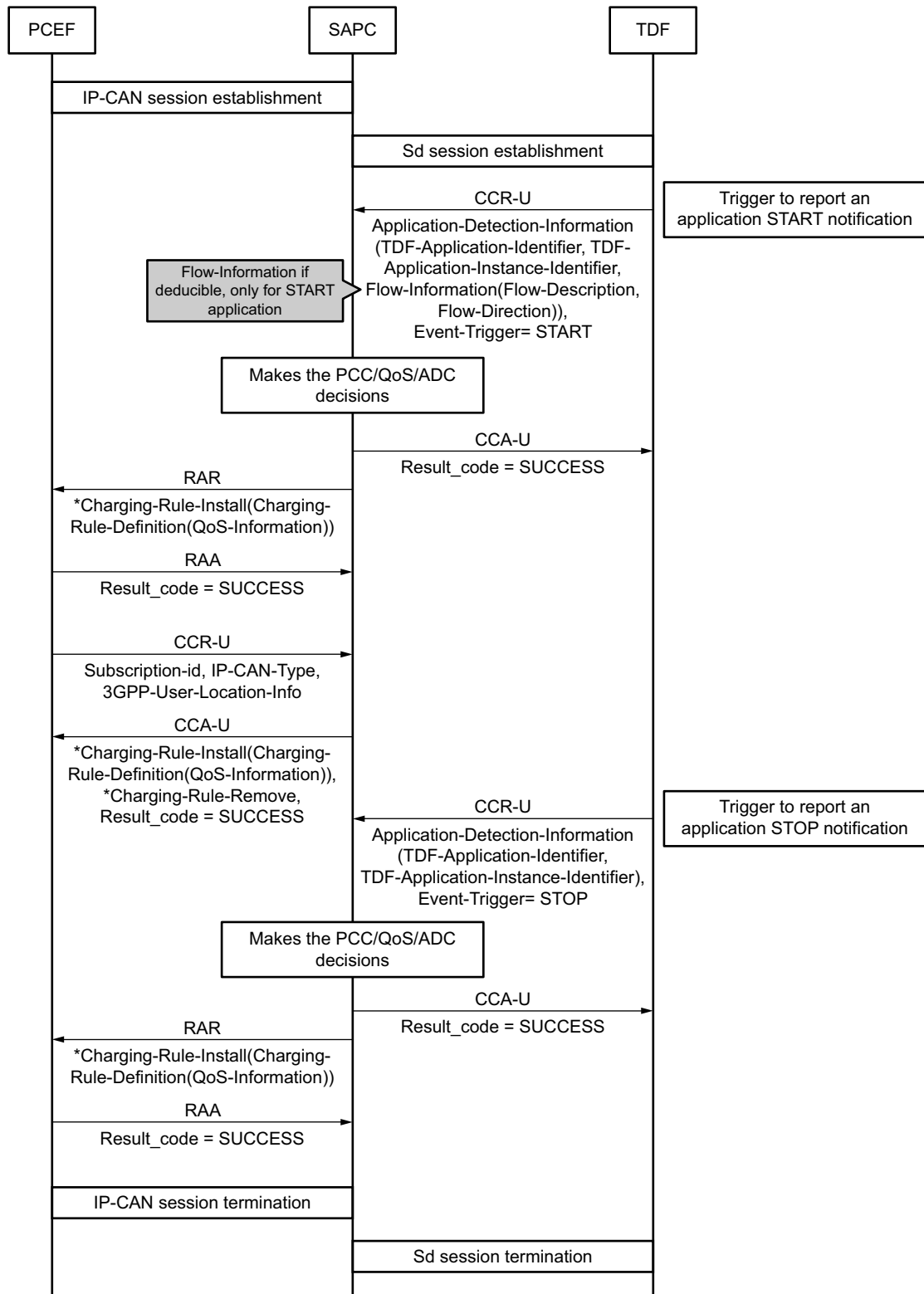


Figure 14 Dedicated Bearer QoS Control Based on Sd Application Detection Notification



4.3.1 Session Establishment

See [Sd Session Establishment](#) on page 19.

4.3.2 Download Dedicated Bearer at Application Start Detected

- 1. The subscriber starts application traffic that is to be detected by the ADC rule.
- 2. The TDF reports the application traffic start event by sending a CCR-U message including the following AVPs:
 - Event-Triggers AVP, including the APPLICATION_START event
 - Application-Detection-Information AVP, including the TDF - Application-Identifier, TDF-Application-Instance-Identifier, and the Flow-Information AVPs for the detected application.
- 3. The SAPC performs session binding. As a result, the SAPC identifies the IP-CAN session the current Sd session is related to. The SAPC reauthorizes the Sd and Gx sessions. As a result, a dedicated bearer is download to the PCEF.
- 4. If, based on the received information, the Sd session needs to be updated as a result of policy evaluation, the SAPC answers to the TDF with a CCA-U message, including a new ADC-Rule-Install or ADC-Rule-Remove AVP.
- 5. The TDF stores the information received in the Diameter CCA-U message and activates or deactivates the ADC rules according the new ADC decisions provided.
- 6. The SAPC sends a RAR message to the PCEF for the affected IP-CAN session, including a Charging-Rule-Install AVP.
- 7. The PCEF answers to the SAPC with an RAA message.
- 8. The SAPC receives a CCR-U message from the PCEF indicating IP-CAN session modification. The CCR triggered by the IP-CAN session modification only contains the new or modified parameters together with the associated event triggers.
- 9. The SAPC performs Gx session reauthorization. As a result, the dynamic PCC rule that was installed in step 6 can be affected.
- 10. The SAPC answers to the PCEF with a CCA-U message, including the following AVPs:
 - Charging-Rule-Install AVP, including the Charging-Rule-Definition AVP to update the previously installed dynamic service
- 11. The PCEF applies the downloaded QoS parameters to the dedicated bearer.



4.3.3 Remove Dedicated Bearer at Application Stop Detected

- 1. The subscriber stops the application traffic detected by the ADC rule.
 - 2. The TDF reports the application stop event using a CCR-U message, including the following AVPs:
 - Event-Triggers AVP, including the APPLICATION_STOP event
 - Application-Detection-Information AVP, including the TDF - Application-Identifier AVP.
- Note:** The application stop event must be received with the TDF - Application-Instance-Identifier AVP in the Application-Detection-Information AVP if the corresponding CCR-Update with the APPLICATION_START event trigger includes it. If the Flow-Information AVP is included in a STOP notification, the AVP is ignored, and the CCR-U message is processed normally.
- 3. The SAPC reevaluates the data to be applied to the subscriber. As a result, a dedicated bearer is terminated in the PCEF.
 - 4. If, based on the received information, the Sd session needs to be updated as a result of policy evaluation, the SAPC answers to the TDF with a CCA-U message, including a new ADC-Rule-Install or ADC-Rule-Remove AVP.
 - 5. The TDF stores the received information in the Diameter CCA-U message and activates or deactivates the ADC rules according the new ADC decisions provided.
 - 6. The SAPC sends a RAR message to the PCEF for the affected IP-CAN session, including the Charging-Rule-Remove AVP.
 - 7. The PCEF answers to the SAPC with an RAA message.

4.4 ADC over Sd Error Handling

4.4.1 Error Handling at Sd Session Establishment

[Table 1](#) shows the potential error codes of Sd session establishment.

Table 1 Error Handling at Sd Session Establishment

Error Condition	Action	Code
The SAPC does not receive a TSA message after sending a TSR.	The Sd session will not be created and the SAPC logs the error (Timeout receiving a TSA).	-
The SAPC receives a TSA with one of the following error codes: — DIAMETER_UNABLE_TO_DELIVER	The Sd session will not be created and the SAPC logs the error (Unsuccessful TSA received).	-



Error Condition	Action	Code
—DIAMETER_LOOP_DETECTED —DIAMETER_INVALID_AVP_VALUE —DIAMETER_USER_UNKNOWN —DIAMETER_ADC_RULE_EVENT		
The SAPC receives a TSA with the DIAMETER_TOO_BUSY error code.	The Sd session will not be created and the SAPC does not log the error either.	-

Note: Regardless the error circumstance over the Sd interface, the SAPC answers with a Gx CCA message according to the Gx processing result.

4.4.2 Error Handling at Sd Session Modification

Table 2 shows the potential error codes of Sd session modification.

Table 2 Error Handling at Sd Session Modification

Error Condition	Action	Code
After sending the RAR message, the SAPC does not receive an RAA.	The SAPC logs the error (Timeout receiving RAA).	-
The SAPC receives an RAA message with one of the following error codes: —DIAMETER_UNABLE_TO_DELIVER —DIAMETER_LOOP_DETECTED —DIAMETER_INVALID_AVP_VALUE	The SAPC logs the error (Unsuccessful RAA received).	-
The SAPC receives an RAA message with either of the following error codes: —DIAMETER_USER_UNKNOWN —DIAMETER_UNKNOWN_SESSION_ID	The Sd session will be deleted, the corresponding dynamic PCC rules will be removed and the SAPC logs the error (Unsuccessful RAA received).	-
The SAPC receives an RAA message with the DIAMETER_TOO_BUSY error code.	The SAPC does not log the error.	-
The SAPC receives an RAA message with the DIAMETER_UNABLE_TO_COMPLY error code.	The SAPC logs the error (Unsuccessful RAA received).	-

4.4.3 Error Handling at Sd Session Termination

Table 3 shows the potential error codes of Sd session termination.

Table 3 Error Handling at Sd Session Termination

Error Condition	Action	Code
After sending a Re-Authorization-Request-Terminate (RAR-T) message, the SAPC does not receive a Re-Authorization Answer-Terminate (RAA-T) message.	The SAPC logs the error (Timeout receiving RAA).	-



Error Condition	Action	Code
The SAPC receives an RAA-T message with one of the following error codes: — DIAMETER_UNABLE_TO_DELIVER — DIAMETER_LOOP_DETECTED — DIAMETER_INVALID_AVP_VALUE	The SAPC logs the error (Unsuccessful RAA received).	-
The SAPC receives an RAA-T message with either of the following error codes: — DIAMETER_USER_UNKNOWN — DIAMETER_UNKNOWN_SESSION_ID	The Sd session will be deleted and the SAPC logs the error (Unsuccessful RAA received).	-
The SAPC receives an RAA-T message with the DIAMETER_TOO_BUSY error code.	The SAPC logs the error.	-
The SAPC receives an RAA-T message with the DIAMETER_UNABLE_TO_COMPLY error code.	The SAPC logs the error (Unsuccessful RAA received).	-
The SAPC receives a CCR-T message, but the SAPC does not have an existing Sd session.	The SAPC rejects the transaction and returns a CCA message indicating an error.	The Result-Code AVP is set to DIAMETER_UNKNOWN_SESSION_ID (5002).
The SAPC receives a DIAMETER_UNKNOWN_SESSION_ID error code from the PCEF in the Gx RAA message.	The SAPC deletes the IP-CAN session, and terminates the related Sd session by sending a RAR-T command.	-

4.4.4 Error Handling at Application Reporting

Table 4 shows how the SAPC handles the errors when receiving an Sd CCR-U, missing certain AVPs.

Table 4 Application Reporting Error Handling

Error Condition	Action	Code
The SAPC receives a CCR-U message for an obsolete session (the SAPC already initiated the Sd session termination procedure).	The SAPC returns a CCA message indicating an error and logs the error (Internal Error)	The Result-Code AVP is set to DIAMETER_UNABLE_TO_COMPLY (5012).
The SAPC receives a CCR-U message for an application start or stop event, but the Application-Detection-Information AVP is not included in it.	The SAPC returns a CCA message indicating an error.	The Result-Code AVP is set to DIAMETER_MISSING_AVP (5005).
The SAPC receives a CCR-U message, including one or more Application-Detection-Information AVP, but the start or stop event triggers are not included in it.	The SAPC returns a CCA message indicating an error.	The Result-Code AVP is set to DIAMETER_MISSING_AVP (5005).
The SAPC receives a CCR-U message for an application start or stop event trigger, but the TDF-Application-Identifier AVP is not included in one or more Application-Detection-Information AVP.	The SAPC returns a CCA message indicating an error.	The Result-Code AVP is set to DIAMETER_MISSING_AVP (5005).
The SAPC receives a CCR-U message for an application start event trigger with the Application-Detection-Information	The SAPC returns a CCA message indicating an error.	The Result-Code AVP is set to DIAMETER_MISSING_AVP (5005).



Error Condition	Action	Code
AVP, including the TDF-Application-Instance-Identifier AVP, but not including the corresponding Flow-Information AVP.		
The SAPC receives a CCR-U message for an application start event trigger with the Application-Detection-Information AVP, including the Flow-Information AVP, but not including the corresponding TDF-Application-Instance-Identifier AVP.	The SAPC returns a CCA message indicating an error.	The Result-Code AVP is set to DIAMETER_MISSING_AVP (5005).
The SAPC receives a CCR-U message for an application start event with the TDF-Application-Instance-Identifier AVP, but the CCR-U message for the corresponding stop event does not have it. (1)	The SAPC returns a CCA message indicating an error.	The Result-Code AVP is set to DIAMETER_MISSING_AVP (5005).
The SAPC receives a CCR-U message for an application start event with the TDF-Application-Instance-Identifier AVP, and another CCR-U with the application start is received without the TDF-Application-Instance-Identifier AVP. (2)	The SAPC returns a CCA message indicating an error.	The Result-Code AVP is set to DIAMETER_MISSING_AVP (5005).
The SAPC receives a CCR-U but the SAPC does not have an existing Sd session	The SAPC rejects the transaction and returns a CCA message indicating an error.	The Result-Code AVP is set to DIAMETER_UNKNOWN_SESSION_ID (5002).

- (1) If the SAPC receives a CCR-U message for an application start event without the TDF-Application-Instance-Identifier AVP, but the corresponding stop event includes it, the SAPC ignores the application stop event trigger, but reauthorizes the session.
- (2) If the SAPC receives a CCR-U message for an application start event without the TDF-Application-Instance-Identifier AVP and another CCR-U with the application start is received with the TDF-Application-Instance-Identifier AVP, then this CCR-U is ignored, not rejected.

4.4.5 Error Handling at Dedicated Bearer Reported as Inactive by PCEF

Upon receiving a Gx CCR-U message notifying about the termination of a dedicated bearer, the SAPC removes the dynamic service from the Gx IP-CAN session and performs policy evaluation ignoring the affected PCC rules.

The SAPC can reauthorize the Sd by installing or removing ADC rules, if this depends on the services running on the IP-CAN session. This is especially important in those scenarios where the TDF is performing charging for a detected application. If a dedicated bearer is created for the service data flow of this application, or the application receives a QoS treatment, based on the default bearer characteristics, the charging can be different.