ETSI TS 129 513 V15.0.0 (2018-06)

5G;
5G System;
Policy and Charging Control signalling flows and QoS parameter mapping;
Stage 3
(3GPP TS 29.513 version 15.0.0 Release 15)

Reference
DTS/TSGC-0329513vf00

Keywords
5G

ETSI

650 Route des Lucioles
F-06921 Sophia Antipolis Cedex - FRANCE

Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Siret N° 348 623 562 00017 - NAF 742 C
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° 7803/88

Intellectual Property Rights

Essential patents

IPRs essential or potentially essential to normative deliverables may have been declared to ETSI. The information pertaining to these essential IPRs, if any, is publicly available for **ETSI members and non-members**, and can be found in ETSI SR 000 314: *"Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards"*, which is available from the ETSI Secretariat. Latest updates are available on the ETSI Web server (https://ipr.etsi.org/).

Pursuant to the ETSI IPR Policy, no investigation, including IPR searches, has been carried out by ETSI. No guarantee can be given as to the existence of other IPRs not referenced in ETSI SR 000 314 (or the updates on the ETSI Web server) which are, or may be, or may become, essential to the present document.

Trademarks

The present document may include trademarks and/or tradenames which are asserted and/or registered by their owners. ETSI claims no ownership of these except for any which are indicated as being the property of ETSI, and conveys no right to use or reproduce any trademark and/or tradename. Mention of those trademarks in the present document does not constitute an endorsement by ETSI of products, services or organizations associated with those trademarks.

Foreword

This Technical Specification (TS) has been produced by ETSI 3rd Generation Partnership Project (3GPP).

The present document may refer to technical specifications or reports using their 3GPP identities, UMTS identities or GSM identities. These should be interpreted as being references to the corresponding ETSI deliverables.

The cross reference between GSM, UMTS, 3GPP and ETSI identities can be found under http://webapp.etsi.org/key/queryform.asp.

Modal verbs terminology

In the present document "**shall**", "**shall not**", "**should**", "**should not**", "**may**", "**need not**", "**will**", "**will not**", "**can**" and "**cannot**" are to be interpreted as described in clause 3.2 of the ETSI Drafting Rules (Verbal forms for the expression of provisions).

"**must**" and "**must not**" are **NOT** allowed in ETSI deliverables except when used in direct citation.

Contents

Foreword

This Technical Specification has been produced by the 3rd Generation Partnership Project (3GPP).

The contents of the present document are subject to continuing work within the TSG and may change following formal TSG approval. Should the TSG modify the contents of the present document, it will be re-released by the TSG with an identifying change of release date and an increase in version number as follows:

Version x.y.z

where:

- x the first digit:
  - 1 presented to TSG for information;
  - 2 presented to TSG for approval;
  - 3 or greater indicates TSG approved document under change control.
- y the second digit is incremented for all changes of substance, i.e. technical enhancements, corrections, updates, etc.
- z the third digit is incremented when editorial only changes have been incorporated in the document.

1 Scope

The present document specifies detailed call flows of Policy and Charging Control (PCC) over the Npcf, Nsmf, Namf, Nudr, Nnef and Nnwdaf service-based interfaces and their relationship with the flow level signalling in 5G system.

NOTE: The call flows depicted in this Technical Specification do not cover all traffic cases.

The stage 2 definition and procedures of PCC are contained in 3GPP TS 23.502 [3] and 3GPP TS 23.503 [4]. The 5G System Architecture is defined in 3GPP TS 23.501 [2].

Detailed stage 3 procedures are provided in 3GPP TS 29.507 [7], 3GPP TS 29.508 [8], 3GPP TS 29.512 [9], 3GPP TS 29.514 [10], 3GPP TS 29.520 [11], 3GPP TS 29.519 [12] 3GPP TS 29.521 [22], 3GPP TS 29.594 [23], 3GPP TS 29.522 [24], 3GPP TS 29.551 [25] and 3GPP TS 29.554 [26].

The Technical Realization of the Service Based Architecture and the Principles and Guidelines for Services Definition of the 5G System are specified in 3GPP TS 29.500 [5] and 3GPP TS 29.501 [6].

The present specification also describes the PCC reference architectures for non-roaming and roaming scenarios in 5G system.

The present specification also describes the mapping of QoS parameters at AF, PCF and SMF.

The present specification also describes the session binding at PCF, and the QoS flow binding at SMF.

The present specification also describes the PCF addressing.

2 References

The following documents contain provisions which, through reference in this text, constitute provisions of the present document.

- References are either specific (identified by date of publication, edition number, version number, etc.) or non-specific.
- For a specific reference, subsequent revisions do not apply.
- For a non-specific reference, the latest version applies. In the case of a reference to a 3GPP document (including a GSM document), a non-specific reference implicitly refers to the latest version of that document *in the same Release as the present document*.

[1] 3GPP TR 21.905: "Vocabulary for 3GPP Specifications".

[2] 3GPP TS 23.501: "System Architecture for the 5G System; Stage 2".

[3] 3GPP TS 23.502: "Procedures for the 5G System; Stage 2".

[4] 3GPP TS 23.503: "Policy and Charging Control Framework for the 5G System; Stage 2".

[5] 3GPP TS 29.500: "5G System; Technical Realization of Service Based Architecture; Stage 3".

[6] 3GPP TS 29.501: "5G System; Principles and Guidelines for Services Definition; Stage 3".

[7] 3GPP TS 29.507: "5G System; Access and Mobility Policy Control Service; Stage 3".

[8] 3GPP TS 29.508: "5G System; Session Management Event Exposure Service; Stage 3".

[9] 3GPP TS 29.512: "5G System; Session Management Policy Control Service; Stage 3".

[10] 3GPP TS 29.514: "5G System; Policy Authorization Service; Stage 3".

[11] 3GPP TS 29.520: "5G System; Network Data Analytics Services; Stage 3".

[12] 3GPP TS 29.519: "5G System; Usage of the Unified Data Repository Service for Policy Data, Application Data and Structured Data for Exposure; Stage 3".

[13] 3GPP TS 23.203: "Policies and Charging control architecture; Stage 2".

[14] 3GPP TS 26.114: "IP Multimedia Subsystem (IMS); Multimedia Telephony; Media handling and interaction".

[15] 3GPP TS 29.201: "Representational State Transfer (REST) reference point between Application Function (AF) and Protocol Converter (PC)".

[16] IETF RFC 4566: "SDP: Session Description Protocol".

[17] 3GPP TS 26.247: "Transparent end-to-end Packet-switched Streaming Service (PSS) Progressive Download and Dynamic Adaptive Streaming over HTTP (3GP-DASH)".

[18] 3GPP TS 29.214: "Policy and Charging Control over Rx reference point".

[19] 3GPP TS 26.234: "End-to-end transparent streaming service; Protocols and codecs".

[20] 3GPP2 C.S0046-0 v1.0: "3G Multimedia Streaming Services".

[21] 3GPP2 C.S0055-A v1.0: "Packet Switched Video Telephony Services (PSVT/MCS)".

[22] 3GPP TS 29.521: "5G System; Binding Support Management Service; Stage 3".

[23] 3GPP TS 29.594: "5G System; Spending Limit Control Service; Stage 3".

[24] 3GPP TS 29.522: "5G System; Network Exposure Function Northbound APIs; Stage 3".

[25] 3GPP TS 29.551: "5G System; Packet Flow Description Management Service; Stage 3".

[26] 3GPP TS 29.554: "5G System; Background Data Transfer Policy Control Service; Stage 3".

[27] 3GPP TS 29.504: "5G System; Unified Data Repository Services; Stage 3".

[28] 3GPP TS 32.240: "Charging management; Charging architecture and principles".

3 Definitions, symbols and abbreviations

3.1 Definitions

For the purposes of the present document, the terms and definitions given in 3GPP TR 21.905 [1] and the following apply. A term defined in the present document takes precedence over the definition of the same term, if any, in 3GPP TR 21.905 [1].

3.2 Abbreviations

For the purposes of the present document, the abbreviations given in 3GPP TR 21.905 [1] and the following apply. An abbreviation defined in the present document takes precedence over the definition of the same abbreviation, if any, in 3GPP TR 21.905 [1].

5GC	5G Core Network
5QI	5G QoS Identifier
AF	Application Function
AMF	Access and Mobility Management Function
ARP	Allocation and Retention Priority
BSF	Binding Support Function
CHF	Charging Function
LBO	Local Breakout
MBR	Maximum Bitrate
MPD	Media Presentation Description
MPS	Multimedia Priority Service
NEF	Network Exposure Function
NRF	Network Repository Function
NWDAF	Network Data Analytics Function
PCC	Policy and Charging Control

PCF	Policy Control Function
QoS	Quality of Service
SDP	Session Description Protocol
SMF	Session Management Function
UDR	Unified Data Repository
UPF	User Plane Function

4 Reference architecture

The policy framework functionality in 5G is comprised by the functions of the Policy Control Function (PCF), the policy and charging enforcement functionality supported by SMF and UPF, the access and mobility policy enforcement functionality supported by the AMF, the Network Data Analytics Function (NWDAF), the Network Exposure Function (NEF), the Charing Function (CHF), the Unified Data Repository (UDR) and the Application Function (AF).
3GPP TS 23.503 [4] specifies the 5G policy framework stage 2 functionality.

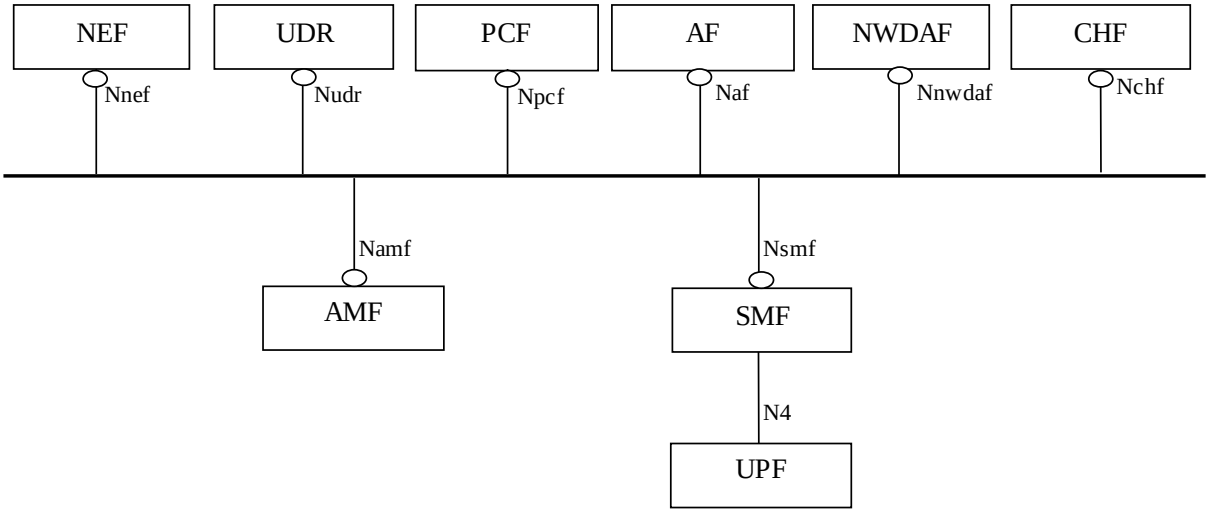


Figure 4.1-1a: Overall non-roaming 5G Policy framework architecture (service based representation)

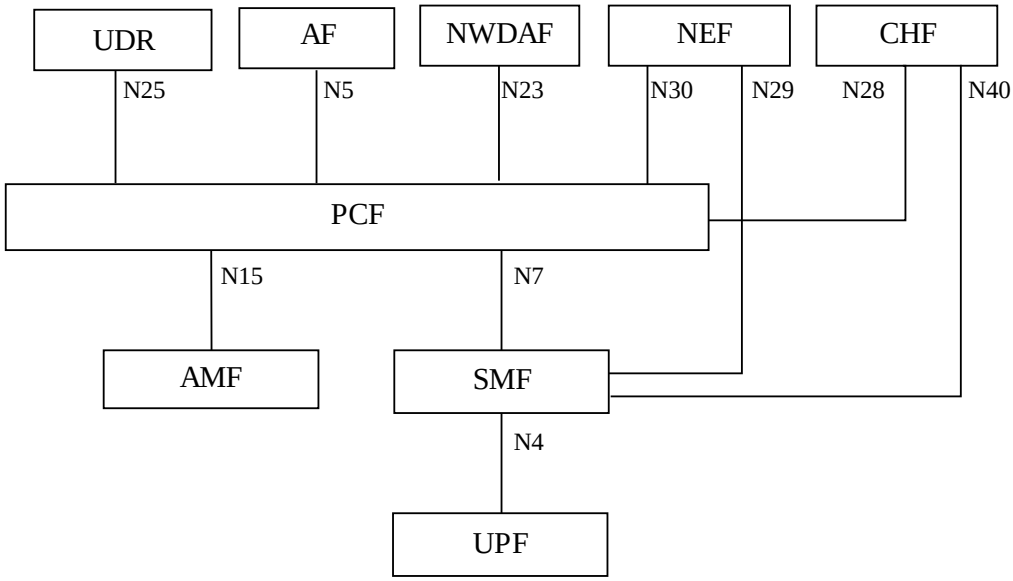


Figure 4.1-1b: Overall non-roaming 5G Policy framework architecture (reference point representation)

NOTE 1: The N4 interface is not part of the Policy Framework architecture but shown in the figures for completeness.

NOTE 2: The interactions between the PCF and the AF need to provide the Rx functionalities as defined in 3GPP TS 23.203 [13] to allow the 5GC to interwork with the AFs related to the existing services e.g. IMS based services and Mission critical services.

The Nchf service for online and offline charging consumed by the SMF is defined in 3GPP TS 32.240 [28].

The Nchf service for Spending Limit Control consumed by the PCF is defined in 3GPP TS 29.594 [23].

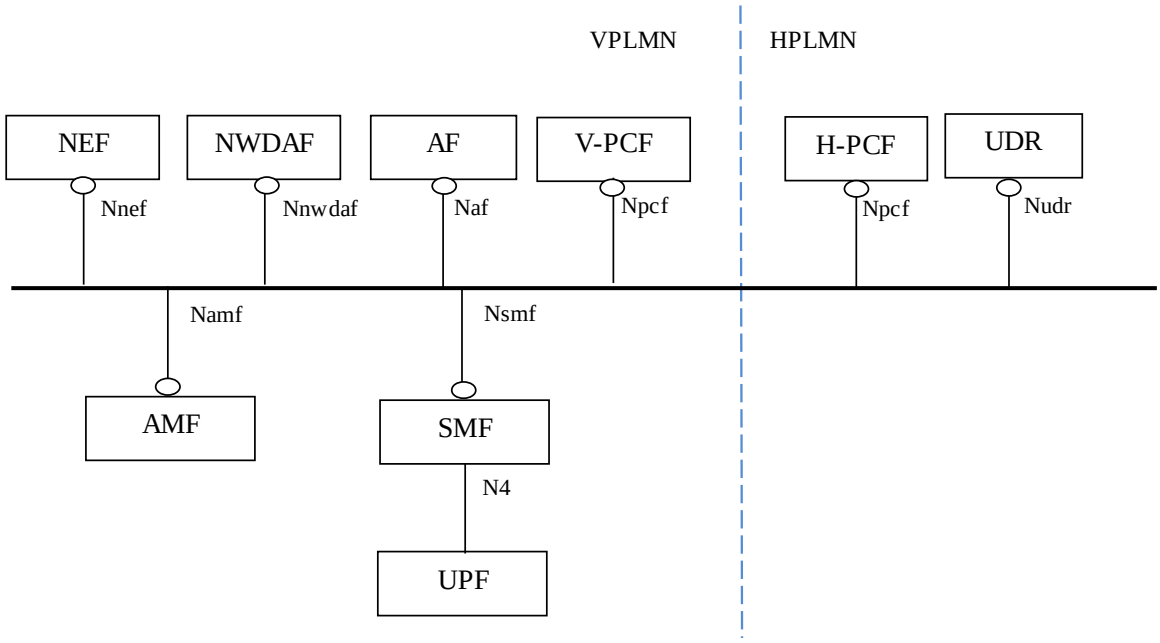


Figure 4.1-2a: Overall roaming policy framework architecture - LBO (service based representation)

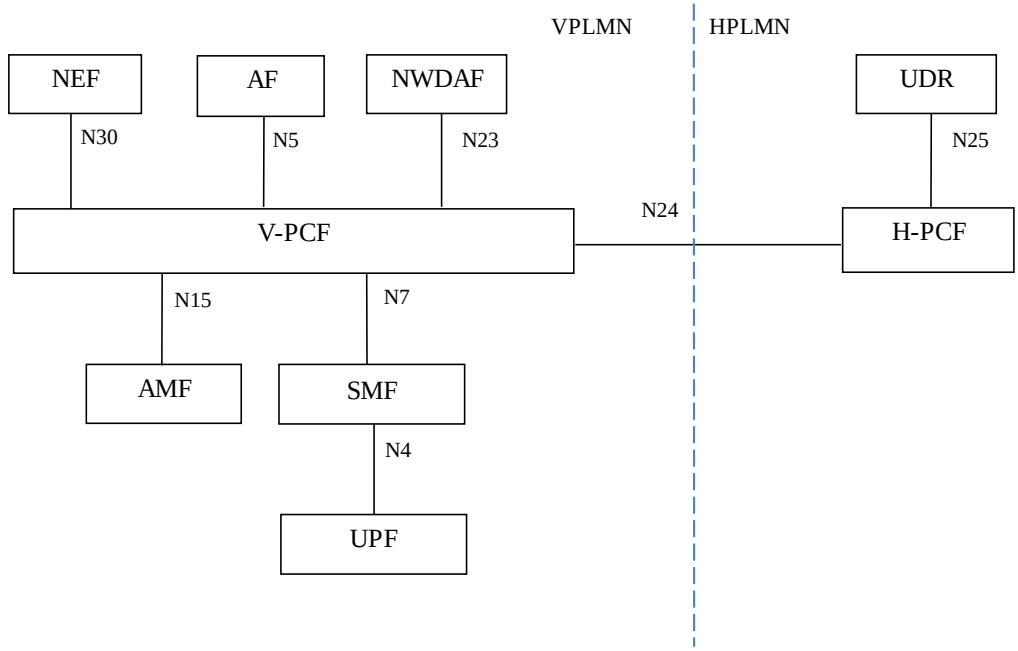


Figure 4.1-2b: Overall roaming policy framework architecture - LBO (reference point representation)

NOTE 3: In the LBO scenario, the PCF in the VPLMN may interact with the AF in order to generate PCC rules for services delivered via the VPLMN. The PCF in the VPLMN uses locally configured policies according to the roaming agreement with the HPLMN operator as input for PCC rule generation. The PCF in VPLMN has no access to subscriber policy information from the HPLMN to retrieve input for PCC Rule generation. The interactions between the PCF in the VPLMN and the PCF in the HPLMN through the Npcf service based interface enables the PCF in the HPLMN to provision UE policies to the PCF in the VPLMN, as described in 3GPP TS 23.503 [4] subclause 5.2.5.

NOTE 4: In the LBO scenario, AF requests targeting a DNN (and slice) and / or a group of UEs are stored in the UDR by the NEF. The PCF in the VPLMN subscribes to and get notification from the UDR in the VPLMN for those AF requests. Details are defined in subclause 5.6.7 of 3GPP TS 23.501[2].

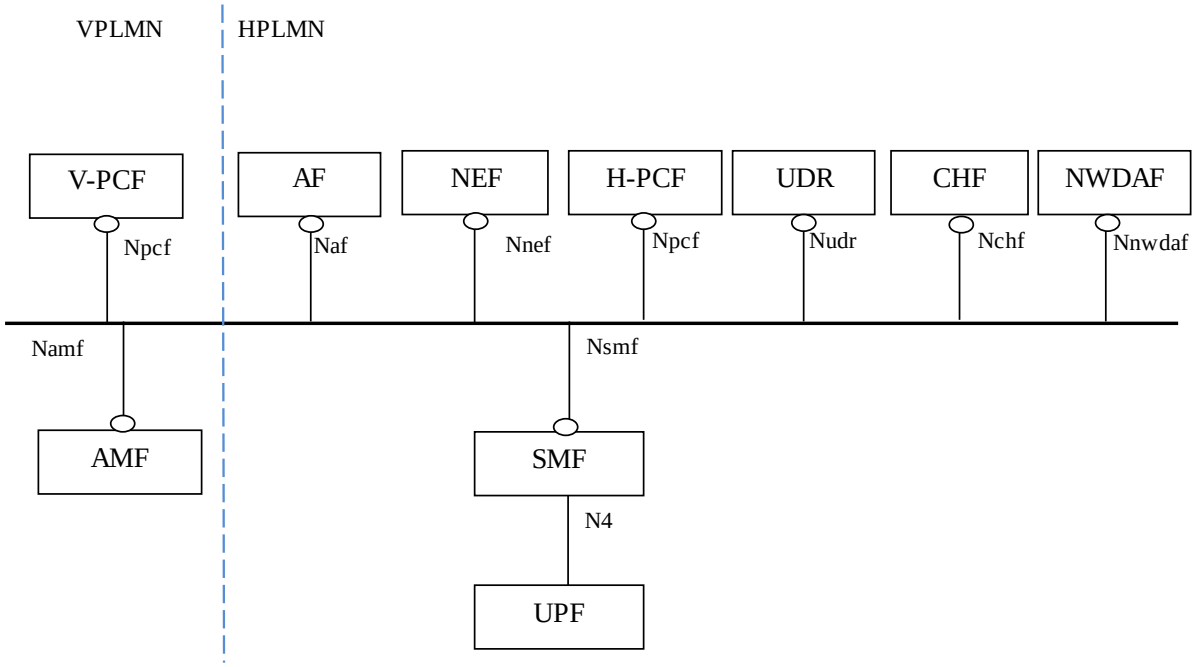


Figure 4.1-3a: Overall roaming policy framework architecture - home routed scenario (service based representation)

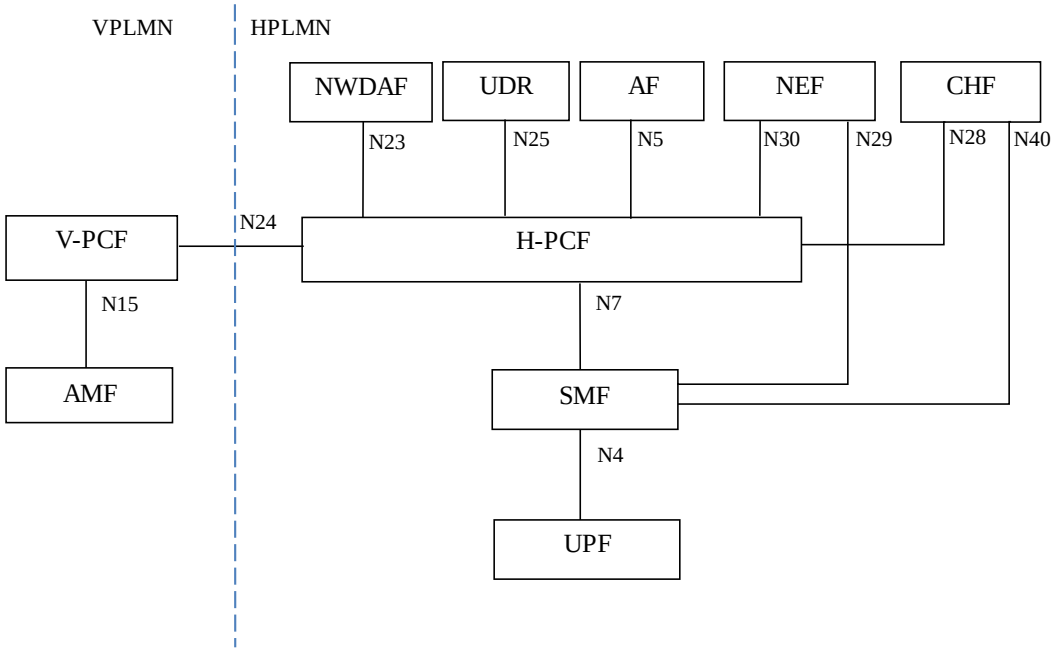


Figure 4.1-3b: Overall roaming policy framework architecture - home routed scenario (reference point representation)

5 Signalling Flows for the Policy Framework

5.1 AM Policy Association Management

5.1.1 AM Policy Association Establishment

This procedure concerns the following scenarios:

1. UE initial registration with the network.
2. The AMF re-allocation without PCF change in handover procedure and registration procedure.
3. The AMF re-allocation with PCF change in handover procedure and registration procedure.

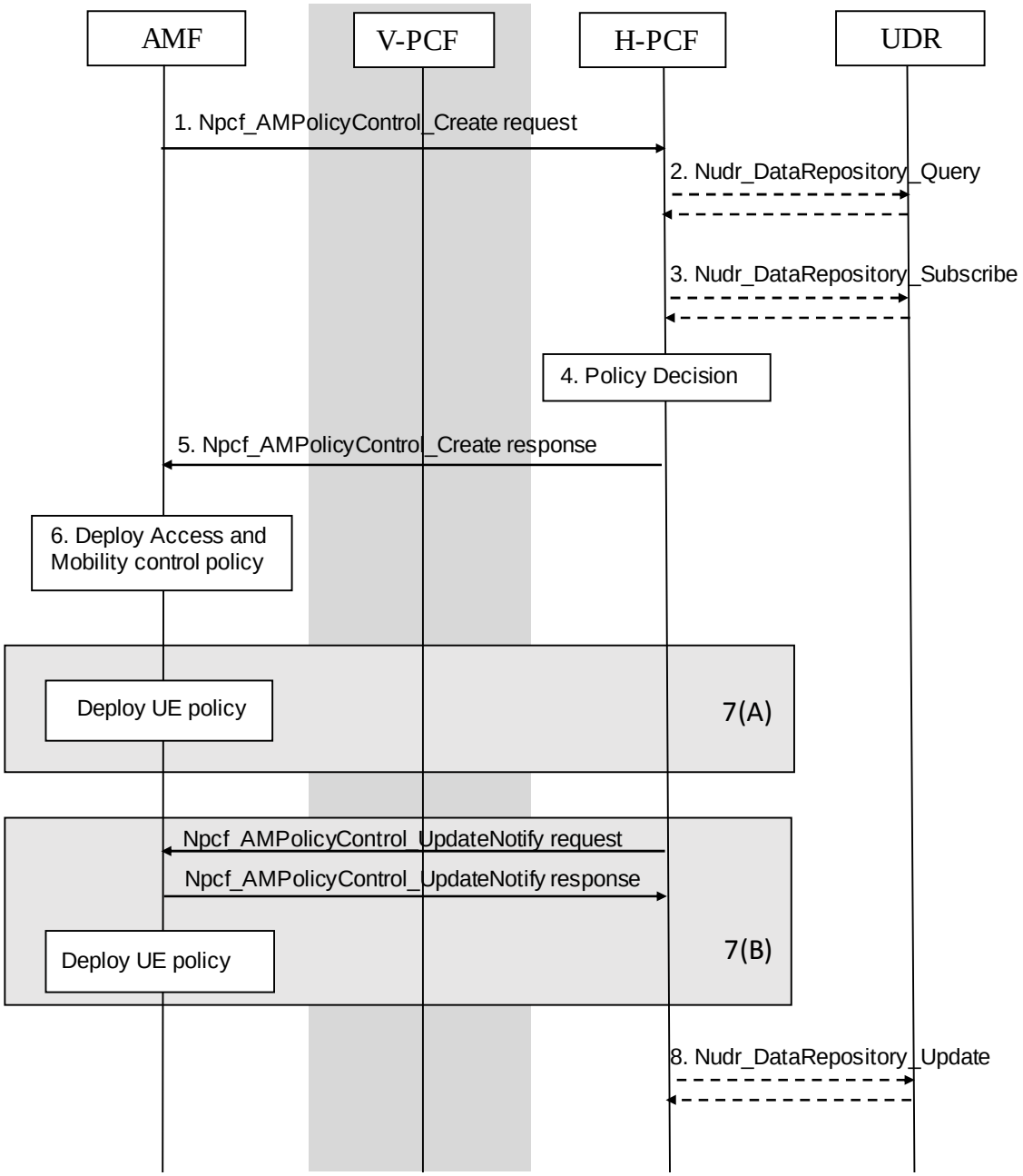


Figure 5.1.1-1 AM Policy Association Establishment procedure

This procedure concerns both roaming and non-roaming scenarios.

In the non-roaming case the V-PCF is not involved and the role of the H-PCF is performed by the PCF. For the roaming scenarios, the V-PCF interacts with the AMF.

1. The AMF receives the registration request from the AN. Based on local policy, the AMF selects to contact the (V-) PCF to create the policy association with the (V-) PCF and to retrieve the UE policy and/or Access and Mobility control policy. The AMF selects the PCF as described in subclause 8.2 and invokes the Npcf_AMPolicyControl_Create service operation by sending the HTTP POST request to the resource URI "{apiRoot}/npcf-am-policy-control/v1/policies". The request operation provides the SUPI, and if received from the UDM, the Service Area Restrictions, RFSP index, and GPSI, and may provide the access type, the PEI if received in the AMF, the User Location Information if available, the UE Time Zone if available, Serving Network, RAT type, the list of stored PSIs. The request includes a Notification URI to indicate to the PCF where to send a notification when the policy is updated. If the AMF receives a PCF ID and decides to contact the (V-) PCF identified by the PCF ID, the AMF may also provide the PCF ID.

   In roaming scenario, the AMF may provide to the V-PCF the PCF ID of the selected H-PCF. The V-PCF contacts the H-PCF.

NOTE 1: The UE provides the list of PSIs that are currently stored in the UE (UE policies pre-configured in the UE are not included in this message).

2. If the (H-)PCF does not have the subscription data or the latest list of PSIs for the UE, it invokes the Nudr_DataRepository_Query service operation and includes in the request to the UDR the SUPI, PCF Identifier, the Data Set Identifier (Policy Data) and the Data Subset Identifier (UE context policy control).

   The UDR responds to the (H-)PCF with the latest PSIs and/or the subscription data that may include UE policy and Access and Mobility control policy.

3. The (H-)PCF may request notifications from the UDR on changes in the subscription information by invoking Nudr_DataRepository_Subscribe service operation. The request operation provides the SUPI , PCF Identifier, the Data Set Identifier (Policy Data), the Data Subset Identifier (UE context policy control), and Event Reporting Information (continuous reporting) . The (H-)PCF also supplies a Notification URI to the UDR to indicate where to send a notification, and a Notification Correlation ID to correlate notifications with this subscription.

4. The PCF makes the requested policy decision including Access and Mobility control policy information, and may determine applicable Policy Control Request Trigger(s). The PCF compares the stored list of PSIs included in the UE policy information, received from the UE, with the latest list of PSIs to determine whether and which UE policy information have to be included in the answer to the AMF.

5. The PCF sends an HTTP "201 Created" response to the AMF with the determined policies as described in subclause 4.2.2 of 3GPP TS 29.507 [7]:

   - UE policy including UE Access Network discovery and selection policies and/or UE Route Selection Policies (URSP) of the UE; and/or

   - Access and Mobility control Policy including Service Area Restrictions, and/or a RAT Frequency Selection Priority (RFSP) Index; and/or

   - Policy Control Request Trigger parameters;

   In roaming scenario, the H-PCF responds to the V-PCF including UE policy information and/or Policy Control Request Trigger, then the V-PCF responds to the Npcf_AMPolicyControl_Create service operation, and provides to the AMF the Access and Mobility control policy information, UE policy information and the Policy Control Request Trigger parameters.

   If the PCF provides the Access and Mobility control policy, step 6 is executed. If the PCF provides the UE policy, step 7 is executed, and the PCF checks if the size of these policies exceeds a predefined limit.

NOTE 2: NAS messages from AMF to UE cannot exceed the maximum size limit allowed in NG-RAN (PDCP layer), so the predefined size limit in PCF is related to that limitation.

   - If the size is under the limit then the Access and Mobility control policy and UE policy information are included in the Npcf_AMPolicyControl_Create response.

   - If the size exceeds the predefined limit the PCF only includes Access and Mobility control policy in the Npcf_AMPolicyControl_Create response. The PCF splits the UE policy information in smaller logical

independent UE policy information and ensures the size of each is under the predefined limit. Each UE policy information will be then sent in additional Npcf_AMPolicyControl_UpdateNotify service operations as described in step 7(B).

NOTE 3: The mechanism used to split the UE policy information is described in 3GPP TS 29.507 [7].

NOTE 4: The PCF can reject the AM Policy Association establishment, e.g. the PCF cannot obtain the subscription-related information from the UDR and the PCF cannot make the policy decisions, as described in 3GPP TS 29.512 [9]. In this case, the remaining steps in this procedure are not followed.

6. The AMF deploys the Access and Mobility control policy information which includes storing the Service Area Restrictions, provisioning the Service Area Restrictions to the UE and provisioning the RFSP index and Service Area Restrictions to the NG-RAN.

7(A). If the PCF included UE policy information in the answer of Npcf_AMPolicyControl_Create service operation in step 5, the AMF deploys the UE policy information to the UE. This UE policy information indicates a new set of UE policy to be added in UE or to delete/modify an existing set of UE policy in UE.

7(B). If the PCF applied splitting in step 5 it invokes Npcf_AMPolicyControl_UpdateNotify service operation to the AMF by sending the HTTP POST request to the resource URI "{Notification URI}/update" with one piece of UE policy information, which indicates a new set of UE policy to be added in UE or to delete/modify an existing set of UE policy in UE.

The AMF sends an HTTP "204 No Content" response to the PCF and deploys the UE policy information to the UE.

NOTE 5: The AMF handles transparently the UE policy information received from the PCF.

8. The (H-) PCF maintains the latest list of UE policy information delivered to the UE updated in step 7 and updates UE policy including the latest list of PSIs in the UDR by invoking Nudr_DataRepository_Update service operation.

NOTE 6: After this step the PCF can subscribe to AMF events for the UE.

5.1.2 AM Policy Association Modification

5.1.2.1 AM Policy Association Modification initiated by the AMF

This procedure is performed when a Policy Control Request Trigger condition is met.

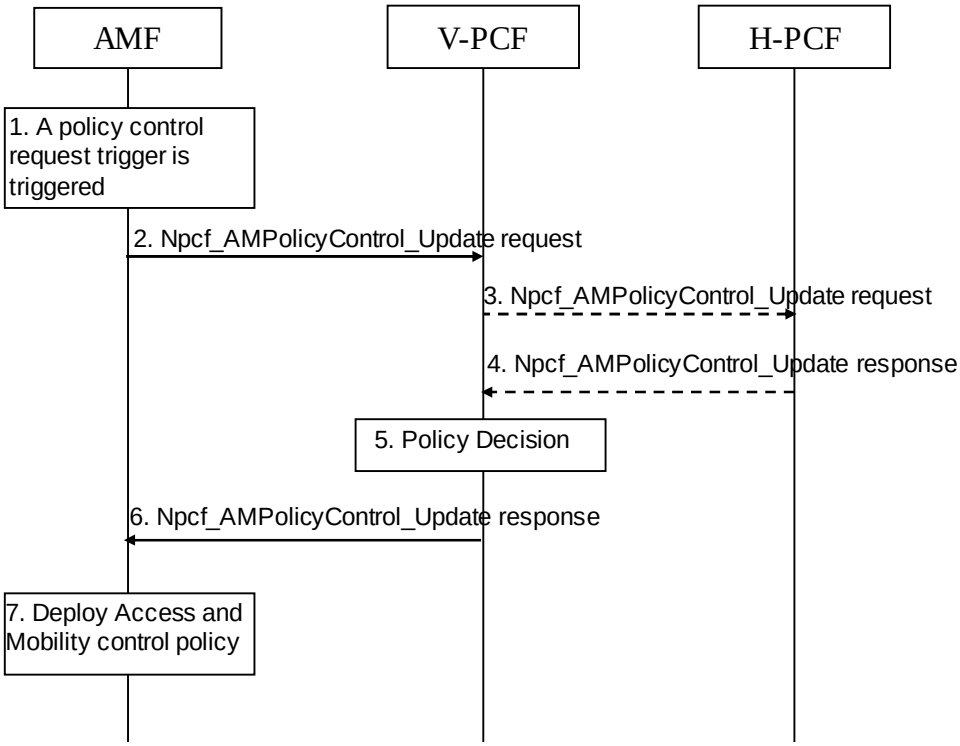


Figure 5.1.2.1-1 AMF-initiated AM Policy Association Modification procedure

This procedure concerns both roaming and non-roaming scenarios.

In the non-roaming case the V-PCF is not involved. In the roaming case, it is the V-PCF to make a final policy decision.

1. The AMF detects a Policy Control Request Trigger condition is met.
2. The AMF invokes the Npcf_AMPolicyControl_Update service operation to the (V-) PCF by sending the HTTP POST request to the resource URI "{apiRoot}/npcf-am-policy-control/v1/policies/{polAssoId}/update" with information on the conditions that have changed.
3. In the roaming case, if H-PCF has subscribed the policy control request trigger, the V-PCF by sending the HTTP POST request with "{apiRoot}/npcf-am-policy-control/v1/policies/{polAssoId}/update" as the resource URI to contact the H-PCF.
4. The H-PCF sends an HTTP "200 OK" response to the V-PCF with the updated Policy Control Request Trigger parameters.
5. The PCF stores the information received in step 2 and makes the policy decision.
6. The PCF sends an HTTP "200 OK" response to the AMF with the updated Access and Mobility control policy information and the updated Policy Control Request Trigger parameters.
7. The AMF deploys the Access and Mobility control policy, which includes storing the Service Area Restrictions, provisioning the Service Area Restrictions to the NG-RAN and UE, and provisioning the RFSP index to the NG-RAN.

5.1.2.2 AM Policy Association Modification initiated by the PCF

This procedure is performed when the UE policies and/or Access and Mobility control policies are changed.

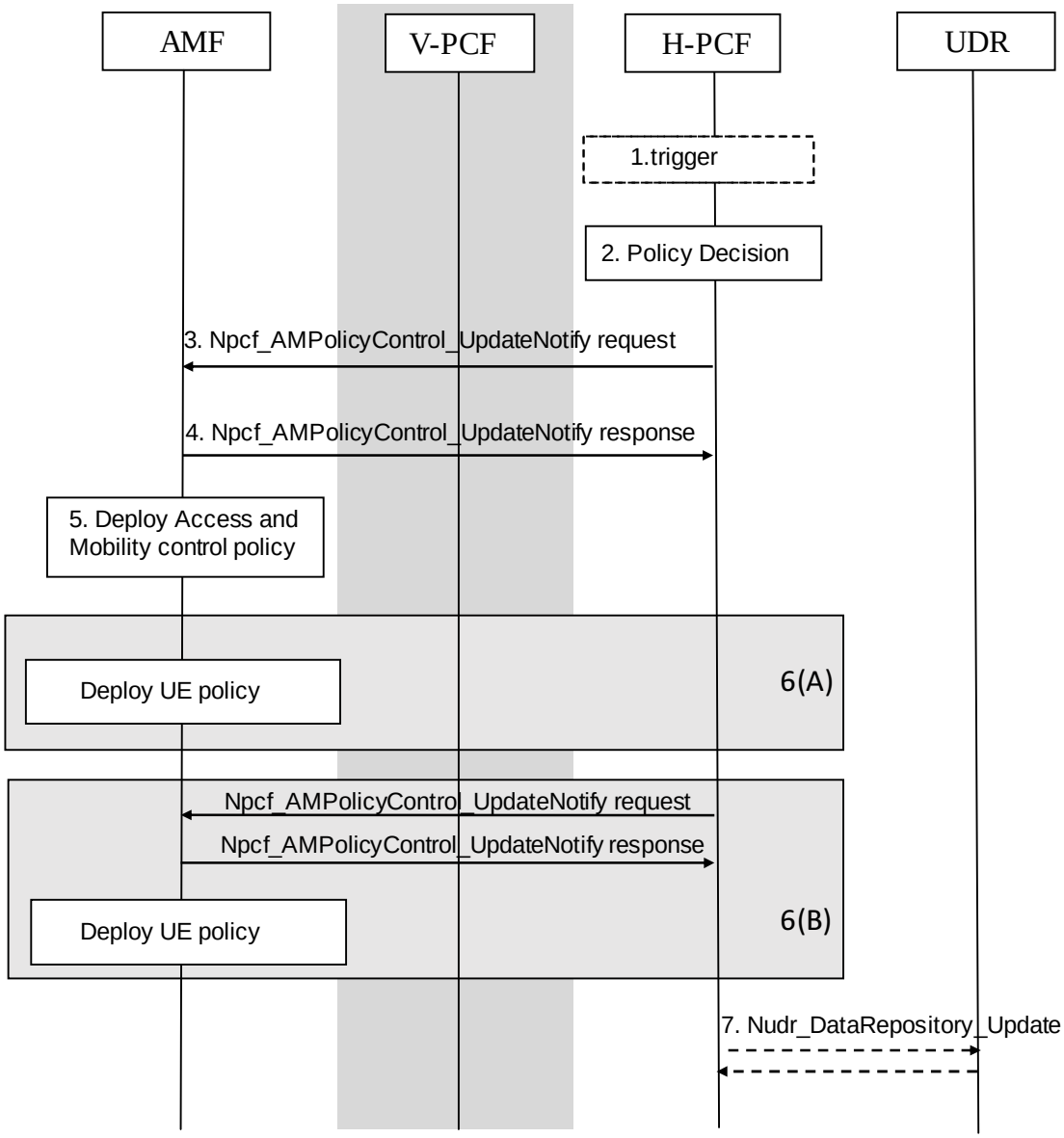


Figure 5.1.2.2-1 PCF-initiated AM Policy Association Modification procedure

This procedure concerns both roaming and non-roaming scenarios.

In the non-roaming case the V-PCF is not involved and the role of the H-PCF is performed by the PCF. In the roaming case, the H-PCF provides the UE policies to the AMF via V-PCF, and the V-PCF provides AMF Access and Mobility control policies to the AMF.

NOTE 1: The V-PCF stores the Access and Mobility control policy information provided to the AMF.

1. The (H-) PCF receives an external trigger, e.g. the subscriber policy data of a UE is changed, or the (V-) (H-)PCF receives an internal trigger, e.g. operator policy is changed, to re-evaluate Access and Mobility control policy and/or UE policy decision for a UE.

2. The PCF makes the policy decision including, UE policy and/or Access and Mobility control policy, and may determine applicable Policy Control Request Trigger(s). The H-PCF interacts with the V-PCF in roaming case.

3. The PCF invokes the Npcf_AMPolicyControl_UpdateNotify service operation by sending the HTTP POST request with "{Notification URI}/update" as the resource URI to the AMF that has previously subscribed, as described in subcaluse 4.2.4.2 of 3GPP TS 29.507 [7]. If this procedure is required to update Access and Mobility policy, the request operation also includes Service Area Restrictions and/or RFSP index, and step 5 is executed. If this procedure is required to update the UE policy, the request operation includes URSP and/or UE

Access Network discovery and selection policies, in this case step 6 is executed, and the PCF checks if the size of these policies exceeds a predefined limit.

NOTE 2: NAS messages from AMF to UE cannot exceed the maximum size limit allowed in NG-RAN (PDCP layer), so the predefined size limit in PCF is related to that limitation.

- If the size is under the limit then the Access and Mobility control policy and UE policy information are included in a single Npcf_AMPolicyControl_UpdateNotify service operation as described in step 3.

- If the size exceeds the predefined limit the PCF only includes Access and Mobility control policy in the Npcf_AMPolicyControl_UpdateNotify service operation. The PCF splits the UE policy information in smaller logical independent UE policy information and ensures the size of each is under the predefined limit. Each UE policy information will be then sent in additional Npcf_AMPolicyControl_UpdateNotify service operations as described in step 6(B).

NOTE 3: The mechanism used to split the UE policy information is described in 3GPP TS 29.507 [7].

4. The AMF sends an HTTP "204 No Content" response the PCF.

5. The AMF deploys the Access and Mobility control policy information which includes storing the Service Area Restrictions, provisioning the Service Area Restrictions to the UE and provisioning the RFSP index and Service Area Restrictions to the NG-RAN.

6(A). If the PCF included UE policy information in Npcf_AMPolicyControl_UpdateNotify service operation in step 3, the AMF deploys the UE policy information to the UE. This UE policy information indicates a new set of UE policy to be added in UE or to delete/modify an existing set of UE policy in UE.

6(B). If the PCF applied split in step 3 it invokes Npcf_AMPolicyControl_UpdateNotify service operation to the AMF by sending the HTTP POST request to the resource URI "{Notification URI}/update" withone piece of UE policy information, which indicates a new set of UE policy to be added in UE or to delete/modify an existing set of UE policy in UE.

The AMF sends an HTTP "204 No Content" response to the PCF.

NOTE 4: The AMF handles transparently the UE policy information received from the PCF.

7. The (H-) PCF maintains the latest list of UE policy information delivered to the UE updated in step 6 and updates UE policy including the latest list of PSIs in the UDR by invoking Nudr_DataRepository_Update service operation.

5.1.3 AM Policy Association Termination

5.1.3.1 AM Policy Association Termination initiated by the AMF

This procedure is performed when the UE deregisters from the network or when the old AMF removes the AM Policy Association during AMF relocation.

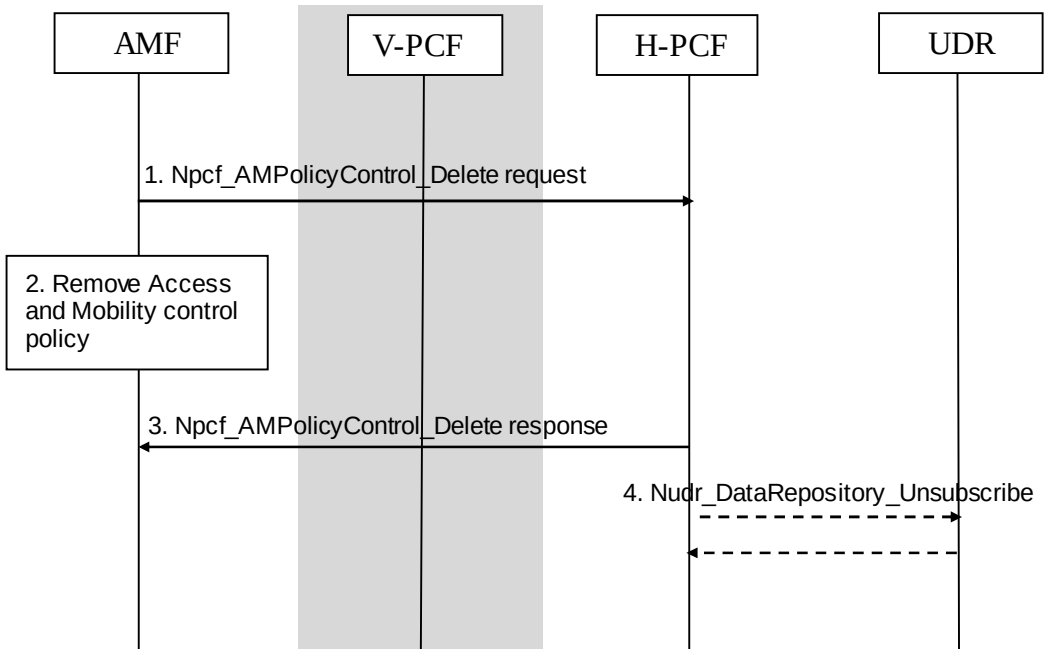


Figure 5.1.3.1-1 AMF-initiated AM Policy Association Termination procedure

This procedure concerns both roaming and non-roaming scenarios.

In the non-roaming case, the V-PCF is not involved and the role of the H-PCF is performed by the PCF. For the roaming scenarios, the V-PCF interacts with the AMF. The V-PCF contacts the H-PCF to request removing the AM Policy Association if an AM Policy Association was established with the H-PCF.

1. The AMF invokes the Npcf_AMPolicyControl_Delete service operation to delete the policy context in the (V-) PCF by sending the HTTP DELETE request to the resource URI "{apiRoot}/npcf-am-policy-control/v1/policies/{polAssoId}". The V-PCF may interact with the H-PCF.

2. The AMF removes the UE context for this UE, including the Access and Mobility Control Policy related to the UE and policy control request triggers.

3. The PCF removes the policy context for the UE and sends an HTTP "204 No Content" response to the AMF.

4. The (H-) PCF unsubscribes the notification of subscriber policy data modification from the UDR by invoking Nudr_DataRepository_Unsubscribe service operation if it has subscribed such notification. The request includes Subscription Correlation Id.

   The UDR acknowledges to the PCF with the result (success/failure) of the Nudr_DataRepository_Unsubscribe service operation.

5.1.3.2 AM Policy Association Termination initiated by the PCF

This procedure is performed when the UDR notifies the PCF that the policy profile is removed.

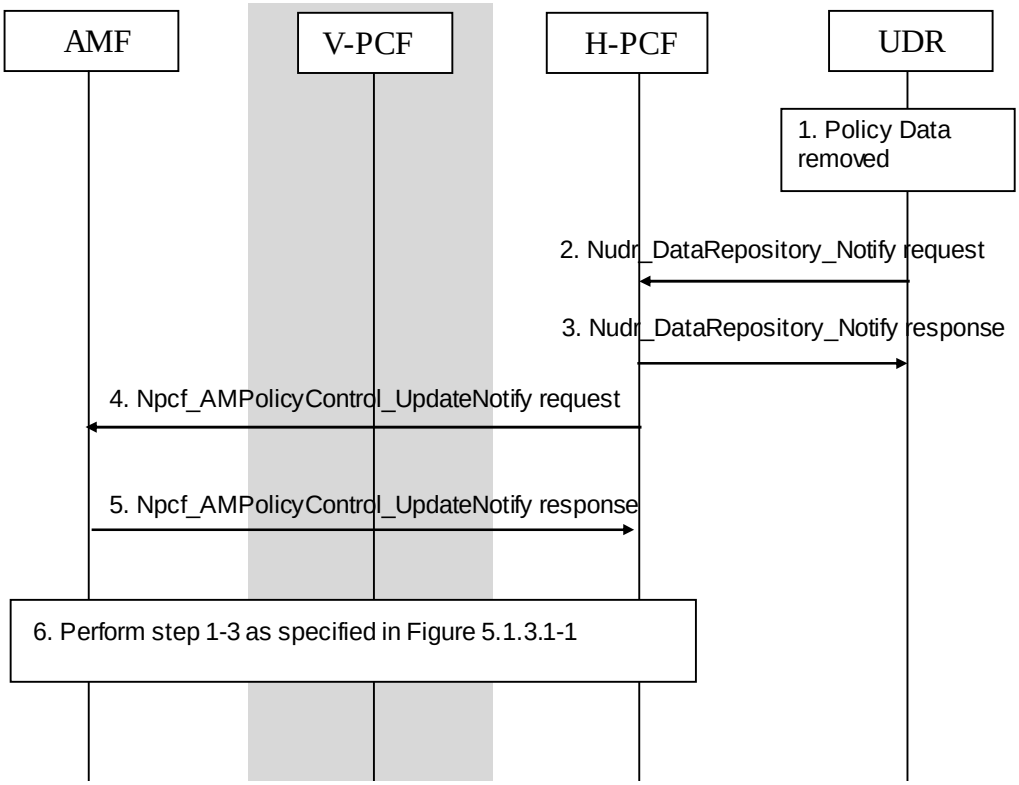


Figure 5.1.3.2-1 PCF-initiated AM Policy Association Termination procedure

This procedure concerns both roaming and non-roaming scenarios.

In the non-roaming case, the V-PCF is not involved and the role of the H-PCF is performed by the PCF. For the roaming scenarios, the H-PCF interacts with the V-PCF to request removing the AM Policy Association.

1. The subscriber policy control data is removed from the UDR.
2. The UDR sends the Nudr_DataRepository_Notify service operation to notify the PCF that the policy profile is removed if PCF has subscribed such notification. The serivce request includes the SUPI, the Notification Correlation ID, the Data Set Identifier, the Data Subset Identifier and the Updated Data including empty "Policy Data" or empty "UE context policy control".
3. The PCF sends the response to the Nudr_DataRepository_Notify service operation.
4. The PCF may, depending on operator policies, send the Npcf_AMPolicyControl_UpdateNotify service operation to the AMF of the removal of the Access and Mobility control policy control information. The request operation is sent by the HTTP POST request to the resource URI "{Notification URI}/terminate" as described in subcaluse 4.2.4.3 of 3GPP TS 29.507 [7].

   Alternatively, the PCF may decide to maintain the Policy Association if a default profile is applied, and then step 4 through 6 are not executed.
5. The AMF sends an HTTP "204 No Content" response to the PCF.
6. Step 1 through step 3 as specified in Figure 5.1.3.1-1 are executed.

5.2 SM Policy Association Management

5.2.1 SM Policy Association Establishment

This clause is applicable if a new SM Policy Association is being established.

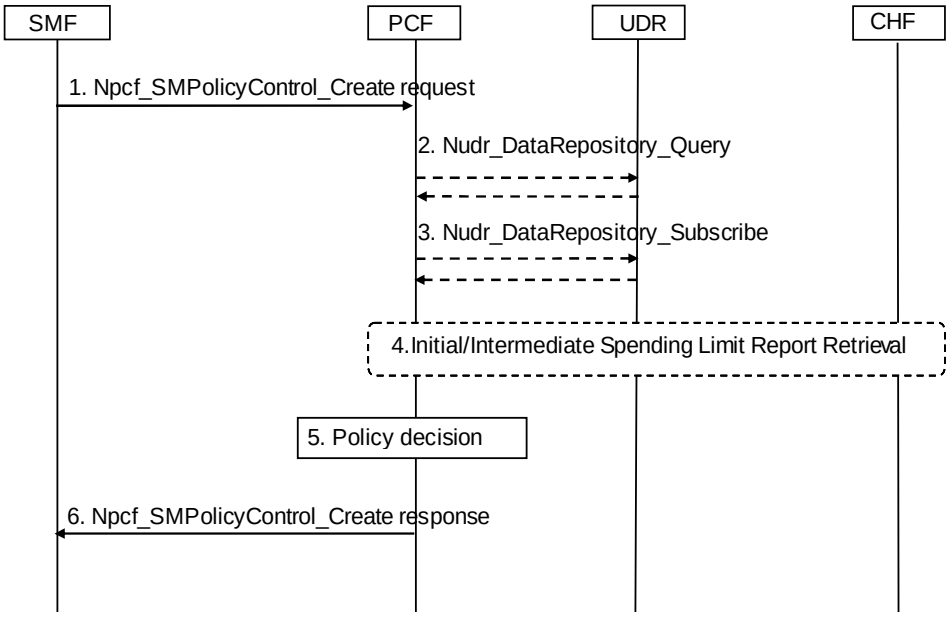


Figure 5.2.1-1: SM Policy Association Establishment procedure

This procedure concerns both roaming and non-roaming scenarios.

In the home routed roaming case, the PCF acts as the H-PCF. In the LBO roaming case, the PCF acts as the V-PCF, and the step 2 to 4 shall be skipped.

1. The SMF receives a PDU session establishment request from the UE. The SMF selects the PCF as described in subclause 8.3 and invokes the Npcf_SMPolicyControl_Create service operation by sending the HTTP POST request to the resource URI "{apiRoot}/npcf-smpolicycontrol/v1/sm-policies". The request operation provides the SUPI, the PDU session ID, PDU Session Type, DNN, and S-NSSAI, and may provide the GPSI, the Internal Group Identifier, the Access Type, the IPv4 address or the IPv6 network prefix (if available), the PEI if received in the SMF, the User Location Information, the UE Time Zone, Serving Network, RAT type, charging information, the subscribed Session-AMBR and the subscribed default 5QI/ARP, if available. The request operation also includes a Notification URI to indicate to the PCF where to send a notification when the SM related policies are updated.

2. If PCF does not have the subscription data for the SUPI and DNN, the PCF invokes the Nudr_DataRepository_Query service operation to the UDR and includes the PCF Identifier, SUPI, the Data Set Identifier "Policy Data", and the Data Subset Identifier "PDU Session policy control".

   The UDR responds to the PCF with the policy control subscription data (see 3GPP TS 29.519 [12]).

3. The PCF may request notifications from the UDR on changes in the subscription information by invoking Nudr_DataRepository_Subscribe service operation. The request operation provides the PCF Identifier, SUPI, the Data Set Identifier "Policy Data", the Data Subset Identifier "PDU Session policy control", and Event Reporting Information (continuous reporting). A Notification URI is also provided to the UDR to indicate where to send a notification.

   The UDR acknowledges the subscription from the PCF.

4. If the PCF determines that the policy decision depends on the status of the policy counters available at the CHF, and such reporting is not established for the subscriber, the PCF initiates an Initial Spending Limit Report Retrieval as defined in subclause 5.3.2. If policy counter status reporting is already established for the subscriber, and the PCF determines that the status of additional policy counters are required, the PCF initiates an Intermediate Spending Limit Report Retrieval as defined in subclause 5.3.3.

5. The PCF makes the policy decision to determine the information provided in step 6.

6. The PCF sends an HTTP "201 Created" response to the SMF with the determined policies as described in subclause 4.2.2 of 3GPP TS 29.512 [9].

NOTE: After this step the PCF can subscribe to SMF events associated with the PDU Session.

5.2.2 SM Policy Association Modification

5.2.2.1 General

The following procedures concern both roaming and non-roaming scenarios.

In the LBO roaming case, the PCF acts as the V-PCF, and the V-PCF shall not contact the UDR/CHF. In the home routed roaming case, the PCF acts as the H-PCF and the H-PCF interacts with the H-SMF.

The SM Policy Association Modification procedure may be initiated either by the SMF or by the PCF.

NOTE: The following procedures cover both Npcf_PolicyAuthorization service operations over the N5 reference point and Rx interactions between AF and PCF. It is assumed that for the interactions between one AF and one PCF, only one of those possibilities is used. For details of Rx interface refer to 3GPP TS 29.214[18] and for details on the Npcf_PolicyAuthorization service refer to 3GPP TS 29.514[10].

Editor's note: How the AF supports the Ethernet PDU Session is FFS.

5.2.2.2 SM Policy Association Modification initiated by the PCF

5.2.2.2.1 Interactions between SMF, PCF and CHF

This procedure is performed when the PCF decides to modify policy decisions for a PDU session.

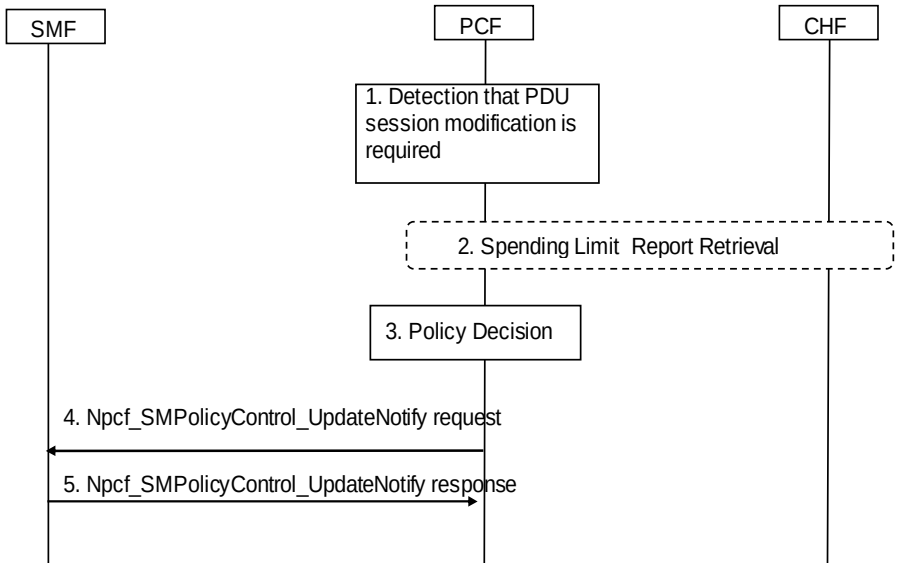


Figure 5.2.2.2-1 Interactions between SMF, PCF and CHF for PCF-initiated SM Policy Association Modification procedure

1. The PCF receives an internal or external trigger to re-evaluate PCC Rules and policy decision for a PDU Session. Possible external trigger events are described in clause 5.2.2.2.2. In addition, this procedure is triggered by the following cases:

   - The UDR notifies the PCF about a policy subscription change (e.g. change in MPS EPS Priority, MPS Priority Level and/or IMS Signalling Priority, or change in user profile configuration indicating whether supporting application detection and control).

   - The CHF provides a Spending Limit Report to the PCF as described in subclause 5.3.5.

2. If the PCF determines that the policy decision depends on the status of the policy counters available at the CHF and such reporting is not established for the subscriber, the PCF initiates an Initial Spending Limit Report as defined in subclause 5.3.2. If policy counter status reporting is already established for the subscriber, and the PCF decides to modify the list of subscribed policy counters, the PCF sends an Intermediate Spending Limit Report as defined in subclause 5.3.3. If the PCF decides to unsubscribe any future status notification of policy

counters, it sends a Final Spending Limit Report Request to cancel the request for reporting the change of the status of the policy counters available at the CHF as defined in subclause 5.3.4.

3. The PCF makes a policy decision. The PCF can determine that updated or new policy information need to be sent to the SMF.

4. The PCF invokes the Npcf_SMPolicyControl_UpdateNotify service operation by sending the HTTP POST request with "{Notification URI}/update" as the resource URI to the SMF that has previously subscribed.The request operation provides the PDU session ID and the updated policies, as described in subclause 4.2.4 of 3GPP TS 29.512[9].

5. The SMF sends an HTTP "200 OK" to the PCF.

5.2.2.2.2 Interactions between PCF, AF and UDR

5.2.2.2.2.1 AF Session Establishment

This procedure is performed when the AF/NEF requests to create an AF application session context for the requested service.

NOTE: The NEF acts as an AF to support the network exposure functionality.

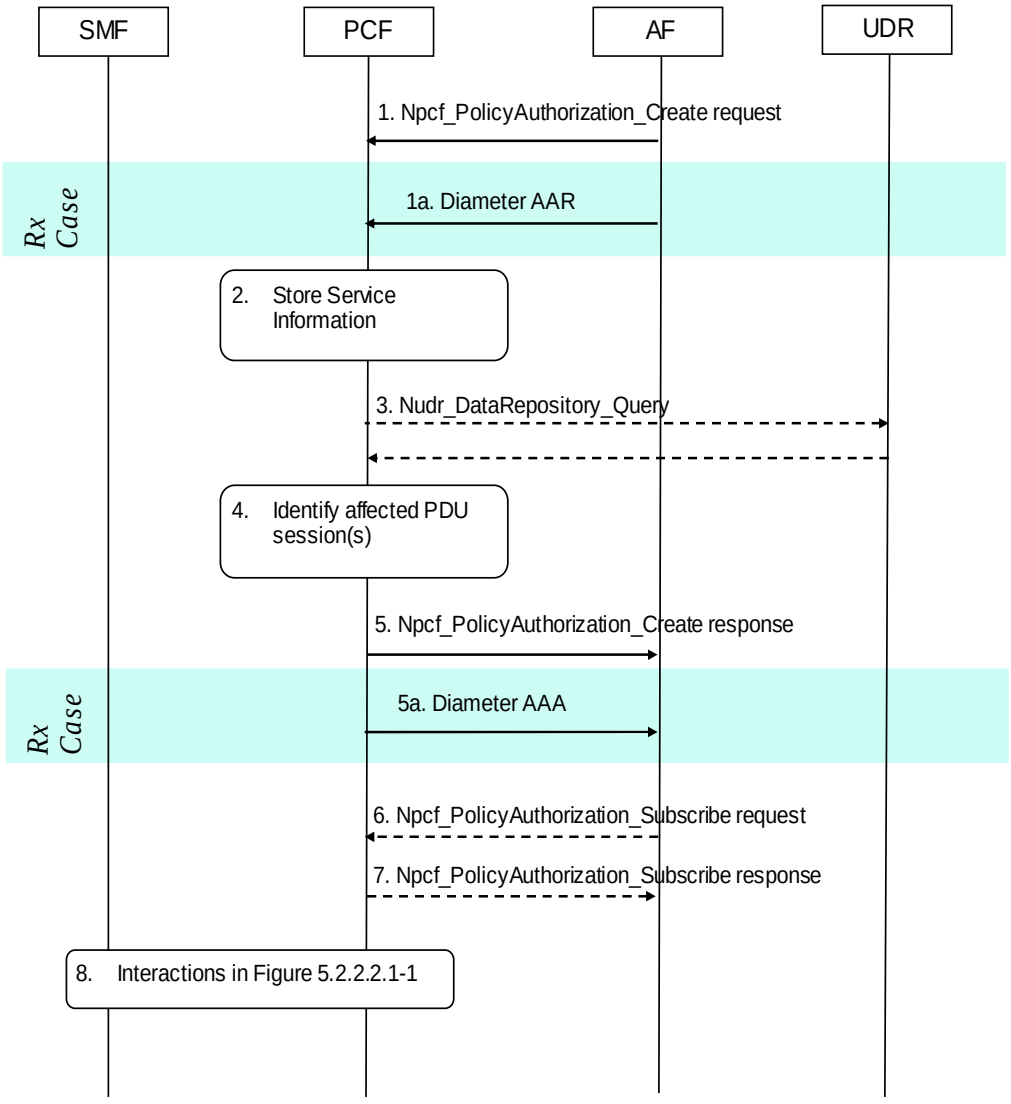


Figure 5.2.2.2.2.1-1 AF Session Establishment triggers PCF-initiated SM Policy Association Modification procedure

1. When the AF receives an internal or external trigger to set-up a new AF session, the AF invokes the Npcf_PolicyAuthorization_Create service operation by sending the HTTP POST request with "{apiRoot}/npcf-policyauthorization/v1/app-sessions" as the resource URI to the PCF. The request operation includes the AF Identifier, the IP address of the UE, the identification of the application session context, the SUPI if available, the DNN if available, Media information, bandwidth requirements, sponsored data connectivity if applicable, flow description, AF application identifier, Flow status, Priority indicator, emergency indicator, Application service provider, resource allocation outcome, etc. The request operation may also include the subscription to notifications on certain user plane events, e.g. subscription to QoS notification control.

   1a. The AF provides the Service Information to the PCF by sending a Diameter AAR for a new Rx Diameter session.

2. The PCF stores the Service Information received in step 1.

3. If the PCF does not have the subscription data for the SUPI and DNN, the PCF invokes the Nudr_DataRepository_Query service operation to the UDR including the PCF identifier, the SUPI and the requested subscription data. Additionally, if the AF provided a Background Data Transfer Reference ID in step 1 or step 1a and the corresponding transfer policy is not locally stored in the PCF, the PCF shall retrieve it from the UDR by invoking the Nudr_DataRepository_Query service operation, described in subclause 5.5.y.

   The UDR responds to the PCF with the subscription data and/or the Background Data Transfer policies.

4. The PCF identifies the affected established PDU Session (s) using the information previously received from the SMF and the Service Information received from the AF.

5. The PCF sends an HTTP "201 Created" response to the AF.

   5a. The PCF sends a Diameter AAA to the AF.

6. The AF may invoke the Npcf_PolicyAuthorization_Subscribe service operation by sending the HTTP PUT request with "{apiRoot}/npcf-policyauthorization/v1/app-sessions/{appSessionId}/events-subscription" as the resource URI to subscribe to events in the PCF. The request includesthe events that subscribesand a Notification URI to indicate to the PCF where to send the notification of the subscribed events, as described in subclause 4.2.6 of 3GPP TS 29.514 [10].

7. The PCF sends an HTTP "201 Created" response to the AF.

8. The PCF interacts with SMF according to Figure 5.2.2.2-1.

5.2.2.2.2 AF Session Modification

This procedure is performed when the AF/NEF requests to update an AF application session context for the requested service.

NOTE: The NEF acts as an AF to support the network exposure functionality.

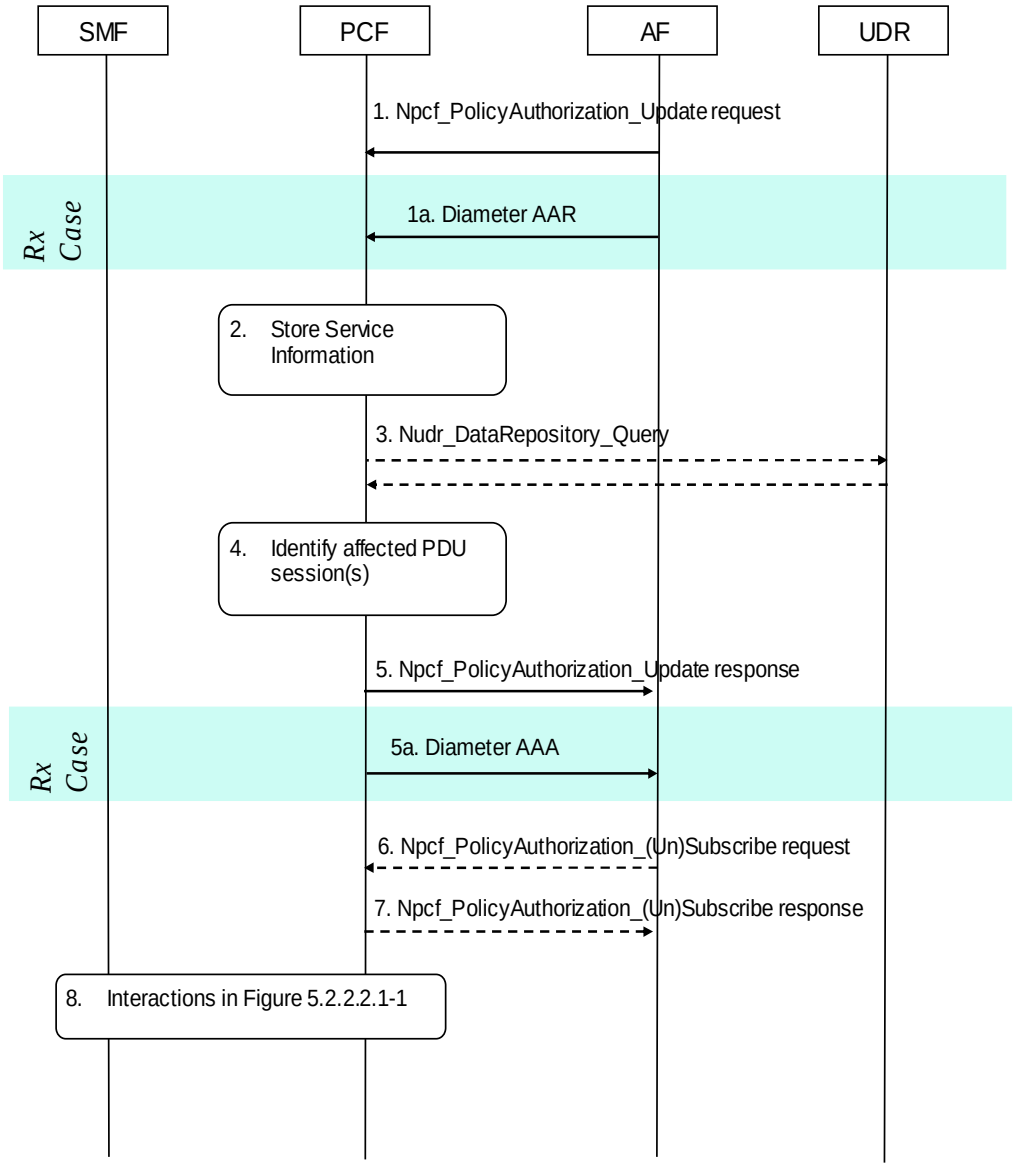


Figure 5.2.2.2.2-1 AF Session Modification triggers PCF-initiated SM Policy Association Modification procedure

1. When the AF receives an internal or external trigger to modify an existing AF session, the AF invokes the Npcf_PolicyAuthorization_Update service operation by sending the HTTP PATCH request with "{apiRoot}/npcf-policyauthorization/v1/app-sessions/{appSessionId}"as the resource URI to the PCF including the modified service information. The AF may also provide the updated subscription to notifications on user plane events.

   1a. The AF provides the Service Information to the PCF by sending a Diameter AAR for the existing Rx Diameter session corresponding to the modified AF session.

2. The PCF stores the received Service Information.

3. If PCF does not have the subscription data for the SUPI and DNN corresponding to the application session context to update, the PCF sends the Nudr_DataRepository_Query service operation to the UDR including the PCF identifier, the SUPI and the requested subscription data. Additionally, if the AF provided a Background Data Transfer Reference ID in step 1 or step 1a and the corresponding transfer policy is not locally stored in the PCF, the PCF shall retrieve it from the UDR by invoking the Nudr_DataRepository_Query service operation, described in subclause 5.5.y.

   The UDR responds to the PCF with the subscription data and/or the Background Data Transfer policies.

4. The PCF identifies the affected existing PDU Session(s) using the information previously received from the SMF and the Service Information received from the AF.

5. The PCF sends an HTTP "200 OK" response to the AF.

   5a. The H-PCF sends a Diameter AAA to the AF.

6. The AF may decide to (un)subscribe to events for the active AF application session context in relation to the corresponding PDU session.

   - If the AF decides to create a subscription to events or modify the events subscription, it invokes the Npcf_PolicyAuthorization_Subscribe service operation by sending the HTTP PUT request to the resource URI "{apiRoot}/npcf-policyauthorization/v1/app-sessions/{appSessionId}/events-subscription". The HTTP request includes the events that subscirbes and may also includes a Notification URI to indicate to the PCF where to send the notification of the subscribed events.

   - If the AF decides to remove subscription to all subscribed events for the existing application session context, it invokes the Npcf_PolicyAuthorization_Unsubscribe service operation by sending the HTTP DELETE request to the resource URI "{apiRoot}/npcf-policyauthorization/v1/app-sessions/{appSessionId}/events-subscription".

7. The PCF responses to the AF.

   - If the PCF accept the HTTP PUT request to create a subscription to events, it sends an HTTP "201 Created" response.

   - If the PCF accept the HTTP PUT request to modify the events subscription, it sends an HTTP "204 No Content" response.

   - Upon receipt of the HTTP DELETE request to remove subscription to all subscribed events, the PCF sends an HTTP "204 No Content" response.

8. The PCF interacts with SMF according to Figure 5.2.2.2-1.

5.2.2.2.2.3 AF Session Termination

This procedure is performed when the PCF requests the AF/NEF to delete the AF application session context.

NOTE: The NEF acts as an AF to support the network exposure functionality for policy/charging capability.

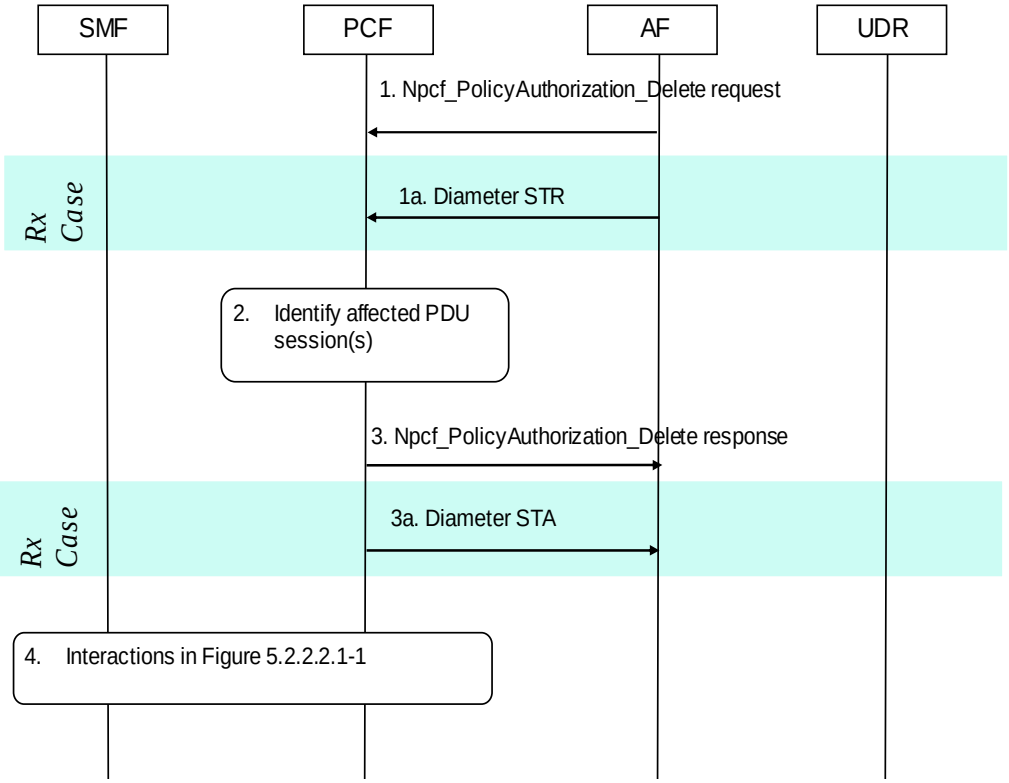


Figure 5.2.2.2.2.3-1 AF Session Termination triggers PCF-initiated SM Policy Association Modification procedure

1. The AF sends the Npcf_PolicyAuthorization_Delete service operation by sending the HTTP POST request with "{apiRoot}/npcf-policyauthorization/v1/app-sessions/{appSessionId}/delete" as the resource URI to request the removal of the AF application session. The request may include the events to subscibe to.

   1a. The AF sends a session termination request, Diameter STR, to the PCF to request the removal of the session.

2. The PCF identifies the affected PDU Session where PCC rules related with this AF session are installed. These PCC rules need to be removed.

3. The PCF removes the AF application session context and sends an HTTP "204 No Content" response to the AF. Optionally, the PCF shall send an HTTP "200 OK", if it needs to include the notification of event.

   3a. The PCF sends a Diameter STA, session termination answer, to the AF.

4. The PCF interacts with SMF according to Figure 5.2.2.2-1.

5.2.2.3 SM Policy Association Modification initiated by the SMF

This procedure is performed when the SMF observes some policy control trigger condition is met..

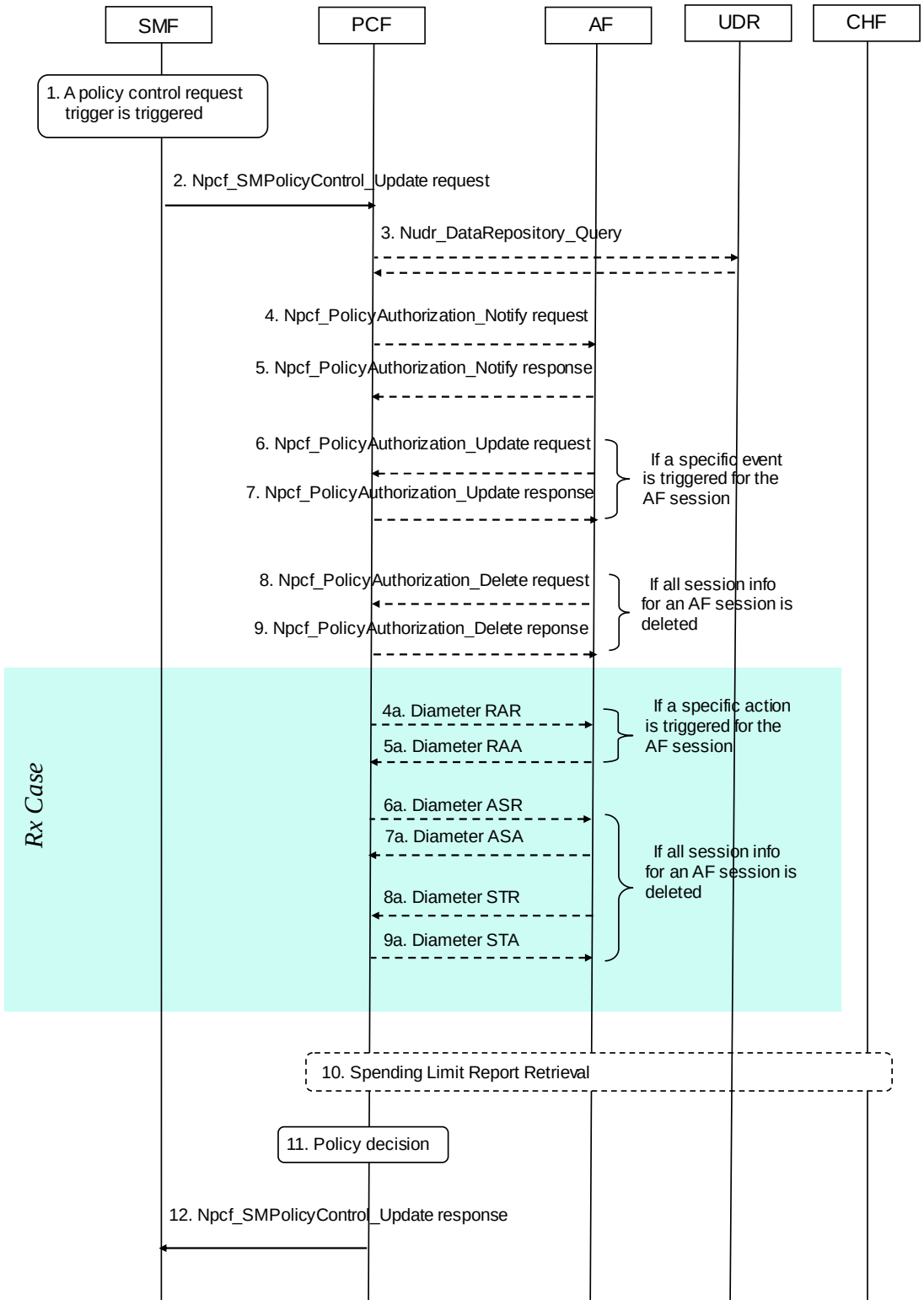


Figure 5.2.2.3-1 SMF-initiated SM Policy Association Modification procedure

1. The SMF detectsa policy control request tirgger condition is met.

2. The SMF invokes the Npcf_SMPolicyControl_Update service operation by sending the HTTP POST request with "{apiRoot}/npcf-smpolicycontrol/v1/sm-policies/{smPolicyId}" as the resource URI to the PCF with information on the conditions that have changed.

3. If the (H-)PCF requires subscription-related information and does not have it, the (H-)PCF sends the Nudr_DataRepository_Query service operation to the UDR in order to receive the information.

The UDR replies with the subscription related information containing the information about the allowed service(s) and PCC Rules information.

4. The PCF invokes the Npcf_PolicyAuthorization_Notify service operation by sending the HTTP POST request with "{notifUri}/notify" as the resource URI to the AF to indicate that an event for the active application session has occurred.

   4a. If the AF requested a notification of the corresponding event, the PCF sends a Diameter RAR with the Specific-Action AVP set to indicate the event that caused the request.

5. The AF sends an HTTP "204 No Content" response to the PCF.

   5a. The AF replies with a Diameter RAA and may provide updated service information within.

6. The AF may invoke the Npcf_PolicyAuthorization_Update service operation to the PCF including the modified service information.

7. The PCF sends an HTTP "200 OK" response to the AF

8. If the PCF indicates in step 4 that there are no transmission resources for the service, the AF may terminate the AF session by invoking the Npcf_PolicyAuthorization_Delete service operation by sending the HTTP POST request with "{apiRoot}/npcf-policyauthorization/v1/app-sessions/{appSessionId}/delete" as the resource URI to terminate the AF session. The request may include the events to subscibe to.

9. The PCF removes the AF application session context and sends an HTTP "204 No Content". If the PCF need to include the notification of event, it sends an HTTP "200 OK" response.

   6a-9a. If all service data flows for an AF session are deleted, the AF session is terminated.

10. If the PCF determines that the policy decision depends on the status of the policy counters available at the CHF and such reporting is not established for the subscriber, the PCF initiates an Initial Spending Limit Report as defined in subclause 5.3.2. If policy counter status reporting is already established for the subscriber, and the PCF decides to modify the list of subscribed policy counters, the PCF sends an Intermediate Spending Limit Report as defined in subclause 5.3.3. If the PCF decides to unsubscribe any future status notification of policy counters, it sends a Final Spending Limit Report Request to cancel the request for reporting the change of the status of the policy counters available at the CHF as defined in subclause 5.3.4.

11. The PCF makes a policy decision. The PCF may determine that updated or new policy information needs to be sent to the SMF.

12. The PCF sends an HTTP "200 OK" response to the SMF with updated policy information about the PDU Session determined in step 11.

5.2.3 SM Policy Association Termination

5.2.3.1 SM Policy Association Termination initiated by the SMF

This procedure is performed when the UE requests to terminate a PDU session or based on some internal triggers in the SMF(e.g. operator policy).

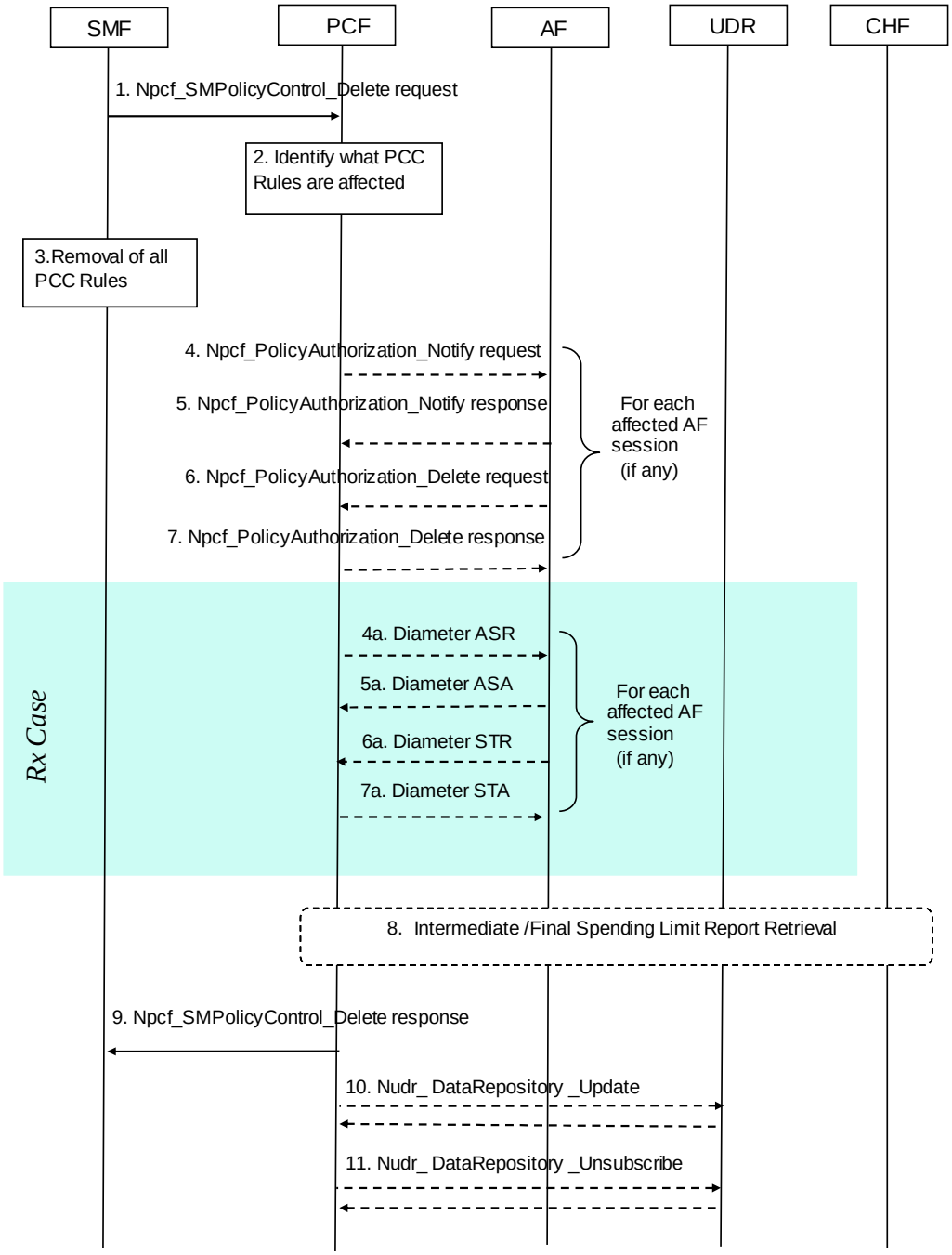


Figure 5.2.3.1-1 SMF-initiated SM Policy Association Termination procedure

This procedure concerns both roaming and non-roaming scenarios.

In the LBO roaming case, the PCF acts as the V-PCF, and the step 8, step 10 and step 11 shall be skipped. In the home routed roaming case, the PCF acts as the H-PCF, and the H-PCF interacts only with the H-SMF.

1. The SMF invokes the Npcf_SMPolicyControl_Delete service operation by sending the HTTP POST request with "{apiRoot}/npcf-smpolicycontrol/v1/sm-policies/{smPolicyId}/delete" as the resource URI to request the PCF to delete the context of the SM related policy. The request operation may include usage monitoring information (if applicable) and access network information.

2. Upon receipt of Npcf_SMPolicyControl_Delete service operation, the PCF identifies the PCC Rules that require an AF to be notified and removes PCC Rules for the PDU Session.

3. The SMF removes all the PCC Rules which are applied to the PDU session.

4. The PCF invokes the Npcf_PolicyAuthorization_Notify service operation by sending the HTTP POST request with "{notifUri}/notify" as the resource URI to the AF to indicate that there are no transmission resources for the service if this is requested by the AF.

   4a. The PCF indicates the session abort to the AF by sending a diameter ASR to the AF.

5. The AF sends an HTTP "204 No Content" response to the PCF.

   5a. The AF responds by sending a diameter ASA to the PCF.

6. The AF invokes the Npcf_PolicyAuthorization_Delete service operation by sending the HTTP POST request to the resource URI "{apiRoot}/npcf-policyauthorization/v1/app-sessions/{appSessionId}/delete". The request may include the events to subscibe to.

   6a. The AF sends a diameter STR to the PCF to indicate that the session has been terminated.

7. The PCF removes the AF application session context and sends an HTTP "204 No Content" response to the AF. If the PCF need to report usage data or the access network information, it sends an HTTP "200 OK" response. If usage thresholds were provided by the AF earlier, and the PCF has usage data that has not yet been reported to the AF, the PCF informs the AF about the resources that have been consumed by the user since the last report. If the SMF in step 1 reports the access network information and if the AF requested the PCF to report access network information previously, the PCF informs the AF about the access network information. The PCF also deletes the subscription to PCF detected events for that AF application Session.

   7a. The PCF responds by sending a diameter STA to the AF.

8. If this is the last PDU session for this subscriber the Final Spending Limit Report Request as defined in clause 5.3.4 is sent. If any existing PDU sessions for this subscriber require policy counter status reporting, the Intermediate Spending Limit Report Request as defined in clause 5.3.3 can be sent to alter the list of subscribed policy counters.

9. The PCF removes PCC Rules for the terminated PDU Session and sends an HTTP "204 No Content" response to the SMF.

10. The PCF stores the remaining usage allowance in the UDR by invoking Nudr_DataRepository_Update service operation if all PDU sessions of the user to the same DNN are terminated.

    The UDR responds to the PCF and in the response the UDR indicates result (success/failure) of the Nudr_DataRepository_Update service operation.

11. The PCF unsubscribes the notification of the PDU session related data modification from the UDR by invoking Nudr_DataRepository_Unsubscribe service operation if it has subscribed such notification.

    The UDR acknowledges to the PCF with the result (success/failure) of the Nudr_DataRepository_Unsubscribe service operation.

5.2.3.2 SM Policy Association Termination initiated by the PCF

This procedure is performed when the PCF requests to terminate a SM Policy Association based on some external or internal triggers as described in step 1 below.

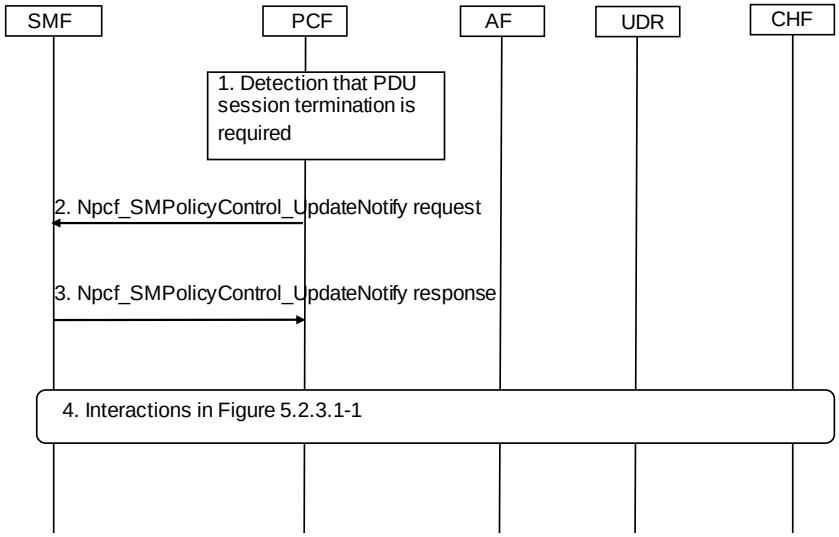


Figure 5.2.3.2-1 PCF-initiated SM Policy Association Termination procedure

This procedure concerns both roaming and non-roaming scenarios.

In the LBO roaming case, the PCF acts as the V-PCF. In the home routed roaming case, the PCF acts as the H-PCF, and the H-PCF interacts only with the H-SMF.

1. The PCF makes policy decisions to terminate a PDU session based on an external trigger, e.g. UE subscription data is deleted, or based on an internal trigger, e.g. operator policy is changed.

2. The PCF sends the Npcf_SMPolicyControl_UpdateNotify service operation by sending the HTTP POST request with "{Notification URI}/delete" as the resource URI to trigger the SMF to request the release of the PDU session. The request includes SUPI and the PDU session ID.

3. The SMF sends an HTTP "200 OK" response to the PCF.

4. The PCF interacts with SMF/AF/UDR/CHF according to Figure 5.2.3.1-1.

5.3 Spending Limit Procedures

5.3.1 General

The PCF may interact with the CHF to make PCC decisions based on spending limits. In Home Routed roaming and Non-roaming case, the (H-) PCF will interact with the CHF in HPLMN.

5.3.2 Initial Spending Limit Report Request

This clause describes the signalling flow for the PCF to request the status of the policy counters available at the CHF, and to subscribe to updates of these policy counters by the CHF. If the PCF provides the list of policy counter identifier(s), the CHF returns the policy counter status per policy counter identifier provided by the PCF, and stores the PCF's subscription to spending limit reports for these policy counters. If the PCF does not provide the list of policy counter identifier(s), the CHF returns the policy counter status for all policy counter identifier(s), which are available for this subscriber, and stores the PCF's subscription to spending limit reports for all policy counters.

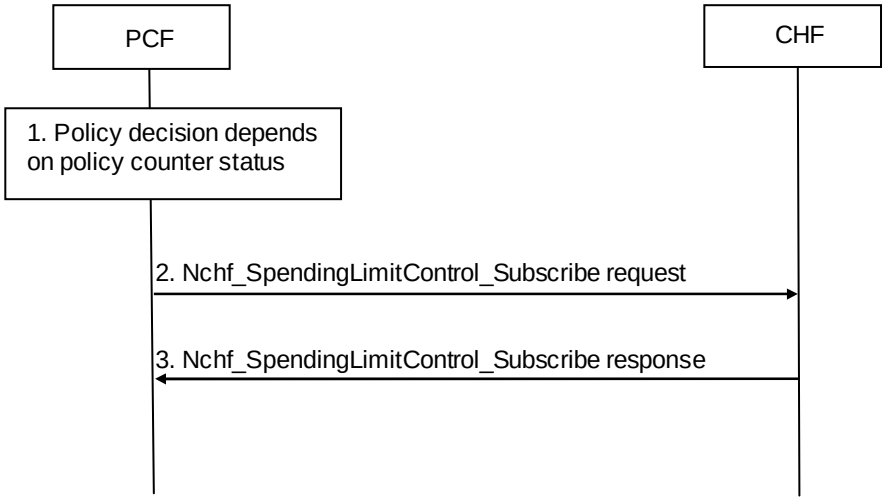


Figure 5.3.2-1 Initial Spending Limit Report Request procedure

1. The PCF retrieves subscription information that indicates that policy decisions depend on policy counter(s) held at the CHF and optionally the list of policy counter identifier(s).

2. The PCF invokes Nchf_SpendingLimitControl_Subscribe service operation by sending the HTTP POST request with "{apiRoot}/nchf-spendinglimitcontrol/v1/subscriptions" as the resource URI to the CHF if such reporting is not established for the subscriber. The request operation includes. SUPI, the EventId "policy counter status change" andoptionally, the list of policy counter identifier(s) as Event Filter, Event Reporting Information (continuous reporting). The PCF also supplies a Notification URI to indicate where to send notifications, and provides a Notification Correlation ID allowing it to correlate notifications with this subscription.

3. The CHF responds to the Nchf_SpendingLimitControl_Subscribe service operation including a Subscription Correlation ID and as Event Information provides the policy counter status, and optionally pending policy counter statuses and their activation times, per required policy counter identifier, and stores the PCF's subscription to spending limit reports for these policy counters. When no policy counter identifier(s) was received from the PCF, it provides the policy counter status, optionally pending policy counter statuses and their activation times, for all policy counters, which are available for this subscriber, and stores the PCF's subscription to spending limit reports for all policy counters.

5.3.3 Intermediate Spending Limit Report Request

This clause describes the signalling flow for the PCF to request the status of additional policy counters available at the CHF or to remove the request for the status of policy counters available at CHF. If the PCF provides the list of policy counter identifier(s), the CHF returns the policy counter status per policy counter identifier provided by the PCF.

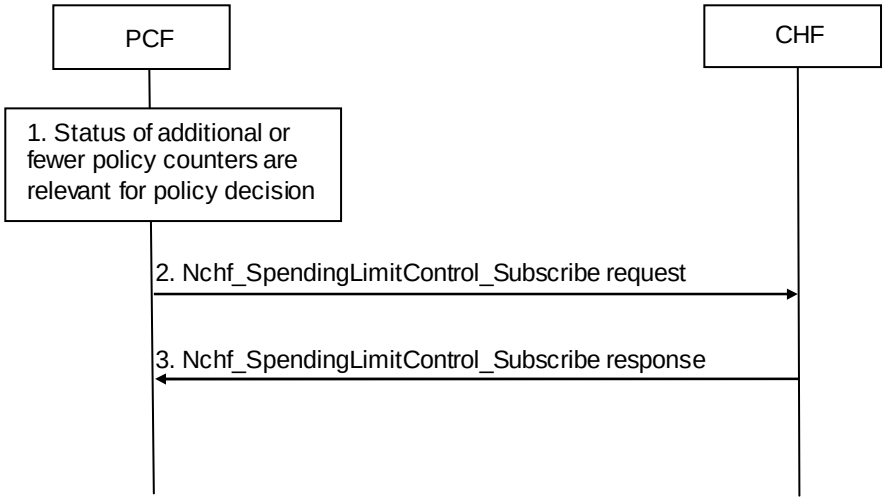


Figure 5.3.3-1 Intermediate Spending Limit Report Request procedure

1. The PCF decides to modify the list of subscribed policy counters, e.g. PCF determines that policy decisions depend on additional policy counter identifier(s) held at the CHF or that notifications of policy counter status changes for some policy counters are no longer required.

2. The PCF invokes Nchf_SpendingLimitControl_Subscribe service operation by sending the HTTP POST request with "{apiRoot}/nchf-spendinglimitcontrol/v1/subscriptions" as the resource URI to the CHF. The request operation includes the subscription correlation ID, and may include the EventId "policy counter status change" and an updated list of policy counter identifier(s) as EventFilters, that overrides the previously stored list of policy counter identifier(s).

3. The CHF responds to the Nchf_SpendingLimitControl_Subscribe service operation and provides as Event Information the policy counter status and optionally pending policy counter statuses and their activation times, per required policy counter identifier, and stores or removes the PCF's subscription to spending limit reporting by comparing the updated list with the existing PCF subscriptions. When no policy counter identifier(s) was received from the PCF, it provides the policy counter status, optionally pending policy counter statuses and their activation times, for all policy counter(s), which are available for this subscriber, and stores the PCF's subscription to spending limit reports for all policy counters.

5.3.4 Final Spending Limit Report Request

This clause describes the signalling flow for the PCF to unsubscribe to any future updates of policy counters for a given subscriber by the CHF. It cancels the request for reporting the change of the status of the policy counters available at the CHF.

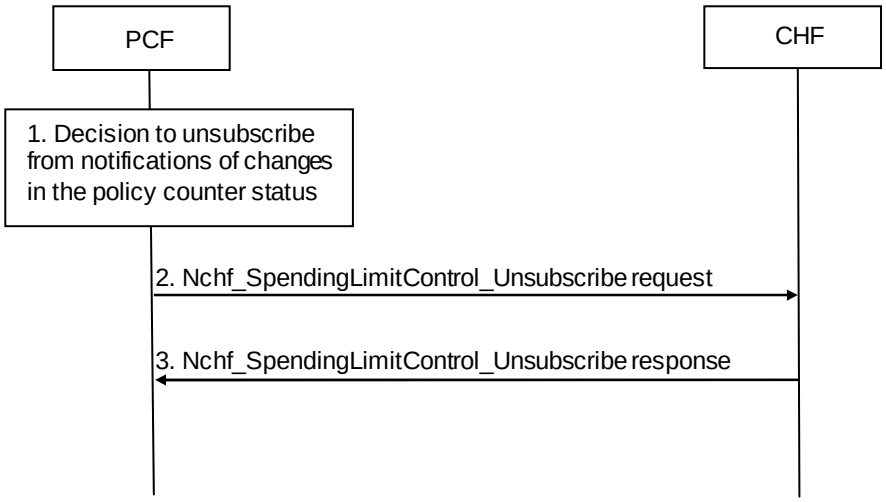


Figure 5.3.4-1 Final Spending Limit Report Request procedure

1. The PCF decides that policy decisions for a given user no longer depend on policy counter(s) to which the PCF has existing subscriptions for status change notification.

2. The PCF sends Nchf_SpendingLimitControl_ Unsubscribe service operation by sending the HTTP DELETE request with "{apiRoot}/nchf-spendinglimitcontrol/v1/subscriptions/{subscriptionId}" as the resource URI to the CHF to cancel the notification request from the CHF on policy counter status, whereby the "{subscriptionId}" is the identification of the existing subscription to be deleted.

3. The CHF removes the PCF's subscription to spending limit reporting and responds to the Nchf_SpendingLimitControl_ Unsubscribe service operation to the PCF.

5.3.5 Spending Limit Report

This clause describes the signalling flow for the CHF to notify the changes of the status of a subscribed policy counter(s) available at the CHF for that subscriber. Alternatively, the signalling flow can be re-used by the CHF to provide one or more pending statuses for a subscribed policy counter together with the time that have to be applied.

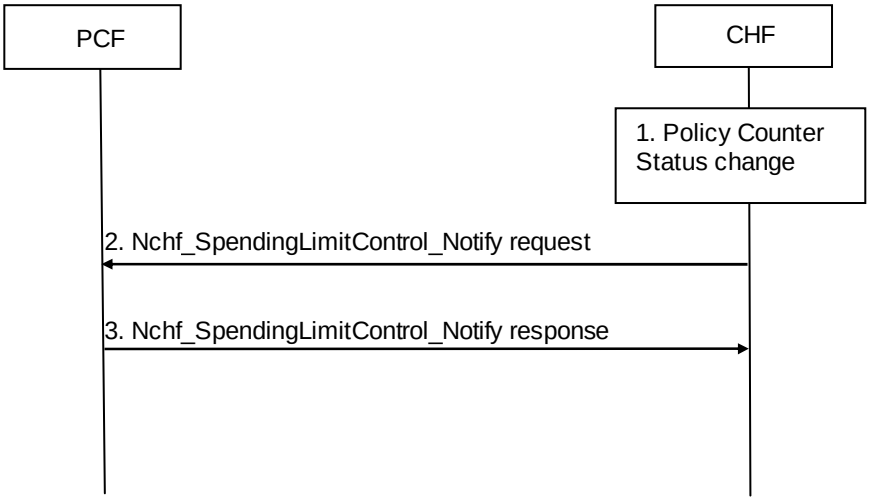


Figure 5.3.5-1 Spending Limit Report procedure

1. The CHF detects that status of a policy counter identifier(s) has changed and the PCF requested notification of changes in the status of a policy counter(s). Alternatively, if the CHF detects a policy counter status will change at a future point in time, the CHF shall be able to instruct the PCF to apply one or more pending statuses for a requested policy counter.

2. When the status of a specific policy counter changes, or the CHF detects that a policy counter status will change at a future point in time and decides to instruct the PCF to apply one or more pending statuses for a requested policy counter, the CHF shall determine the PDU sessions impacted by the change (i.e. those PDU sessions that have subscribed to status change notifications for the changed policy counter) and invoke Nchf_SpendingLimitControl_Notify service operation by sending the HTTP POST request with "{notificationURI}" as the resource URI to the PCF associated with each affected PDU session. The request operation includes SUPI, the Notification Correlation ID, and in the Event Information the updated policy counter status, optionally including pending policy counter statuses and their activation times for any of the subscribed policy counters.

3. The PCF acknowledges the Nchf_SpendingLimitControl_Notify service operation. The PCF uses the status of the received policy counter(s) as input to its policy decision to apply operator defined actions, e.g. downgrade the QoS, and it shall ignore an unknown policy counter status report for all unknown policy counter identifiers in the Nchf_SpendingLimitControl_Notify service operation from the CHF.

5.4 Network Data Analytics Procedures

5.4.1 General

The PCF may interact with the NWDAF to make PCC decisions based on load level information.

5.4.2 Network data analytics Subscribe/Unsubscribe

This procedure is used by the PCF to subscribe/unsubscribe load level information of network slice instance(s) from NWDAF. Periodic notification and notification upon threshold exceeded can be subscribed. The PCF may make policy decisions based on the load level information of network slice instance.

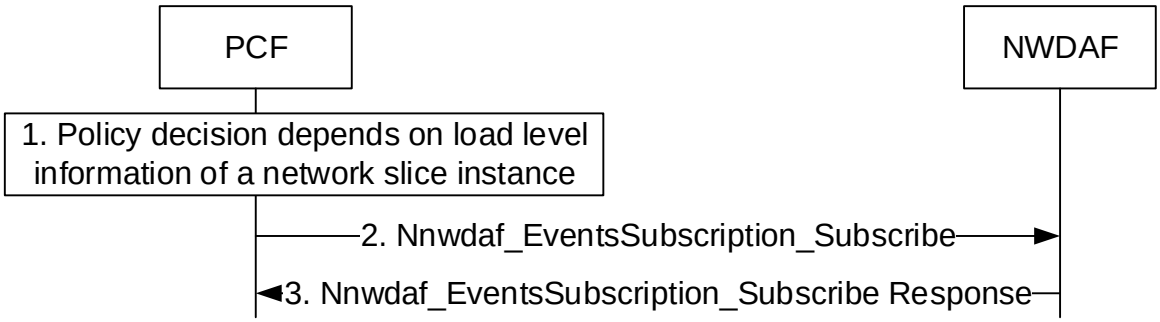


Figure 5.4.2-1 subscribe load level information

1. The PCF makes policy decisions depend on load level information. The PCF have not yet subscribe such load level information of network slice instance(s) from NWDAF.

2. The PCF invokes Nnwdaf_EventsSubscription_Subscribe service operation by sending an HTTP POST request with "{apiRoot}/nnwdaf-eventssubscription/v1/subscriptions" as Resource URI, to the NWDAF to subscribe load level information of network slice instance(s). The request includes the subscribed events and may include the identifier of network slice instance(s), event notification method.

3. The NWDAF responds to the Nnwdaf_EventsSubscription_Subscribe service operation. If the subscription is accepted, the response includes the URI of the created subscription with "201 Created".

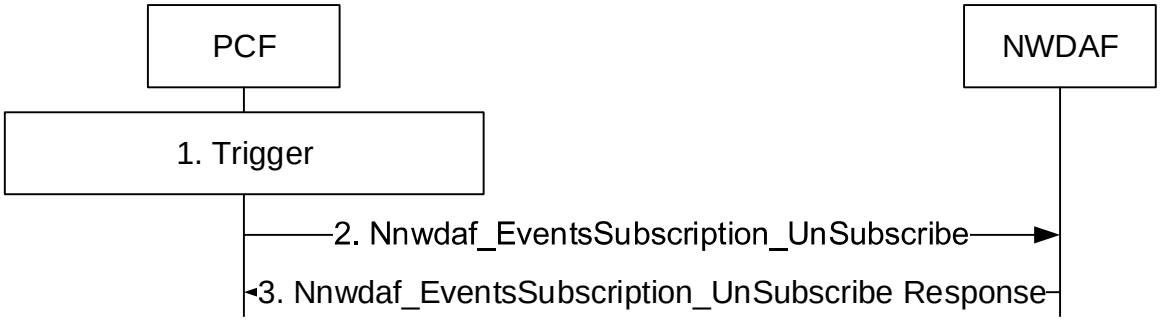


Figure 5.4.2-2 unsubscribe load level information

1. The PCF receives an internal or external trigger to unsubscribe a load level information of network slice instance(s) from NWDAF.

2. The PCF invokes Nnwdaf_EventsSubscription_UnSubscribe service operation by sending an HTTP POST request with "{apiRoot}/nnwdaf-eventssubscription/v1/subscriptions/{subscriptionId}" as Resource URI, to the NWDAF to unsbscribe load level information of network slice instance(s). The request includes the event subscriptionId of the existing subscription that is to be deleted.

3. The NWDAF responds to the Nnwdaf_EventsSubscription_UnSubscribe service operation. If the unsubscription is accepted, the NWDAF responds with "204 No Content".

5.4.3 Network data analytics info request

This procedure is used by the PCF to request load level information of network slice instance(s) from NWDAF. The PCF may make policy decisions based on the load level information of network slice instance.

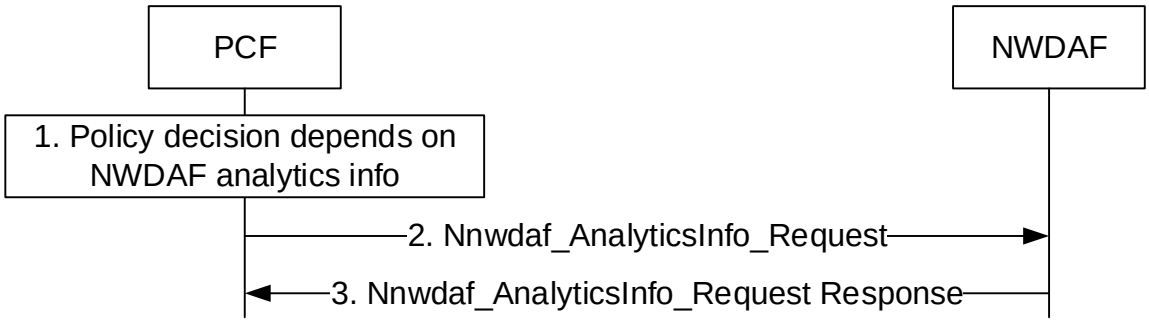


Figure 5.4.3-1 Request analytics info

1. The PCF makes policy decisions depend on load level information of network slice instance(s), especially for one time usage. The PCF have not yet subscribe such load level information of network slice instance(s) from NWDAF.

2. The PCF invokes Nnwdaf_AnalyticsInfo_Request service operation by sending an HTTP GET request with "{apiRoot}/nnwdaf- analyticsinfo/v1/analytics?query_parameters" as Resource URI, to the NWDAF to request load level information of network slice instance(s). The request includes the network slice instance(s) as event filter and may include the identifier of network slice instance(s), event notification method.

3. The NWDAF responds to the Nnwdaf_ AnalyticsInfo_Request service operation. If the request is accepted, the response includes load level information of Network Slice instance(s) with "200 OK".

5.5 Service Capability Exposure Procedures

5.5.1 General

PCC abilities can be exposed to a 3rd party application server via the NEF.

The following procedures are included in this clause:

1. The procedure of Packet Flow Descriptions management.

2. The procedure of AF traffic routing.

3. The procedure of Background Data Transfer negotiation.

5.5.2 Management of Packet Flow Descriptions

5.5.2.1 AF-initiated PFDF management procedure

This subclause describes the procedure initiated by the AF for creation, update or removal of packet flow descriptions of the application(s) in operator's network as depicted in figure 5.5.2.1-1.

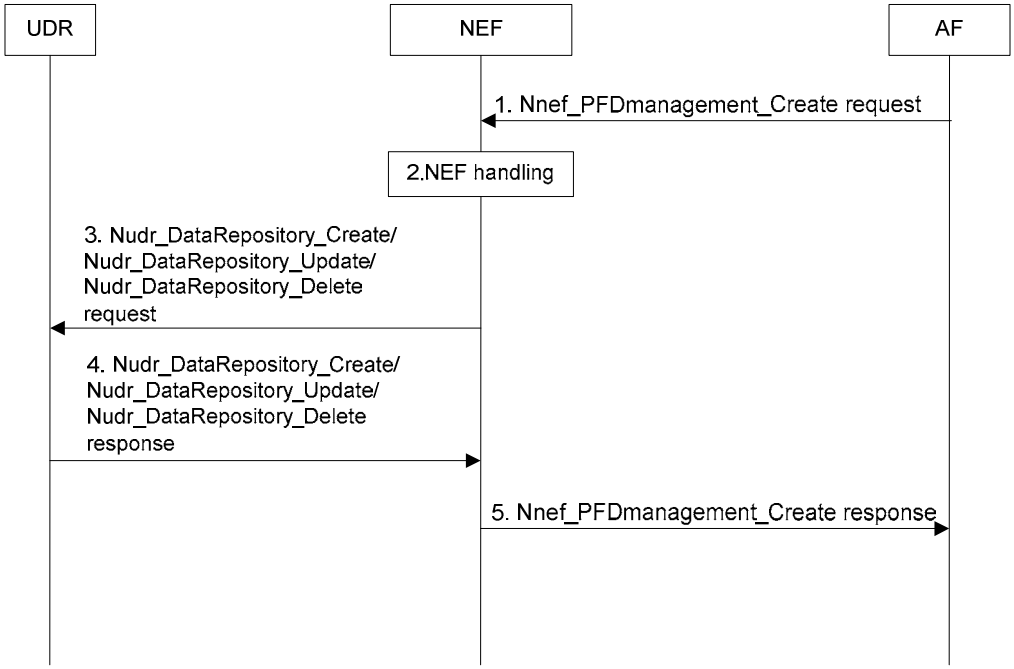


Figure 5.5.2.1-1 AF-initiated PFDF management procedure

1. In order to create, update or remove PFDs resources for one or more application identifier(s) in the operator's network, the AF shall invoke Nnef_PFDmanagement_Create service operation to the NEF. The request message shall include application identifier(s) and PFDs associated with its PFD identifier(s). An Allowed Delay may be included for the application identifier(s) as well.

Editor's note: Nnef_PFDmanagment_Create service operation is FFS.

2. The NEF checks whether the application is authorized to perform this request based on the operator policies.
3. The NEF invokes Nudr_DataRepository operation service to the UDR as follows:
   - if request for PFD creation in step 1, the NEF shall invoke the Nudr_DataRepository_Create service operation by sending an HTTP PUT request message or an HTTP POST request message to the UDR as specified in 3GPP TS 29.504 [27];
   - if request for PFD update in step 1, the NEF shall invoke the Nudr_DataRepository_Update service operation by sending an HTTP PATCH request messge and an HTTP PUT request message to the UDR as specified in 3GPP TS 29.504 [27]; and
   - if request for PFD removal in step 1, the NEF shall invoke the Nudr_DataRepository_Delete service operation by sending an HTTP DELETE request messge to the UDR as specified in 3GPP TS 29.504 [27].
4. The UDR shall send the HTTP response message to the NEF correspondingly.
5. The NEF sends Nnef_PFDManagement_Create Response to the AF.

5.5.2.2 PFDF management towards SMF

5.5.2.2.1 PFD retrieval

This procedure enables the SMF to retrieve PFDs for application identifier(s) from the PFDF as depicted in figure 5.5.2.2.1-1 when

- a PCC rule with the application identifier(s) is provided or activated and PFDs for the corresponding application identifier(s) are not available at the SMF; and
- the caching timer for an application identifier expires and the PCC Rule for this application identifier is still active.

The SMF may retrieve PFDs for one or more application identifiers in the same Request. All PFDs related to an application identifier are provided in the response from the UDR to NEF (PFDF).

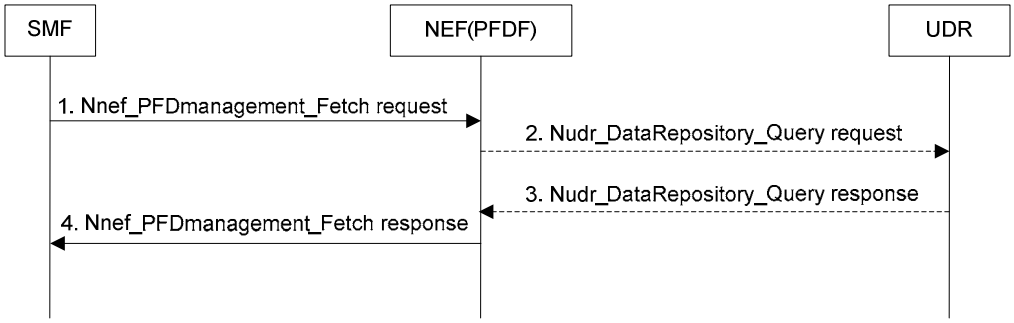


Figure 5.5.2.2.1-1 PFD retrieval by SMF

1. The SMF shall invoke Nnef_PFDmanagement_Fetch service operation by sending an HTTP GET request message to the NEF (PFDF) for retrieval of the PFDs for application identifier(s) as specified in 3GPP TS 29.551 [25].

2. If the requested PFDs are not available in PFDF, PFDF shall invoke Nudr_DataRepository_Query service operation by sending an HTTP GET request message to the UDR as specified in 3GPP TS 29.504 [27].

3. The UDR shall send an HTTP GET response message including the requested PFDs to the NEF.

4. The NEF (PFDF) sends the SMF the HTTP GET response message including the PFDs for the requested application identifier(s) to the SMF.

5.5.2.2.2 PFD management

This procedure enables the SMF to subscribe the notification of events when the PFDs for application identifier change. The PFDF will notify the SMF to update and/or delete the PFDs for application identifier(s) as subscribed previously.

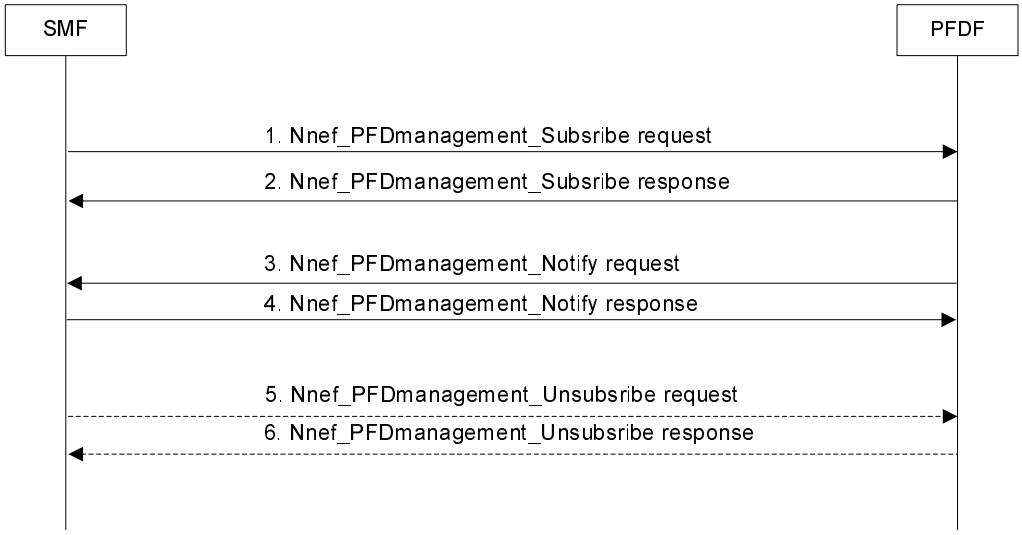


Figure 5.5.2.2.2-1 PFDF management in the SMF

1-2. In order to subscribe the notification of events when the PFDs for application identifier change, the SMF can use Nnef_PFDmanagement_Subscribe service operation by sending an HTTP POST message to the PFDF as specified in 3GPP TS 29.551 [25]. The PFDF shall send the POST response message to the SMF.

3-4. The PFDF shall use Nnef_PFDmanagement_Notify service operation to update and/or delete the PFDs for application identifier(s) in the SMF. The PFDF shall send an HTTP POST request message to the SMF including the changed PFD information as specified in 3GPP TS 29.551 [25]. The SMF replies to the PFDF with an HTTP POST response message.

5-6. The SMF may initiate Nnef_PFDmanagement_Unsubscribe service operation to remove the subscription by sending a HTTP DELETE request message to the PFDF as specified in 3GPP TS 29.551 [25]. The PFDF replies to the SMF with an HTTP DELETE response message.

5.5.3 Processing AF policy requirements for UE(s) via NEF

If the AF is not allowed by the operator to access directly the PCF, the AF uses the NEF to interact with the PCF.

The NEF needs to register itself with the NRF as producer of the Npcf_PolicyAuthorization service, so that the AF can request the 3GPP network to apply policy requirements via the NEF. The Npcf_PolicyAuthrization service used by the AF can target an individual UE, a group of UEs, or any UE. If the request is for an individual UE, the NEF may use the BSF to find the PCF serving the UE; if the request is for a group of UE or any UE, the NEF may use the UDR to store the AF request.

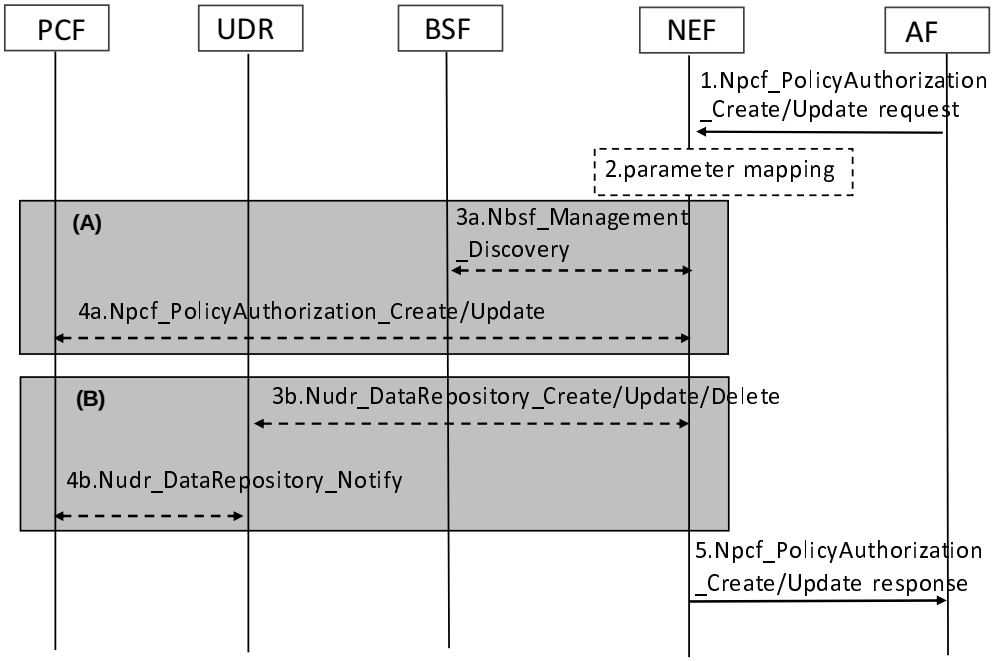


Figure 5.6-1: AF request handling via NEF procedure

1. The AF sends Npcf_PolicyAuthorization_Create or Npcf_PolicyAuthorization_Update request to the NEF.

2. The NEF may perform parameter mapping for the received request according to configured policy.

3a-4a. As depicted in (A), if the AF request is for an individual UE, the NEF may use the Nbsf_Management_Discovery service operation to discover the PCF for the UE. After getting the PCF id, the NEF forwards the AF request to the PCF.

3b-4b. As depicted in (B), if the AF request is for a group of UEs or targetting any UE, the NEF creates/updates/deletes the AF request into the selected UDR by invoking the Nudr_DataRepository_Create, Nudr_DataRepository_Update or Nudr_DataRepository_Delete service operation. If there are PCF(s) which subscribed UDR service before for notification of AF data change, the UDR notifies the PCF(s) by Nudr_DataRepository_Notify service operation.

5. The NEF responds with Npcf_PolicyAuthorization_Create or Npcf_PolicyAuthorization_Update response to the AF.

Editor's note: The procedure and further details for the procedure are FFS.

5.5.4 Negotiation for future background data transfer procedure

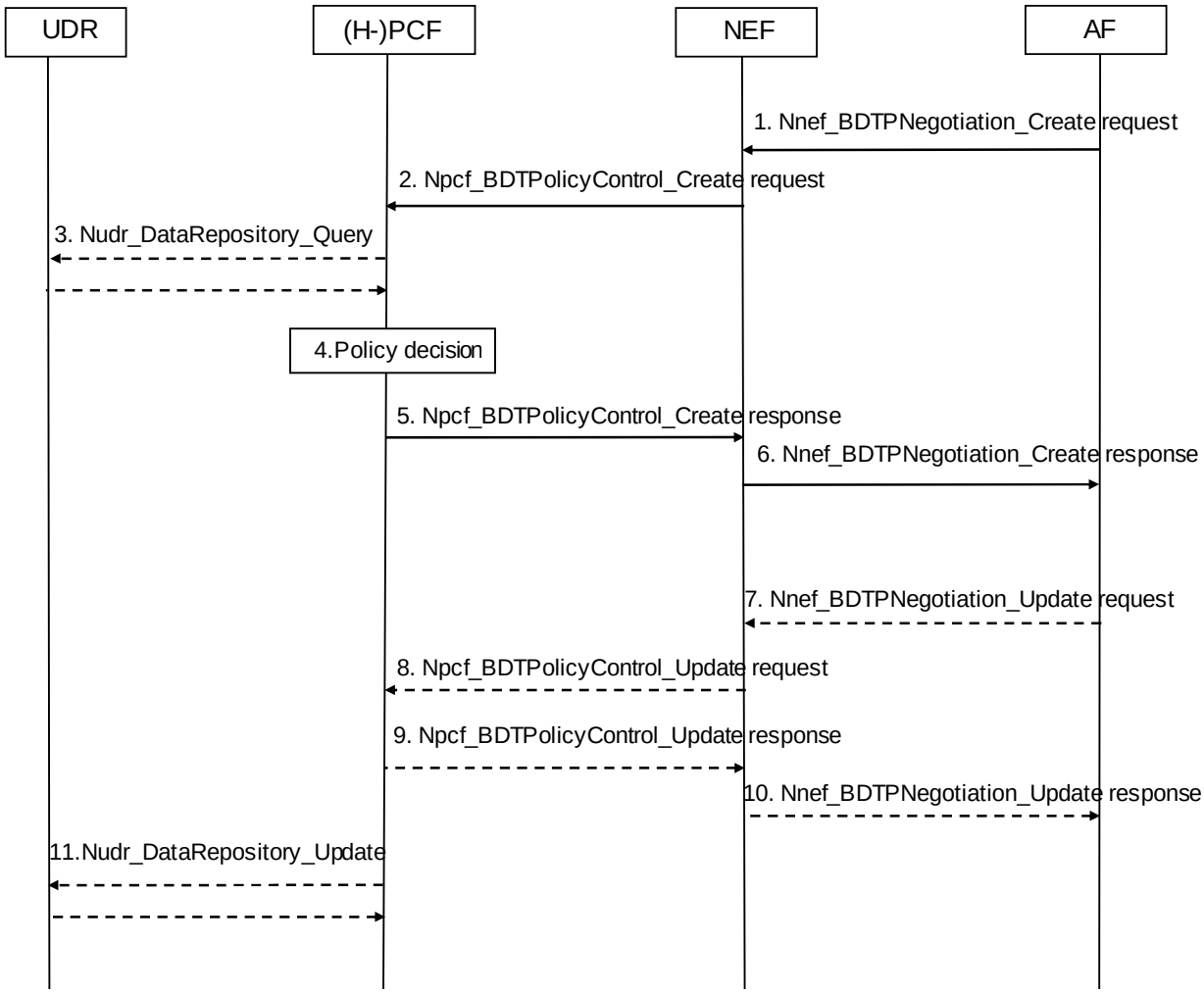


Figure 5.5.y-1: Negotiation for future background data transfer procedure

1. The AF invokes the Nnef_BDTPNegotiation_Create service operation to get background data transfer policies. The AF request shall contain an ASP identifier, the volume of data to be transferred per UE, the expected amount of UEs, the desired time window and optionally, network area information (e.g. list of TAs/RAs).

NOTE 1: A 3rd party application server is typically not able to provide any specific network area information and if so, the AF request is for a whole operator network.

2. Upon receipt of a Background Data Transfer request from the AF indicating a transfer policy request, the NEF invokes the Npcf_BDTPolicyControl_Create service operation with the (H-)PCF by sending an HTTP POST request to the resource URI "{apiRoot}/npcf_bdtpolicycontrol/v1/bdtpolicies". The request operation includes ASP Identifer, Volume per UE, Number of UEs, Desired time window, and may include Network Area Information.

NOTE 2: The NEF may contact any PCF in the operator network.

3. The (H-) PCF may invoke the Nudr_DataRepository_Query service operation, as described in 3GPP TS 29.504 [27] and 3GPP TS 29.519 [12], to request from the UDR all stored transfer policies.

NOTE 3: In case only one PCF is deployed in the network, transfer policies can be locally stored in the PCF and the interaction with the UDR is not required.

4. The (H-) PCF determines one or more transfer policies based on the information received from the NEF and other available information (e.g. network policy, existing transfer policies, load status estimation for the desired time window).

5. The (H-) PCF sends a "201 Created" response to the Npcf_BDTPolicyControl_Create service operation with the acceptable one or more transfer policies and a Background Data Transfer Reference ID, as described in subclause 4.2.2 of 3GPP TS 29.554 [26].

6. The NEF forwards the received transfer policies to the AF by invoking a Nnef_BDTPNegotiation_Create response to the AF. If the NEF received only one background transfer policy from the PCF, steps 7-10 are not executed and the flow proceeds to step 11. Otherwise, the flow proceeds to step 7.

7. The AF invokes the Nnef_BDTPNegotiation_Update service operation to provide the NEF with the selected background data transfer policy.

8. The NEF invokes the Npcf_BDTPolicyControl_Update service operation by sending an HTTP PATCH request to the resource URI "{apiRoot}/npcf_bdtpolicycontrol/v1/bdtpolicies/{bdtPolicyId}" to provide the (H-)-PCF with the selected background data transfer policy.

9. The (H-) PCF sends the acknowledge message to the NEF.

10. The NEF sends the acknowledge message to the AF.

11. If the (H-) PCF decides to locally store the transfer policy, it invokes the Nudr_DataRepository_Update service operation, as described in 3GPP TS 29.504 [27] and 3GPP TS 29.519 [12], to store the new transfer policy together with the associated reference ID and the corresponding network area information in the UDR.

6 Binding Mechanism

6.1 Overview

The binding mechanism associates the session information with the QoS flow that is intended to carry the service data flow(s).

The binding mechanism includes three steps:

1. Session binding.

2 PCC rule authorization.

3. QoS flow binding.

The Session binding function receives the AF session information and determines the relevant PDU session. With this information the PCC rule authorization function runs the policy rules and constructs the PCC rule(s), if the authorization is granted. Finally, the QoS flow binding function selects the QoS flow(s) to carry the service data flow (defined in a PCC rule by means of the SDF template), within the PDU session.

The PCC rule authorization function and the QoS flow binding function can take place without the Session binding function at certain PDU session events (e.g. request of SM related policies initiated by the SMF). The PCF may authorize dynamic PCC rules for service data flows without a corresponding AF session.

NOTE: The relation between AF sessions and rules depends only on the operator configuration. An AF session can be covered by one or more PCC rules, if applicable (e.g. one rule per media component of an IMS session).

6.2 Session Binding

The Session binding is the association of the AF session information to one and only one PDU session.

When the PCF receives the service information from the AF, the PCF shall perform the session binding and shall associate the described IP and Ethernet data flows within the AF session information (and therefore the applicable PCC rules) to one existing PDU session. This association is done comparing the following parameters received from the AF with the corresponding PDU session parameters.

a) For an IP type PDU session, the UE IPv4 address or IPv6 network prefix.

   For an Ethernet type PDU session, the UE MAC address.

b) The UE identity (of the same kind e.g. SUPI), if available.

NOTE 1: In case the UE identity in the access network and the application level identity for the user are of different kinds, the PCF needs to maintain, or have access to, the mapping between the identities. Such mapping is outside the scope of the present document.

c) The information about the data network (DNN) the user is accessing, if available.

Session Binding applies for PDU sessions of IP type. It may also apply to Ethernet PDU session type, and it does not apply to AF requests sent over Rx.

NOTE 2: For the Ethernet PDU session, the PCF needs to subscribe to "UE MAC address change" to the SMF.

The PCF shall identify the PCC rules affected by the AF session information, including new PCC rules to be installed and existing PCC rules to be modified or removed.

If the PCF is not capable of executing the Session binding, the PCF shall reject the AF request.

6.3 PCC rule Authorization

The PCC rule authorization is the selection of the 5G QoS parameters for the PCC rules.

The PCF shall perform the PCC rule authorization after successful Session binding for PCC rules belonging to the AF sessions, as well as for the PCC rules without the corresponding AF sessions. By the authorization process the PCF determines whether the user can have access to the requested services and under what constraints. If so, the PCC rules are created or modified. If the Session information is not authorized, a negative answer shall be issued to the AF.

The PCF shall perform the PCC rule authorization function when the PCF receives the session information from the AF, when the PCF receives a notification of PDU session events (e.g. PDU session establishment, PDU session modification) from the SMF, or when the PCF receives a notification from the UDR that calls for a policy decision.

For the authorization of a PCC rule, the PCF shall consider any 5GC specific restrictions, the AF service information and other information available to the PCF (e.g. user's subscription information, operator policies). The PCF assigns appropriate a set of 5G QoS parameters (5QI, QoS characteristics, ARP, GBR, MBR, QNC, RQI), that can be supported by the access network, to each PCC rule.

The authorization of a PCC rule associated with an emergency service shall be supported without subscription information (e.g. information stored in the UDR). The PCF shall apply policies configured for the emergency service.

Editor's note: Non-IP cases are FFS.

6.4 QoS flow binding

The QoS flow binding is the association of the PCC rule to a QoS flow, identified by the QFI, within a PDU session.

The QoS flow binding function resides in the SMF. The binding is performed using the following binding parameters:

- 5QI;
- ARP;
- QNC (if available in the PCC rule);
- Priority Level (if available in the PCC rule);
- Averaging Window (if available in the PCC rule), and;
- Maximum Data Burst Volume (if available in the PCC rule).

The set of 5G QoS parameters assigned by the PCF to the service data flow is the main input for QFI allocation.

When the PCC rule provides an indication(i.e. "Bind to QoS flow associated with the default QoS rule" parameter) for the service data flow(s) to be bound to the QoS flow of the default QoS rule, the SMF shall use this indication instead of associated with parameters in the PCC rule for the QoS flow binding and keep the binding as long as this parameter remains set.

When "Bind to QoS flow associated with the default QoS rule" parameter is not received, the allocation of QFI to the service data flow(s) is based on the binding parameters. When the PCF provisions a PCC rule, the SMF shall evaluate whether a QoS flow with the same binding parameters combination exists. If a QoS flow with the same binding parameters combination exists, the SMF allocates the same QFI to the service data flows that are assigned for the same values of the binding parameters. If no QoS flow exists, the SMF assigns a QFI for a new QoS flow, derives the QoS parameters for a new QoS flow, using authorized QoS in the PCC rule, and binds the PCC rule to the QoS flow.

NOTE 1: For non-GBR QoS flows, and when standardized 5QIs or pre-configured 5QIs are used, the 5QI value can be used as the QFI of the QoS flow. However, the pre-configured 5QI values cannot be used when the UE is roaming.

NOTE 2: For an unstructured PDU session, there is maximum one QoS flow.

The PCF shall supply the PCC rules to be installed, modified, or removed to the SMF. The SMF shall evaluate whether it is possible to use one of the existing QoS flows or not, and if applicable.

If the PCF removes an indication for the service data flow(s) to be bound to the QoS flow of the default QoS rule the binding is created between service data flow(s) and the QoS flow which have the same binding parameters.

If the PCC rule is removed, the SMF shall remove the association of the PCC rule to the QoS flow. Whenever the authorized QoS of a PCC rule changes, the existing QFI allocation shall be re-evaluated, i.e. the allocation procedure, is performed. The re-evaluation may, for a service data flow, require a new binding with another QoS flow.

NOTE 3: A QoS change of the default 5QI/ARP values doesn't cause the QoS flow rebinding for PCC rules previously bound to the QoS flow associated with the default QoS rule, with the "Bind to QoS flow associated with the default QoS rule" Indication set.

When a QoS flow is removed the SMF shall report to the PCF that the PCC rules bound to the corresponding QoS flow are removed.

7 QoS Parameters Mapping

This clause will describe the QoS parameters mapping for the 5G Policy Framework.

7.1 Overview

Several QoS parameters mapping functions are needed during PCC interaction. These functions are located at the AF, PCF, SMF and UE. The main purpose of these mapping functions is the conversion of QoS parameters from one format to another. QoS information may be:

- parts of a session description language (SDI), e.g. SDP, MPD;
- QoS parameters; and
- access specific QoS parameters.

One QoS mapping function is located at the AF, which maps the application specific information into the appropriate information that are carried over the Rx as specified in 3GPP TS 29.214 [18] or N5 interface as specified in 3GPP TS 29.514 [10].

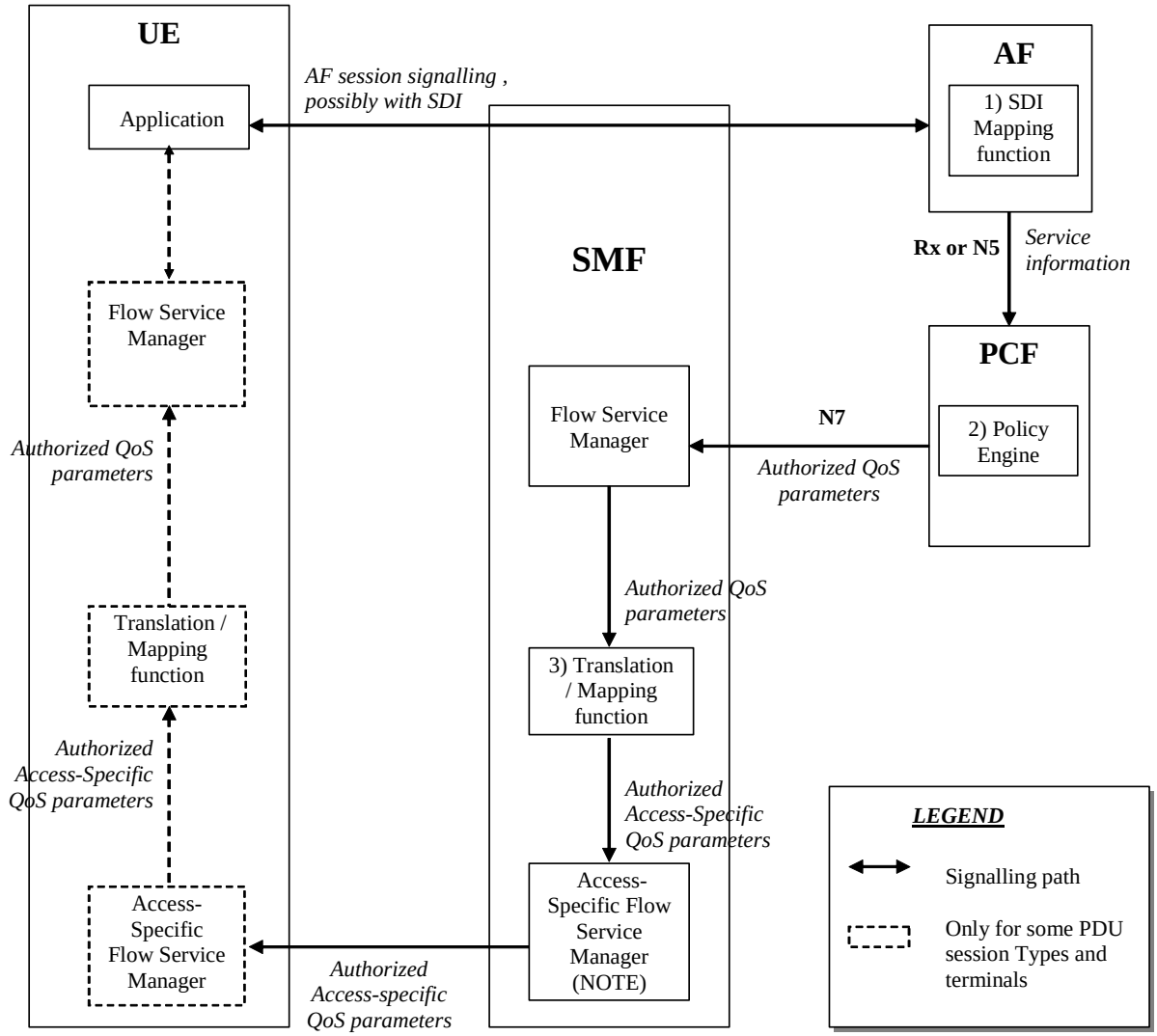
For IMS, the AF may pass service information to the PCF over the Rx interface. The AF derives information about the service from the SDI or from other sources. The mapping is application specific. If SDP (IETF RFC 4566 [16]) is used as SDI, the AF should apply the mapping described in subclause 7.2. If MPD (3GPP TS 26.247 [17]) is used, the AF may apply the mapping described in Annex X in 3GPP TS 26.247 [17]. Subclause 7.2 specifies the QoS parameter mapping functions at the AF. For IMS, the mapping rules in subclause 7.2 shall be used at the P-CSCF.

One QoS mapping function is located at the PCF, which maps the service information received over the Rx or N5 interface into QoS parameters (e.g. 5QI, GBR, MBR, and ARP). This mapping is access independent. Subclause 7.3 specifies the QoS mapping functions at the PCF applicable for all accesses.

The mapping functions located at SMF is specified in subclause 7.4. The mapping function in UE is implementation dependent and not specified within this specification.

The PCF notes and authorizes the service data flows described within this service information by mapping from service information to Authorized QoS parameters for transfer to the SMF via the N7 interface. The SMF will map from the Authorized QoS parameters to the access specific QoS parameters.

For 3GPP 5GS, the network sets up QoS flow(s) with a suitable QoS and indicates to the UE the QoS characteristics of those QoS flow(s). Therefore the flow of QoS related information will be unidirectional as indicated in the figure 7.1-1.



NOTE: Access Specific QoS parameters with Authorized Access-Specific QoS parameters comparison.

Figure 7.1-1: QoS mapping framework

1. The AF shall perform mapping from an SDI received within the AF session signalling to service information passed to the PCF over the Rx or N5 interface (see subclause 7.2 if SDP is used as SDI).

2. The PCF shall perform mapping from the service information received over the Rx or N5 interface to the Authorized QoS parameters that shall be passed to the SMF via the N7 interface. The mapping is performed for each service data flow. The PCF combines per direction the individual Authorized QoS parameters per flow (see subclause 7.3).

3. The SMF shall perform mapping from the Authorized QoS parameters received from PCF to the access specific QoS parameters.

7.2 QoS parameter mapping Functions at AF

7.3 QoS parameter mapping Functions at PCF

7.3.1 Introduction

The QoS authorization process consists of the derivation of the parameters Authorized 5G QoS Identifier (5QI), Authorized Allocation and Retention Priority (ARP) and Authorized Maximum/Guaranteed Data Rate UL/DL. And such process also includes the derivation of the QoS Notification Control (QNC), Reflective QoS Attribute (RQA), Priority Level (PL), Averaging Window (AW) and Maximum Data Burst Volume (MDBV).

When a session is initiated or modified the PCF shall derive Authorized QoS parameters from the service information received from an AF supporting Rx interface or from an AF supporting N5 interface.

7.3.2 PCF Interworking with an AF supporting Rx interface

When the AF interworks with the PCF using the Rx interface, the session binding in the PCF shall be always associated to an IP session and the PCF shall derive IP QoS parameters for the related IP flows.

In the case of SIP forking, the various forked responses may have different QoS requirements for the IP flows of the same media component. Each Authorized IP QoS Parameter should be set to the highest value requested for the IP flow(s) of that media component by any of the active forked responses.

Table 7.3.2-1: Rules for derivation of the Maximum Authorized Data Rates, Authorized Guaranteed Data Rates and Maximum Authorized QoS Class per service data flow or bidirectional combination of service data flows in the PCF

Authorized QoS Parameter	Derivation from service information (see NOTE 4)

Maximum Authorized Data Rate DL (Max_DR_DL) and UL (Max_DR_UL)	

```
IF operator special policy exists THEN
  Max_DR_UL:= as defined by operator specific algorithm;
  Max_DR_DL:= as defined by operator specific algorithm;

ELSE

  IF AF Application Identifier demands application specific data rate
  handling THEN
    Max_DR_UL:= as defined by application specific algorithm;
    Max_DR_DL:= as defined by application specific algorithm;

  ELSE IF Codec Data provides Codec information for a codec that is
  supported by a specific algorithm (NOTE 5, 12 and 13) THEN
    Max_DR_UL:= as defined by specific algorithm;
    Max_DR_DL:= as defined by specific algorithm;

  ELSE
    IF not RTCP flow(s) according to Flow Usage THEN
      IF Flow Status indicates “REMOVED” THEN
        Max_DR_UL:= 0;
        Max_DR_DL:= 0;
      ELSE
        IF Uplink Flow Description is supplied THEN
          IF Maximum UL Supported Bandwidth is present and supported THEN
             Max_DR_UL:= Maximum UL Supported Bandwidth;
         ELSE IF Maximum UL Requested Bandwidth is present THEN
            Max_DR_UL:= Maximum UL Requested Bandwidth;
          ELSE
            Max_DR_UL:= as set by the operator;
          ENDIF;
        ELSE
          Max_DR_UL:= 0;
        ENDIF;

        IF Downlink Flow Description is supplied THEN
          IF Maximum DL Supported Bandwidth is present and supported THEN
            Max_DR_DL:= Maximum DL Supported Bandwidth;
          ELSE IF Maximum DL Requested Bandwidth is present THEN
            Max_DR_DL:= Maximum DL Requested Bandwidth;
          ELSE
            Max_DR_DL:= as set by the operator;
          ENDIF;
        ELSE
          Max_DR_DL:= 0;
        ENDIF;
      ENDIF;

    ELSE /* RTCP IP flow(s) */
      IF RS Bandwidth is present and RR Bandwidth is present THEN
        Max_DR_UL:= (RS Bandwidth + RR Bandwidth);
        Max_DR_DL:= (RS Bandwidth + RR Bandwidth);
      ELSE
        IF Maximum UL Requested Bandwidth is present THEN
          IF RS Bandwidth is present and RR Bandwidth is not present THEN
            Max_DR_UL:= MAX[0.05 * Maximum UL Requested Bandwidth, RS
Bandwidth];
          ENDIF;

          IF RS Bandwidth is not present and RR Bandwidth is present THEN
            Max_DR_UL:= MAX[0.05 * Maximum UL Requested Bandwidth, RR
Bandwidth];
          ENDIF;
          IF RS Bandwidth and RR Bandwidth are not present THEN
            Max_DR_UL:= 0.05 * Maximum UL Requested Bandwidth;
          ENDIF;

        ELSE
          Max_DR_UL:= as set by the operator;
        ENDIF;

        IF Maximum DL Requested Bandwidth is present THEN
          IF RS Bandwidth is present and RR Bandwidth is not present THEN
            Max_DR_DL:= MAX[0.05 * Maximum DL Requested Bandwidth, RS
Bandwidth];
          ENDIF;

          IF RS Bandwidth is not present and RR Bandwidth is present THEN
```

Authorized QoS Parameter	Derivation from service information (see NOTE 4)

	Max_DR_DL:= MAX[0.05 * Maximum DL Requested Bandwidth, RR Bandwidth];
	ENDIF;
	
	IF RS Bandwidth and RR Bandwidth are not present THEN
	Max_DR_DL:= 0.05 * Maximum DL Requested Bandwidth;
	ENDIF;
	
	ELSE
	Max_DR_DL:= as set by the operator;
	ENDIF;
	
	ENDIF;
	ENDIF;
	ENDIF;
	ENDIF;
	
	IF SIP Forking Indication indicates “SEVERAL DIALOGUES” THEN
	Max_DR_UL = MAX[Max_DR_UL, previous Max_DR_UL]
	Max_DR_DL = MAX[Max_DR_DL, previous Max_DR_DL]
	ENDIF;

Authorized QoS Parameter	Derivation from service information (see NOTE 4)

Authorized Guaranteed Data Rate DL (Gua_DR_DL) and UL (Gua_DR_UL) (see NOTE 6, 8, 9 and 10)	IF operator special policy exists THEN
	  Gua_DR_UL:= as defined by operator specific algorithm;
	  Gua_DR_DL:= as defined by operator specific algorithm;
	
	ELSE
	  IF AF Application Identifier demands application specific data rate handling THEN
	  Gua_DR_UL:= as defined by application specific algorithm;
	  Gua_DR_DL:= as defined by application specific algorithm;
	
	  ELSE IF Codec Data provides Codec information for a codec that is supported by a specific algorithm (NOTE 5, 12 and 13) THEN
	  Gua_DR_UL:= as defined by specific algorithm;
	  Gua_DR_DL:= as defined by specific algorithm;
	
	  ELSE
	  IF Uplink Flow Description is supplied THEN
	  IF Minimum UL Desired Bandwidth is present and supported THEN
	  Gua_DR_UL:= Minimum UL Desired Bandwidth;
	  ELSE IF Minimum UL Requested Bandwidth is present THEN
	  Gua_DR_UL:= Minimum UL Requested Bandwidth;
	  ELSE
	  Gua_DR_UL:= as set by the operator;
	  ENDIF;
	
	  ELSE
	  Gua_DR_UL:= Max_DR_UL;
	
	  ENDIF;
	
	  IF Downlink Flow Description is supplied THEN
	  IF Minimum DL Desired Bandwidth is present and supported THEN
	  Gua_DR_DL:= Minimum DL Desired Bandwidth;
	  ELSE IF Minimum DL Requested Bandwidth is present THEN
	  Gua_DR_DL:= Minimum DL Requested Bandwidth;
	  ELSE
	  Gua_DR_DL:= as set by the operator;
	  ENDIF;
	
	  ELSE
	  Gua_DR_DL:= Max_DR_DL;
	
	  ENDIF;
	  ENDIF;
	ENDIF;
	
	IF SIP Forking Indication indicates “SEVERAL DIALOGUES” THEN
	  Gua_DR_UL = MAX[Gua_DR_UL, previous Gua_DR_UL]
	  Gua_DR_DL = MAX[Gua_DR_DL, previous Gua_DR_DL]
	ENDIF;

Authorized QoS Parameter	Derivation from service information (see NOTE 4)

Authorized 5G QoS Identifier (5QI) (see NOTE 1, 2, 3 and 7)	IF an operator special policy exists THEN
	  5QI:= as defined by operator specific algorithm;
	
	ELSE IF MPS Identifier demands MPS specific QoS Class handling THEN
	  5QI:= as defined by MPS specific algorithm (NOTE 11);
	ELSE IF AF Application Identifier demands application specific QoS Class handling THEN
	  5QI:= as defined by application specific algorithm;
	
	ELSE IF Codec Data provides Codec information for a codec that is supported by a specific algorithm THEN
	  5QI:= as defined by specific algorithm; (NOTE 5)
	ELSE
	  /* The following 5QI derivation is an example of how to obtain the 5QI values in a 5GS network */
	  IF Media Type is present THEN
	  CASE Media Type OF
	  “audio”: 5QI := 1;
	  “video”: 5QI := 2;
	  “application”: 5QI := 1 OR 2;
	Editor's note: 5QI derivation for other media types is FFS.
	
	/* NOTE: include new media types here */
	
	  OTHERWISE: 5QI := 9;
	  /*e.g. for TCP-based generic traffic */
	
	  END;
	  ENDIF;
	ENDIF;
	
	IF SIP Forking Indication indicates “SEVERAL DIALOGUES” THEN
	  5QI = MAX[5QI, previous 5QI]
	ENDIF ;

NOTE 1: The 5QI assigned to a RTCP IP flow is the same as for the corresponding RTP media IP flow.
NOTE 2: When audio or video IP flow(s) are removed from a session, the 5QI shall keep the originally assigned value.
NOTE 3: When audio or video IP flow(s) are added to a session, the PCF shall derive the 5QI taking into account the already existing media IP flow(s) within the session.
NOTE 4: The encoding of the service information is defined in 3GPP TS 29.214 [18] and 3GPP TS 29.201 [15]. If AVPs are omitted within a Media Component Description or Media Subcomponent of the service information, the corresponding information from previous service information shall be used, as specified in 3GPP TS 29.214 [18] and 3GPP TS 29.201 [15].
NOTE 5: 3GPP TS 26.234 [19], 3GPP TS 26.114 [14], 3GPP2 C.S0046 [20], and 3GPP2 C.S0055 [21] contain examples of QoS parameters for codecs of interest. The support of any codec specific algorithm in the PCF is optional.
NOTE 6: Authorized Guaranteed Data Rate DL and UL shall not be derived for non-GBR 5QI values.
NOTE 7: Recommended 5QI values for standardised 5QI characteristics are shown in table 5.7.4-1 in 3GPP TS 23.501 [2].
NOTE 8: The PCF may be configured with operator specific preconditions for setting the Authorized Guaranteed Data Rate lower than the corresponding Maximum Authorized Data Rate.
NOTE 9: For certain services (e.g. DASH services according to 3GPP TS 26.247 [17]), the AF may also provide a minimum required bandwidth so that the PCF can derive an Authorized Guaranteed Data Rate lower than the Maximum Authorized Data Rate.
NOTE 10: For 5GS, the PCF shall assign an Authorized Guaranteed Data Rate UL/DL value within the limit supported by the serving network.
NOTE 11: The MPS specific algorithm shall consider various inputs, including the received MPS Identifier and Reservation Priority, for deriving the 5QI.
NOTE 12: When multiple codecs are supported per media stream (e.g. as part of multi-stream multiparty conferencing media handling are negotiated as described in 3GPP TS 26.114 [14]) the codec specific algorithm shall consider the bandwidth related to each codec when calculating the total bandwidth.
NOTE 13: 3GPP TS 26.114 [14] contains examples of how the Authorized Guaranteed Data Rate and Maximum Authorized Data Rate are assumed to be derived for multi-party multimedia conference media handling support. The support of this behaviour is optional.

The PCF should per ongoing session store the Authorized QoS parameters for each service data flow or bidirectional combination of service data flows (as described within a Media Subcomponent).

If the PCF provides a QoS information associated to a PCC rule it may apply the rules in table 7.3.2-2 to combine the Authorized QoS per service data flow or bidirectional combination of service data flows (as derived according to table 7.3.2-1) for all service data flows described by the corresponding PCC rule.

If the PCF provides a QoS information associated to a PDU session (i.e. QoS flow with default QoS rule), it may apply the rules in table 7.3.2-2 to combine the Authorized QoS per service data flow or bidirectional combination of service data flows (as derived according to table 7.3.2-1) for all service data flows allowed to be transported within the PDU session. It is recommended that the rules in table 7.3.2-2 are applied for all service data flows with corresponding AF session. The PCF may increase the authorized QoS further to take into account the requirements of predefined PCC rules without ongoing AF sessions.

NOTE 1: QoS Information related to Maximum Authorized UL/DL Data Rate provided at PDU session level is not derived based on mapping tables in this subclause, but based on subscription and operator specific policies.

NOTE 2: ARP is always calculated at PCC rule level according to table 7.3.2-2.

Table 7.3.2-2: Rules for calculating the Maximum Authorized/Guaranteed Data Rates, 5QI and ARP in the PCF

Authorized QoS Parameter	Calculation Rule
Maximum Authorized Data Rate DL and UL	Maximum Authorized Data Rate DL/UL is the sum of all Maximum Authorized Data Rate DL/UL for all the service data flows or bidirectional combinations of service data flows (as according to table 7.3.2-1).
Guaranteed Authorized Data Rate DL and UL (NOTE 3)	Guaranteed Authorized Data Rate DL/UL is the sum of all Guaranteed Authorized Data Rate DL/UL for all the service data flows or bidirectional combinations of service data flows (as according to table 7.3.2-1).
5QI	5QI = MAX [needed QoS parameters per service data flow or bidirectional combination of service data flows (as operator's defined criteria) among all the service data flows or bidirectional combinations of service data flows.]

ARP (NOTE 1)	IF an operator special policy exists THEN
	ARP:= as defined by operator specific algorithm;
	
	ELSE IF MPS Identifier demands MPS specific ARP handling THEN
	ARP:= as defined by MPS specific algorithm (NOTE 2);
	ELSE IF AF Application Identifier demands application specific ARP handling THEN
	ARP:= as defined by application specific algorithm;
	ELSE IF Reservation Priority demands application specific ARP handling THEN
	ARP:= as defined by application specific algorithm;
	ENDIF;

NOTE 1: The ARP priority levels 1-8 should only be assigned to resources for services that are authorized to receive prioritized treatment within an operator domain. NOTE 2: The MPS specific algorithm shall consider various inputs, including the received MPS Identifier and Reservation Priority, for deriving the ARP. NOTE 3: The PCF may check that the Guaranteed Authorized Data Rate DL/UL does not exceed the limit supported by the serving network to minimize the risk of rejection of the bearer by the serving network.	

7.3.3 PCF Interworking with an AF supporting N5 interface

Editor's Note: QoS mapping table when N5 interface is supported is FFS.

7.4 QoS parameter mapping Functions at SMF

8 PCF addressing

8.1 General

The PCF discovery and selection procedures are needed when there are multiple and separately addressable PCFs in a PLMN. It is also possible that a PCF may serve only specific DN(s).

These procedures correlate the AF service session establishment over N5 or Rx with the associated PDU session (Session binding) handled over N7.

Editor's note: The details for Rx are FFS.

These procedures enable the AMF and SMF to address the PCF.

These procedures enable the NEF to address the PCF.

8.2 PCF discovery and selection by the AMF

The AMF selects the PCF for a UE. In the roaming case, the AMF selects the V-PCF and the H-PCF for a UE.

The AMF may utilize the Nnrf_NFDiscovery service of the Network Repository Function to discover the PCF instance(s) unless PCF information is available by other means, e.g. locally configured on AMF. Local operator policies may be considered during the PCF selection.

8.3 PCF discovery and selection by the SMF

The SMF selects the PCF for a PDU session. The selected PCF may be the same or a different one than the PCF selected by the AMF.

The SMF may utilize the Nnrf_NFDiscovery service of the Network Repository Function to discover the PCF instance(s) unless PCF information is available by other means, e.g. locally configured on SMF or received during the PDU Session Establishment procedure from the AMF. The following factors may be considered during the PCF selection.

- Local operator policies.
- Selected Data Network Name (DNN).
- PCF selected by the AMF

8.4 PCF discovery and selection by the AF

8.4.1 General

When multiple and separately addressable PCFs have been deployed, the BSF is required in order to ensure that an AF for a certain PDU session reaches over N5/Rx the PCF holding the PDU session information. The AF can also select a PCF based on local configuration for Ethernet PDU sessions.

8.4.2 Binding Support Function (BSF)

The BSF has the following characteristics:

a) The BSF has information about the user identity, the DNN, the UE (IP or Ethernet) address(es) and the selected PCF address for a certain PDU session. This information is stored internally in the BSF. Optionally, the BSF can store the binding information in the UDR as structured data by invoking the Nudr_DataRepository_Update service operation, as defined in 3GPP TS 29.519 [12].

b) For the storage of binding information, the PCF utilizes the Nbsf_management service of the BSF to register, update or remove the binding information from the BSF. The PCF ensures that the binding information is

updated each time an IP address is allocated or released for the PDU Session or, for Ethernet PDU Sessions, each time the PCF is notified that a MAC address is taken into use or no more used in the PDU Session.

c) For the retrieval of binding information, any NF, such as NEF or AF, that needs to discover the selected PCF for the tuple (UE address, DNN, SUPI, GPSI, S-NNSAI, NSI ID) (or for a subset of this tuple) uses the Nbsf_Management_Discovery service operation as defined in 3GPP TS 29.521 [22].

d) The BSF is able to proxy or redirect Rx requests based on the IP address of a UE. For any AF using Rx, such as P-CSCF, the BSF determines the selected PCF address according to the information carried by the incoming Rx requests.

e) The BSF may be deployed standalone or may be collocated with other network functions such as the PCF, UDR, NRF, and SMF.

NOTE: Collocation allows combined implementation.

f) The NF may discover the BSF via NRF by invoking the Nnrf_NFDiscovery service operation or based on local configuration. In case of via NRF the BSF registers the NF profile in NRF. The Range(s) of UE IPv4 addresses, Range(s) of UE IPv6 prefixes supported by the BSF may be provided to NRF.

8.5 BSF procedures

8.5.1 General

These procedures concern the storage of binding information in the BSF and the retrieval of binding information from the BSF.

8.5.2 Binding information Creation

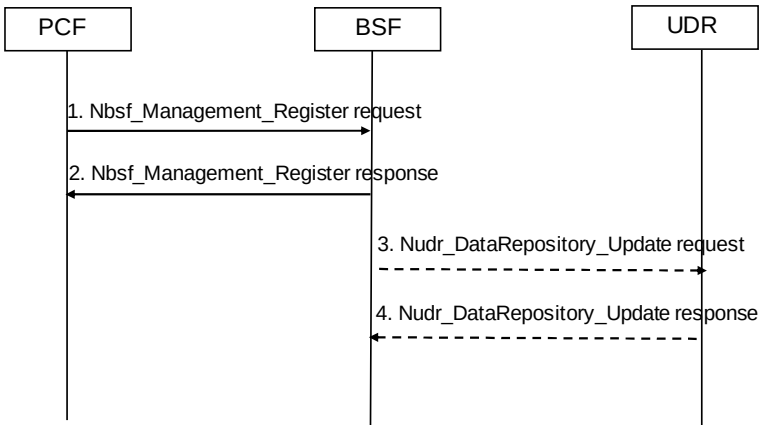


Figure 8.5.2-1 Bind information Creation procedure

1. When an IP address is allocated for the PDU session, or a MAC address is used for the Ethernet PDU session, the PCF invokes the Nbsf_Management_Register service operation by sending the HTTP POST request with "{apiRoot}/nbsf-management/v1/pcfBindings" as Resource URI to store the binding information in the BSF. The binding information provided in the HTTP request is defined in subclause 4.2.2.2 of 3GPP TS 29.521[22].

2. The BSF sends an HTTP "201 Created" response to the PCF and stores the binding information.

3. Optionally, the BSF invokes Nudr_DataRepository_Update service operation to store the binding information in the UDR.

4. The UDR acknowledges the Nudr_DataRepository_Update service operation.

8.5.3 Binding information Deletion

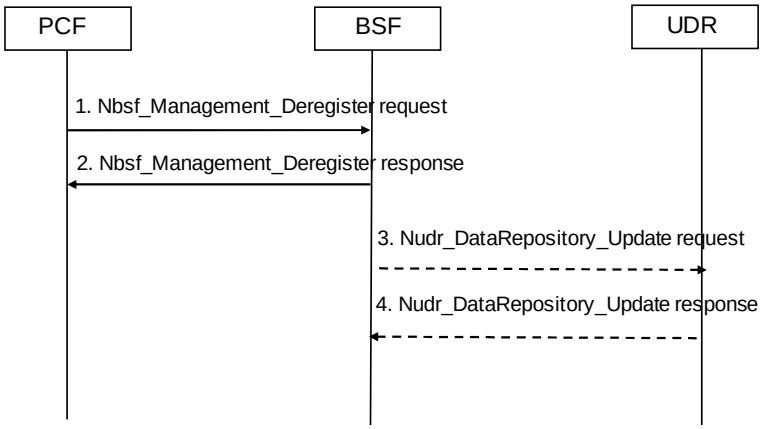


Figure 8.5.3-1 Bind information Deletion procedure

1. When the IP address is released or the MAC address is not used for a certain PDU session, the PCF invokes the Nbsf_Management_Deregister service operation by sending the HTTP DELETE request with "{apiRoot}/nbsf-management/v1/pcfBindings/{bindingId}" as Resource URI to request the BSF to remove the binding information.
2. The BSF sends an HTTP "204 No Content" response to the PCF and removes the binding information which is stored locally.
3. The BSF invokes Nudr_DataRepository_Update service operation to remove the binding information if the binding information is stored in the UDR.
4. The UDR acknowledges the Nudr_DataRepository_Update service operation.

8.5.4 Binding information Retrieval

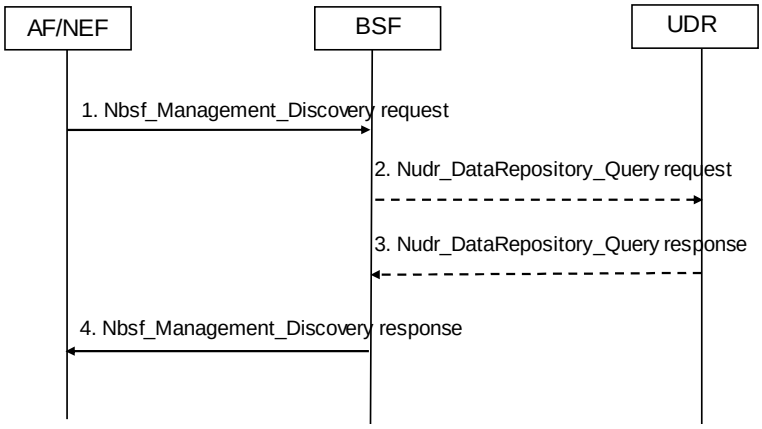


Figure 8.5.4-1 Bind information Retrieval procedure

1. AF/NEF invokes the Nbsf_Management_Descovery service operation by sending the HTTP GET request with "{apiRoot}/nbsf-management/v1/pcfBindings?query_parameters" as Resource URI to the BSF to obtain the selected PCF ID for a certain PDU session,
2. The BSF invokes the Nudr_DataRepository_Query service operation to the UDR to obtain the selected PCF ID for a certain PDU session, if the binding information is stored in the UDR.
3. The UDR responds to the BSF with the PCF ID.
4. The BSF sends an HTTP "200 OK" response to the AF/NEF with the PCF ID.

Annex A (informative): Change history

Change history							
Date	**Meeting**	**TDoc**	**CR**	**Rev**	**Cat**	**Subject/Comment**	**New version**
2017-10						TS skeleton of policy and charging signalling and QoS parameters mapping	0.0.0
2017-10	CT3#92	C3-175378				Inclusion of C3-175332, C3-175355.	0.1.0
2017-12	CT3#93	C3-176398				Inclusion of C3-176258, C3-176372	0.2.0
2018-01	CT3#94	C3-180363				Inclusion of C3-180069, C3-180246, C3-180277, C3-180317	0.3.0
2018-03	CT3#95	C3-181369				Inclusion of C3-181250, C3-181251, C3-181252	0.4.0
2018-04	CT3#96	C3-182517				Inclusion of C3-182222, C3-182340, C3-182341, C3-182342, C3-182343, C3-182374, C3-182375, C3-182376, C3-182377, C3-182378.	0.5.0
2018-05	CT3#97	C3-183901				Inclusion of C3-183385, C3-183387, C3-183388, C3-183495, C3-183496, C3-183497, C3-183503, C3-183527, C3-183528, C3-183529, C3-183530, C3-183823, C3-183828	0.6.0
2018-06	CT#80	CP-181035				TS sent to plenary for approval	1.0.0
2018-06	CT#80	CP-181035				TS approved by plenary	15.0.0

History

Document history		
V15.0.0	June 2018	Publication