ETSI TS 129 513 V15.6.0 (2020-01)

5G;
5G System;
Policy and Charging Control signalling flows and QoS parameter mapping;
Stage 3
(3GPP TS 29.513 version 15.6.0 Release 15)

Reference
RTS/TSGC-0329513vf60

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.

Legal Notice

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. These shall be interpreted as being references to the corresponding ETSI deliverables.

The cross reference between 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, Nchf, Nbsf 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], 3GPP TS 29.525 [31] 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".

[29] IETF RFC 6733: "Diameter Base Protocol".

[30] 3GPP TS 29.213: "Policy and charging control signalling flows and Quality of Service (QoS) parameter mapping".

[31] 3GPP TS 29.525: "UE Policy Control Service; Stage 3".

[32] 3GPP TS 29.518: "Access and Mobility Management Services; Stage 3".

[33] 3GPP TS 24.501: " Non-Access-Stratum (NAS) protocol for 5G System (5GS); Stage 3".

3 Definitions, symbols and abbreviations

3.1 Definitions

For the purposes of the present document, the terms and definitions given in 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 TR 21.905 [1].

3.2 Abbreviations

For the purposes of the present document, the abbreviations given in 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 TR 21.905 [1].

5GC	5G Core Network
5QI	5G QoS Identifier
AF	Application Function
AMBR	Aggregate Maximum Bit Rate
AMF	Access and Mobility Management Function
ARP	Allocation and Retention Priority
AW	Average Window
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
PDB	Packet Delay Budget
PER	Packet Error Rate
PFD	Packet Flow Description
PFDF	Packet Flow Description Function
PL	Priority Level
QNC	QoS Notification Control
QoS	Quality of Service
SDP	Session Description Protocol
SEPP	Security Edge Protection Proxy
SMF	Session Management Function
S-NSSAI	Single Network Slice Selection Assistance Information
UDR	Unified Data Repository
UPF	User Plane Function
UPSI	UE policy section identifier

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). For the roaming scenario, the Security Edge Protection Proxy (SEPP) is deployed between the V-PCF and H-PCF.
3GPP TS 23.503 [4] specifies the 5G policy framework stage 2 functionality.

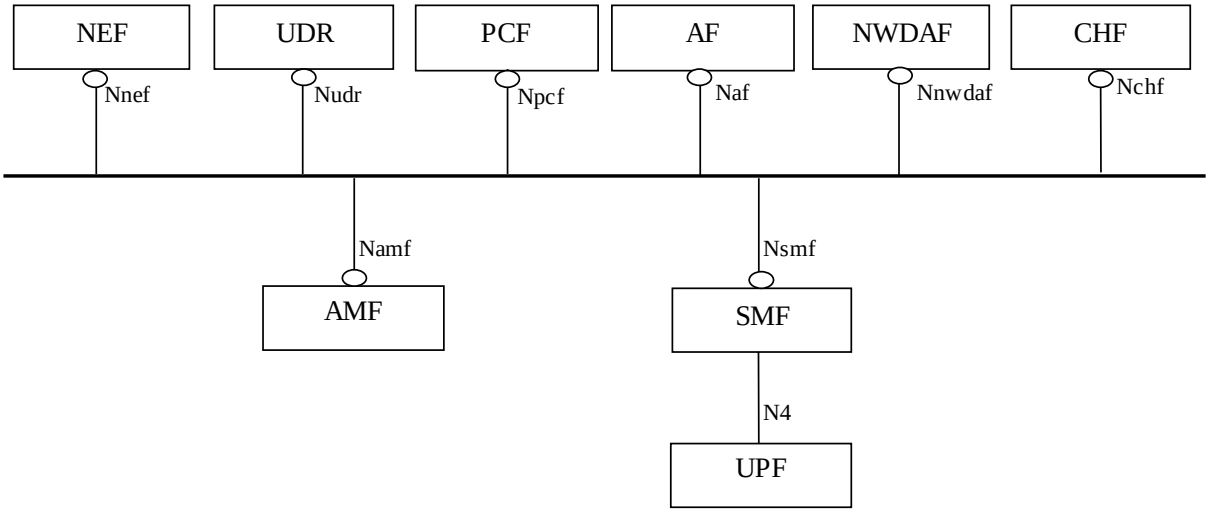


Figure 4.1-1a: Overall non-roaming 5G Policy framework architecture (service based representation)

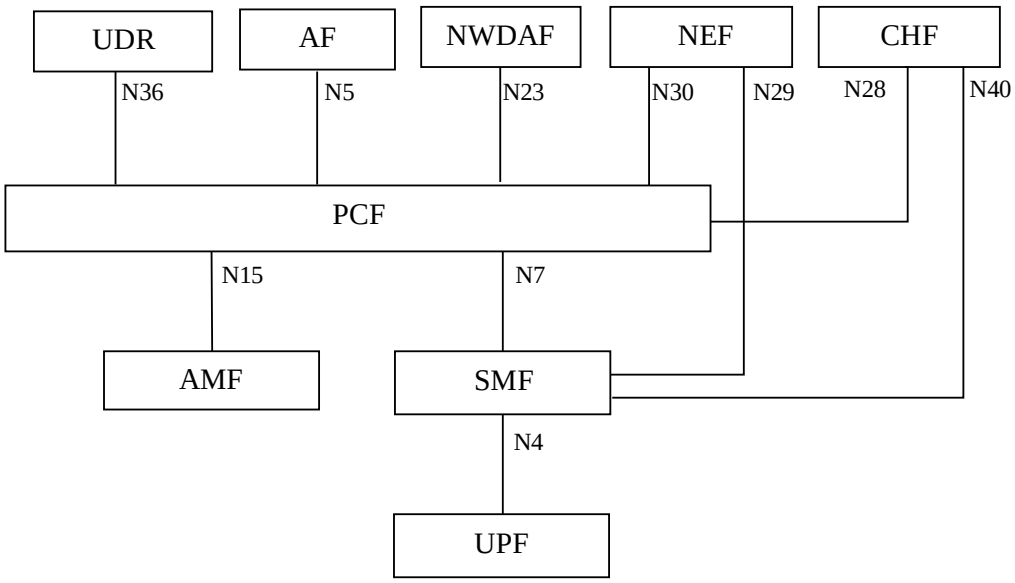


Figure 4.1-1b: Overall non-roaming 5G Policy framework architecture (reference point representation)

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

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].

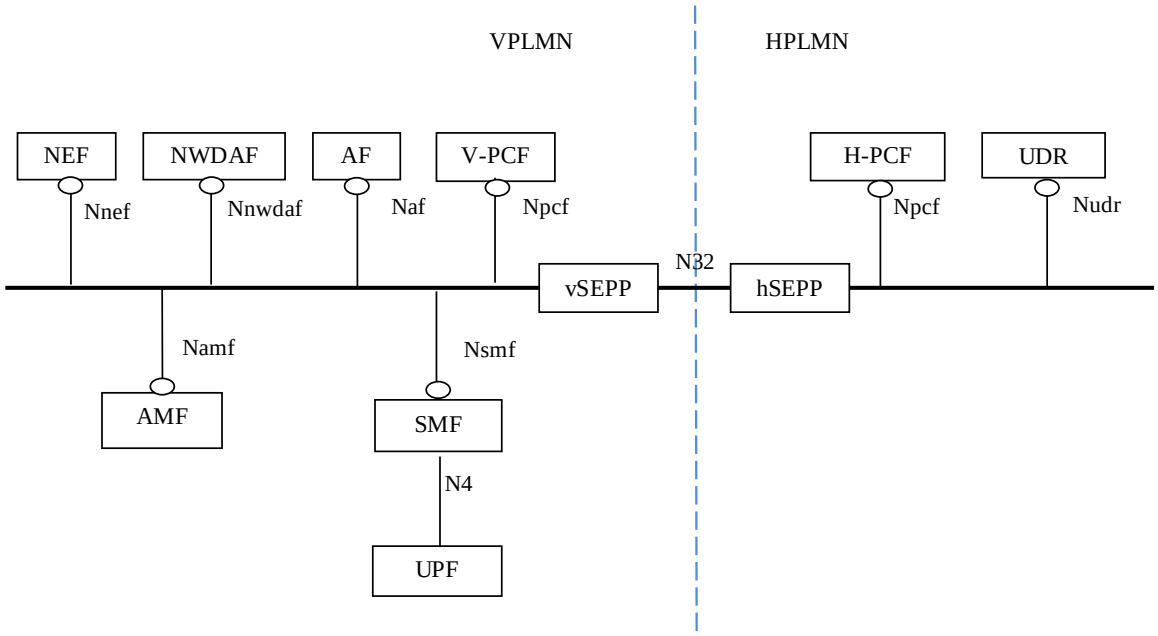


Figure 4.1-2a: Overall roaming policy framework architecture - LBO (service based representation)

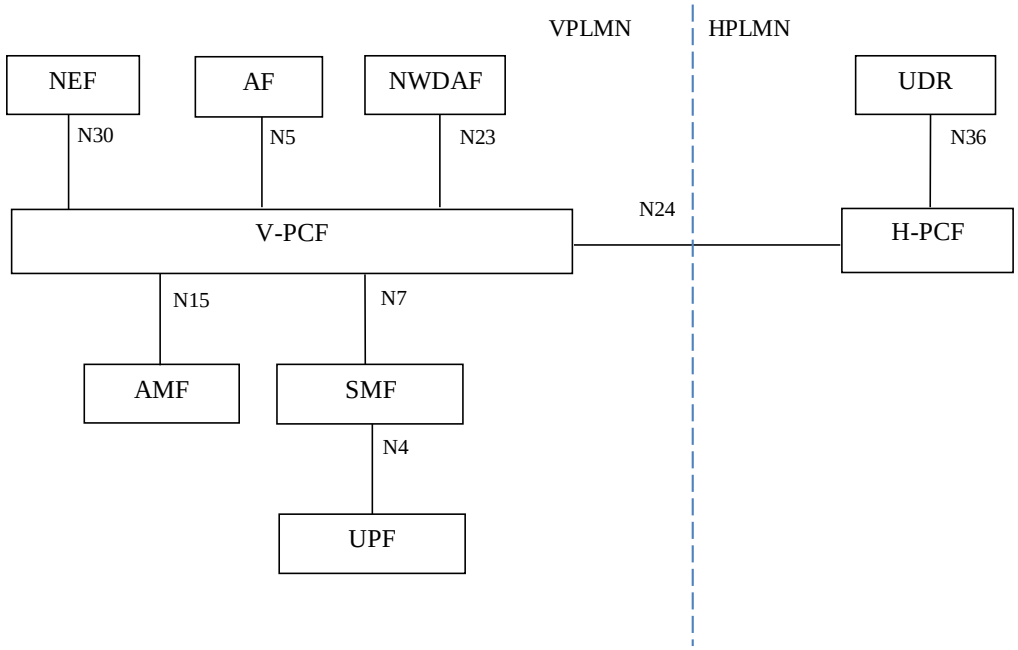


Figure 4.1-2b: Overall roaming policy framework architecture - LBO (reference point representation)

NOTE 2: 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 3: 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].

NOTE 4: For the sake of clarity, SEPPs are not depicted in the roaming reference point architecture figures.

NOTE 5: N4 and N32 are not service based interfaces.

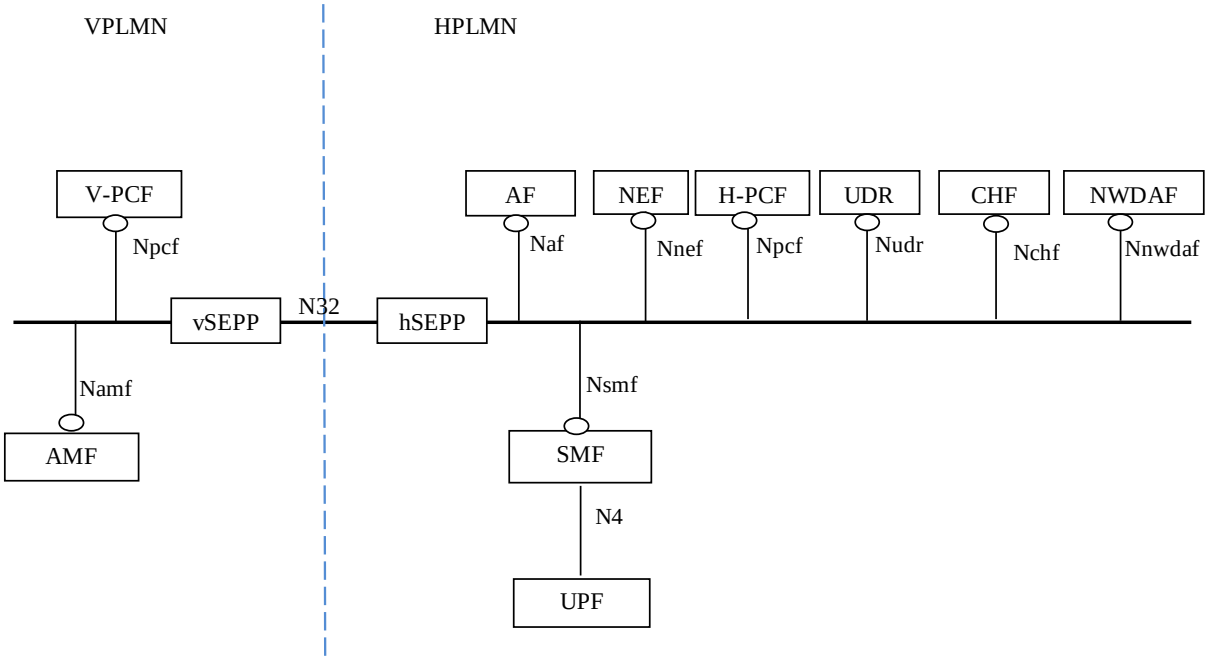


Figure 4.1-3a: Overall roaming policy framework architecture - home routed scenario (service based representation)

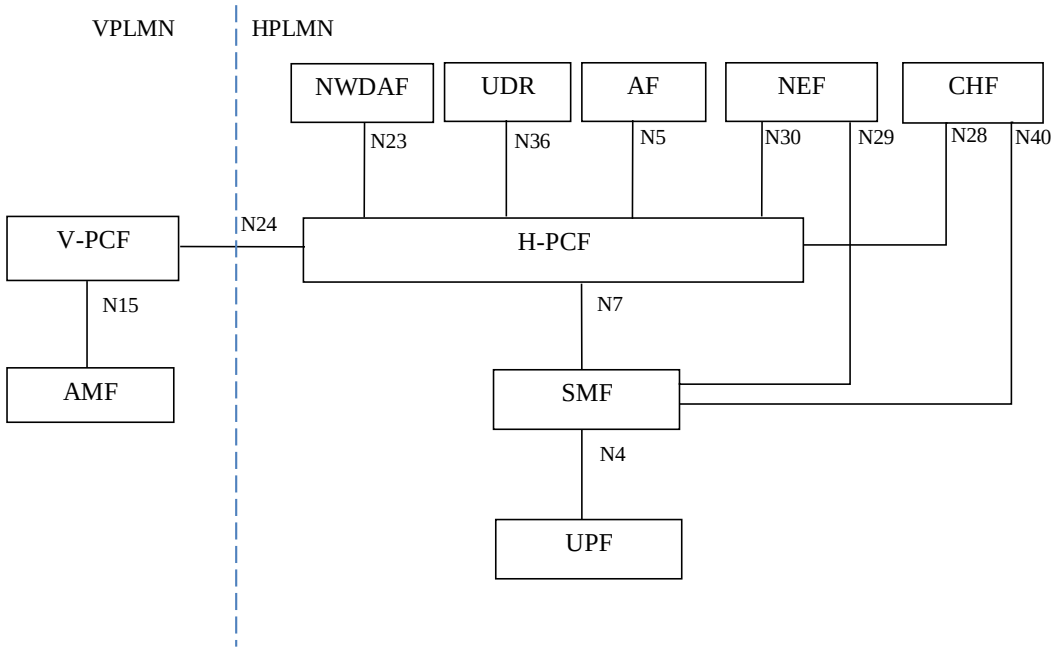


Figure 4.1-3b: Overall roaming policy framework architecture - home routed scenario (reference point representation)

NOTE 6: For the sake of clarity, SEPPs are not depicted in the roaming reference point architecture figures.

NOTE 7: N4 and N32 are not service based interfaces.

To allow the 5G system to interwork with AFs related to existing services, e.g. IMS based services, Mission Critical Push To Talk services, the PCF shall support the corresponding Rx procedures and requirements defined in 3GPP TS 29.214 [18]. This facilitates the migration from EPC to 5GC without requiring these AFs to upgrade to support the N5 interface.

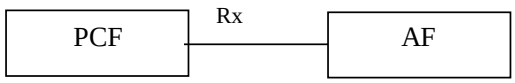


Figure 4.1-4: Interworking between 5G Policy framework and AFs supporting Rx interface

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 with PCF change in handover procedure and registration procedure.
3. UE registers with 5GS during the UE moving from EPS to 5GS when there is no existing AM Policy Association.

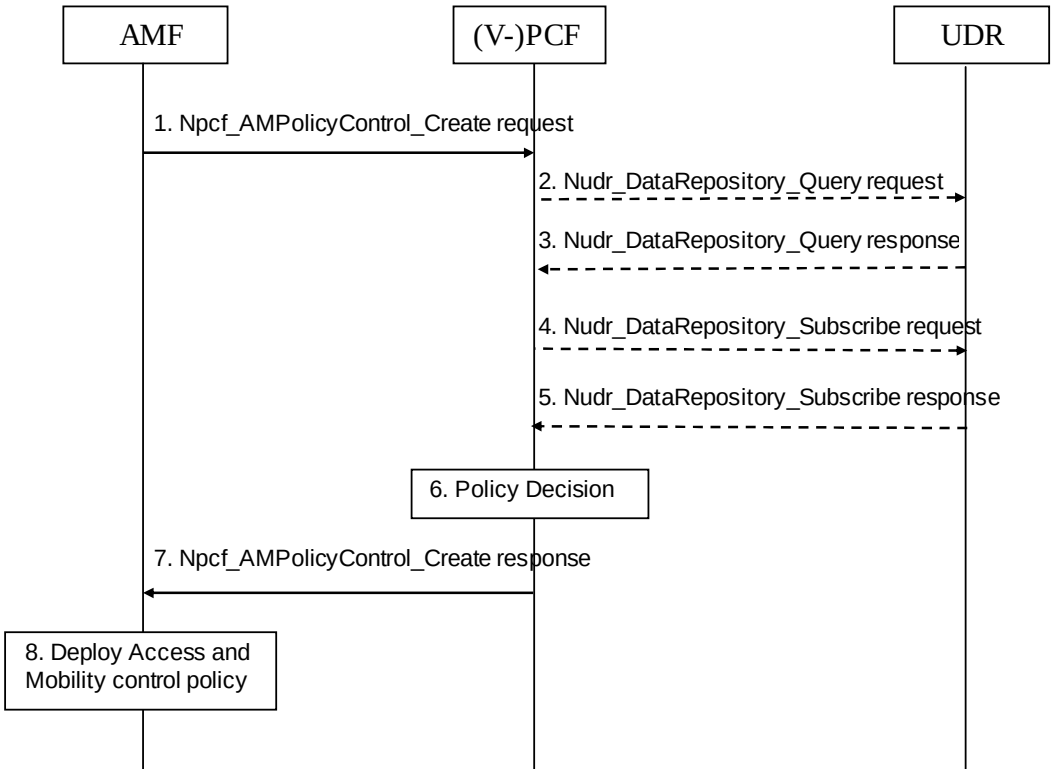


Figure 5.1.1-1: AM Policy Association Establishment procedure

This procedure concerns both roaming and non-roaming scenarios.

In the non-roaming case the role of the V-PCF is performed by the PCF. For the roaming scenarios, the V-PCF interacts with the AMF.

Step 2 - step 5 are not executed in the roaming case.

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 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 "AM Policy Associations" resource. 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 request includes a Notification URI to indicate to the PCF where to send a notification when the policy is updated.

2. If the PCF does not have the subscription data, it invokes the Nudr_DataRepository_Query service operation to the UDR by sending an HTTP GET request to the "AccessAndMobilityPolicyData " resource as specified in TS 29.519 [12]

3. The UDR sends an HTTP "200 OK" response to the PCF with the subscription data.

4. The PCF may request notifications from the UDR on changes in the subscription information by invoking Nudr_DataRepository_Subscribe service operation by sending an HTTP POST request to the "PolicyDataSubscriptions" resource as specified in 3GPP TS 29.519 [12].

5. The UDR sends an HTTP "201 Created" response to acknowledge the subscription from the PCF.

6. The (V-)PCF makes the requested policy decision including Access and Mobility control policy information, and may determine applicable Policy Control Request Trigger(s).

7. The (V)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]:

   - 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;

NOTE: 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.

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

5.1.2 AM Policy Association Modification

5.1.2.1 AM Policy Association Modification initiated by the AMF

5.1.2.1.1 AM Policy Association Modification initiated by the AMF without AMF relocation

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

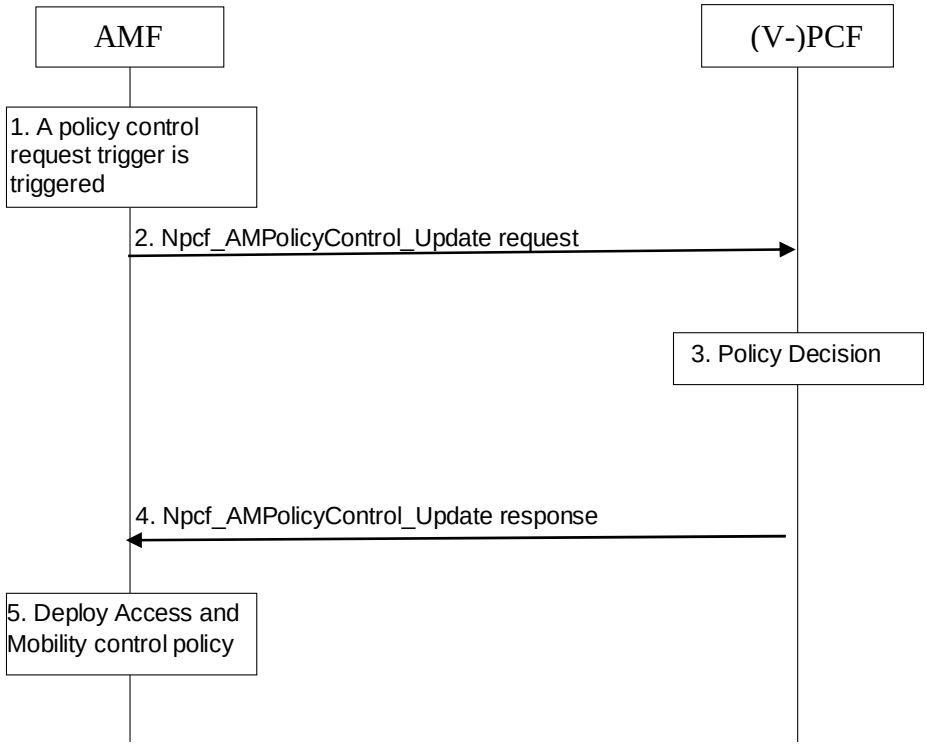


Figure 5.1.2.1.1-1: AMF-initiated AM Policy Association Modification without AMF relocation procedure

This procedure concerns both roaming and non-roaming scenarios.

In the non-roaming case the role of the V-PCF is performed by the PCF. For the roaming scenarios, the V-PCF interacts with the AMF.

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 "Individual AM Policy Association" resource with information on the conditions that have changed.
3. The (V)PCF stores the information received in step 2 and makes the policy decision.
4. The (V)PCF sends an HTTP "200 OK" response to the AMF with the updated Access and Mobility control policy information and/ or the updated Policy Control Request Trigger parameters.
5. The AMF deploys the Access and Mobility control policy if received, which includes storing the Service Area Restrictions, provisioning the Service Area Restrictions to the NG-RAN and UE, and/or provisioning the RFSP index to the NG-RAN.

5.1.2.1.2 AM Policy Association Modification with old PCF during AMF relocation

This procedure is performed when AMF relocation is performed and the old PCF is selected by the target AMF.

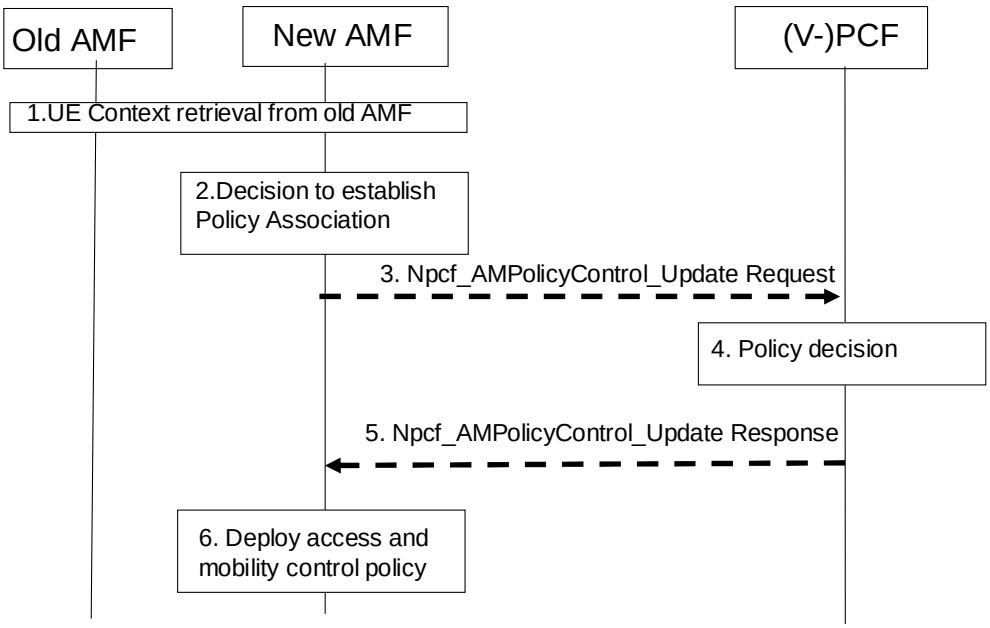


Figure 5.1.2.1.2-1: AMF-initiated AM Policy Association Modification with old PCF during AMF relocation procedure

This procedure concerns both roaming and non-roaming scenarios.

In the non-roaming case the role of the V-PCF is performed by the PCF. For the roaming scenarios, the V-PCF interacts with the AMF.

1. When the old AMF and the new AMF belong to the same PLMN, the old AMF transfers to the new AMF about the AM Policy Association information including policy control request trigger(s) and the resource URI (i.e. {apiRoot}/npcf-am-policy-control/v1/policies/{polAssoId}) of AM Policy Association at the (V-)PCF).

2. Based on local policies, the new AMF decides to contact with (V-)PCF and update the resource identified by the resource URI received in step 1.

3. The new AMF invokes the Npcf_AMPolicyControl_Update service operation to the (V-) PCF by sending the HTTP POST request to the "Individual AM Policy Association" resource with the Notification URI of the new AMF. The request may also include the met policy control request trigger(s) and corresponding information.

4. The (V-)PCF updates the stored information provided by the old AMF with the information provided by the new AMF and make the policy decision.

5. The PCF sends an HTTP "200 OK" response to the AMF with the updated Access and Mobility control policy information and/or the updated Policy Control Request Trigger parameters.

6. The AMF deploys the Access and Mobility control policy if received, which includes storing the Service Area Restrictions, provisioning the Service Area Restrictions to the NG-RAN and UE, and/or 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 Access and Mobility control policies are changed.

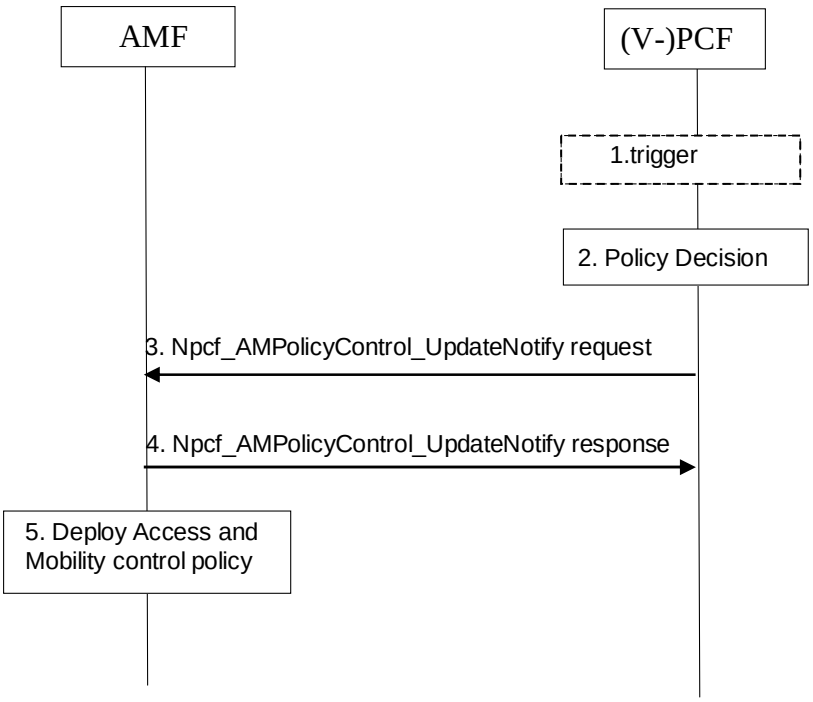


Figure 5.1.2.2-1: PCF-initiated AM Policy Association Modification procedure

This procedure concerns both roaming and non-roaming scenarios.

In the non-roaming case the role of the V-PCF is performed by the PCF. For the roaming scenarios, the V-PCF interacts with the AMF.

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

2. The (V-)PCF makes the policy decision including, Access and Mobility control policy, and may determine applicable Policy Control Request Trigger(s).

3. The (V-)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 subclause 4.2.4.2 of 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 if received which includes storing the Service Area Restrictions, provisioning the Service Area Restrictions to the UE and/or provisioning the RFSP index and Service Area Restrictions to the NG-RAN.

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, when the UE deregisters from 5GS during the UE moving from 5GS to EPS or when the old AMF removes the AM Policy Association during AMF relocation.

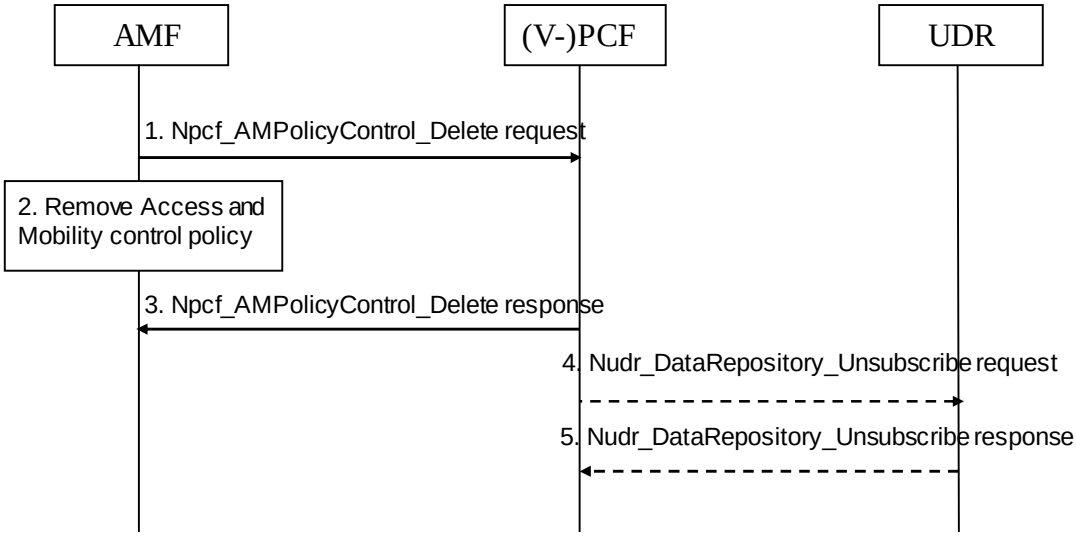


Figure 5.1.3.1-1: AMF-initiated AM Policy Association Termination procedure

This procedure concerns both roaming and non-roaming scenarios.

In the non-roaming case the role of the V-PCF is performed by the PCF. For the roaming scenarios, the V-PCF interacts with the AMF.

Step 4 and step 5 are not executed in the roaming case.

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 "Individual AM Policy Association" resource.
2. The AMF removes the UE context for this UE, including the Access and Mobility Control Policy related to the UE and/or policy control request triggers.
3. The (V-)PCF removes the policy context for the UE and sends an HTTP "204 No Content" response to the AMF.
4. The PCF invokes the Nudr_DataRepository_Unsubscribe service operation to unsubscribe the notification of subscriber policy data modification from the UDR by sending the HTTP DELETE request to the "IndividualPolicyDataSubscription" resource if it has subscribed such notification.5. The UDR sends an HTTP "204 No Content" response to the PCF.

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 or when the PCF decides to terminate the AM Policy Association based on the internal logic, e.g. UE movement triggers a geo-fencing rule.

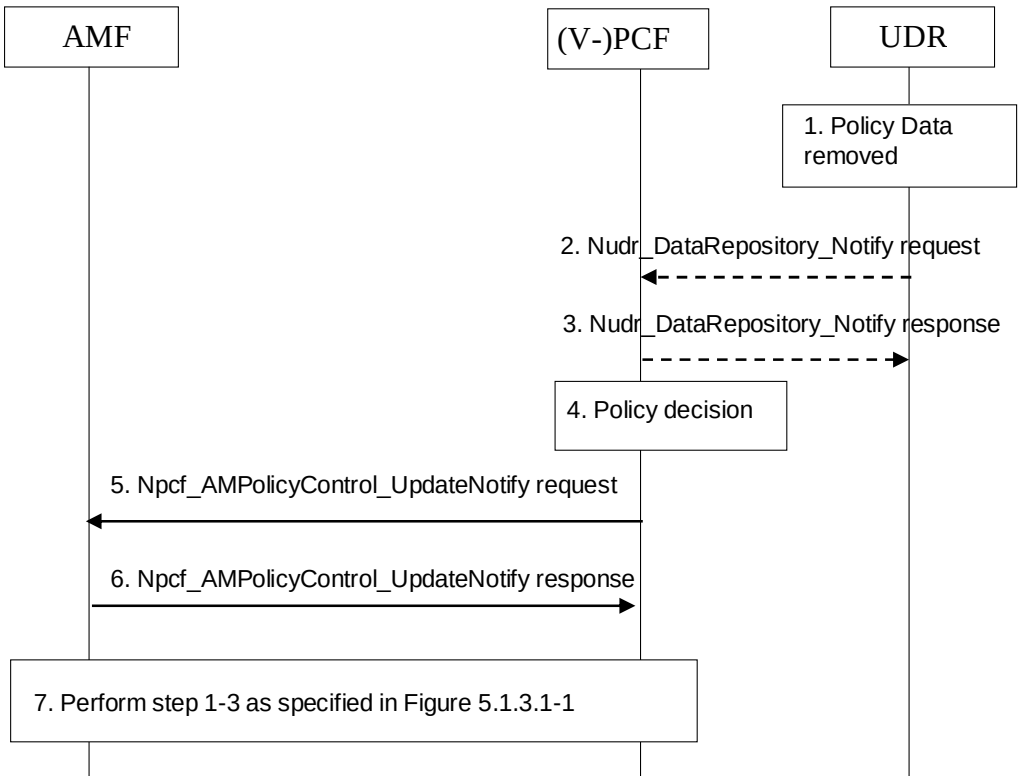


Figure 5.1.3.2-1: PCF-initiated AM Policy Association Termination procedure

This procedure concerns both roaming and non-roaming scenarios.

In the non-roaming case the role of the V-PCF is performed by the PCF. For the roaming scenarios, the V-PCF interacts with the AMF.

Step 1, step 2 and step 3 are not executed in the roaming case or in the case that the PCF decides to terminate the AM Policy Association based on the internal logic.

1. The subscriber policy control data is removed from the UDR.
2. The UDR invokes the Nudr_DataRepository_Notify service operation to notify the PCF that the policy profile is removed if PCF has subscribed such notification by sending the HTTP POST request to the resource URI "{notificationUri}" as specified in 3GPP TS 29.519 [12].
3. The PCF sends the response to the Nudr_DataRepository_Notify service operation.
4. The (V-)PCF decides to terminate the AM Policy Association based on step 2 or an internal trigger, e.g. operator policy is changed, to re-evaluate Access and Mobility control policy for a UE.
5. The (V-)PCF may, depending on operator policies, invokes the Npcf_AMPolicyControl_UpdateNotify service operation to the AMF of the removal of the Access and Mobility control policy control information by sending the HTTP POST request to the request URI "{Notification URI}/terminate" as described in subclause 4.2.4.3 of 3GPP TS 29.507 [7].

   Alternatively, the (V-)PCF may decide to maintain the Policy Association if a default profile is applied, and then step 4 through 6 are not executed.
6. The AMF sends an HTTP "204 No Content" response to the PCF.
7. Step 1 through step 3 as specified in Figure 5.1.3.1-1 are executed with the following difference:
   - the AMF removes the policy control request trigger(s) related to the AM policy association, but still keeps the provisioned AM policies and applies them to the UE.

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.

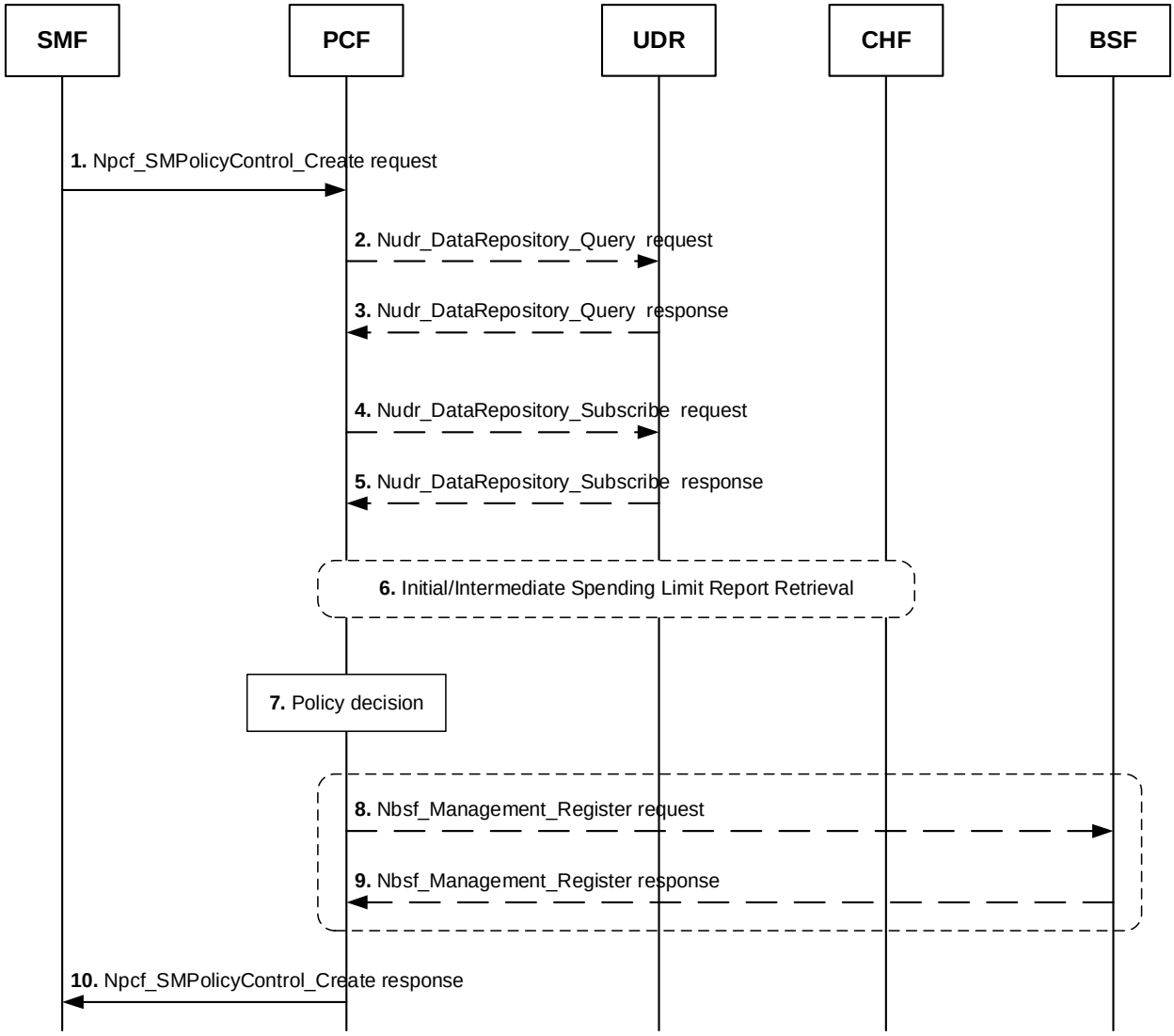


Figure 5.2.1-1: SM Policy Association Establishment procedure

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 5 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 "SM Policies" resource. 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.

2-3. 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 by sending the HTTP GET request to the

"SessionManagementPolicyData" resource as specified in 3GPP TS 29.519 [12].The UDR sends an HTTP "200 OK" response to the PCF with the policy control subscription data.

Additionally, if the TSC feature defined in 3GPP TS 29.512 [9] is supported, the PCF invokes the Nudr_DataRepository_Query service operation to retrieve the stored AF influence data in the UDR by sending the HTTP GET request to the "Influence Data" resource as specified in 3GPP TS 29.519 [12]. The UDR sends an HTTP "200 OK" response with the stored AF request.

4-5. To request notifications from the UDR on changes in the subscription information, the PCF invokes the Nudr_DataRepository_Subscribe service operation by sending an HTTP POST request to the "PolicyDataSubscriptions" resource. The UDR sends an HTTP "201 Created" response to acknowledge the subscription.

Additionally, if the TSC feature defined in 3GPP TS 29.512 [9] is supported, to request notifications from the UDR on changes in the AF influence data, the PCF invokes the Nudr_DataRepository_Subscribe service operation by sending an HTTP POST request to the "Influence Data Subscription" resource. The UDR sends an HTTP "201 Created" response to acknowledge the subscription.

6. 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.

7. The PCF makes the policy decision to determine the information provided in step 10.

8. In the case that the BSF is to be used and that either the IP address/prefix or MAC address is available, the PCF invokes the Nbsf_Management_Register service operation by sending HTTP POST request to create the PDU session binding information for a UE in the BSF as detailed in subclause 8.5.2.

9. The PCF receives an HTTP "201 Created" response from the BSF with the created binding information as detailed in subclause 8.5.2.

10. 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].

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.

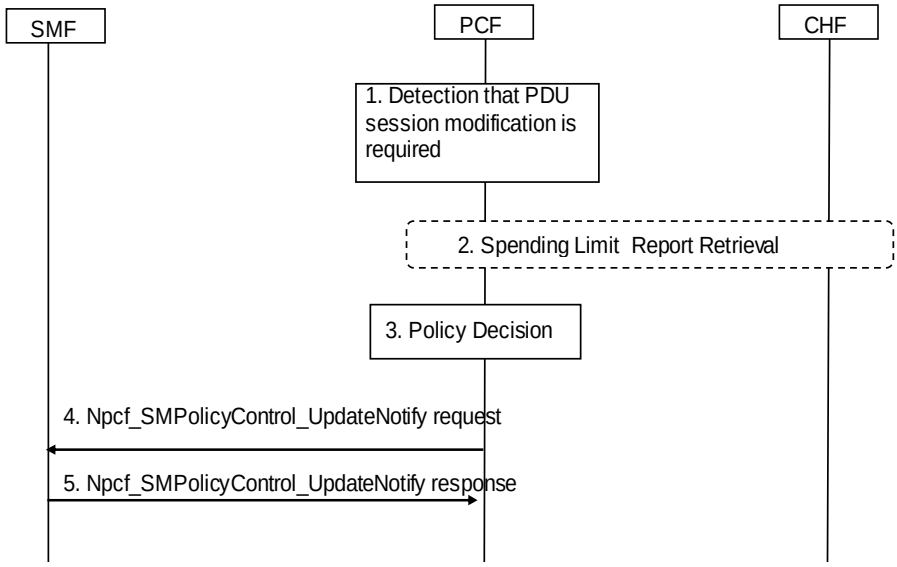


Figure 5.2.2.2-1: Interactions between SMF, PCF and CHF for PCF-initiated SM Policy Association Modification procedure

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 subclause 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.

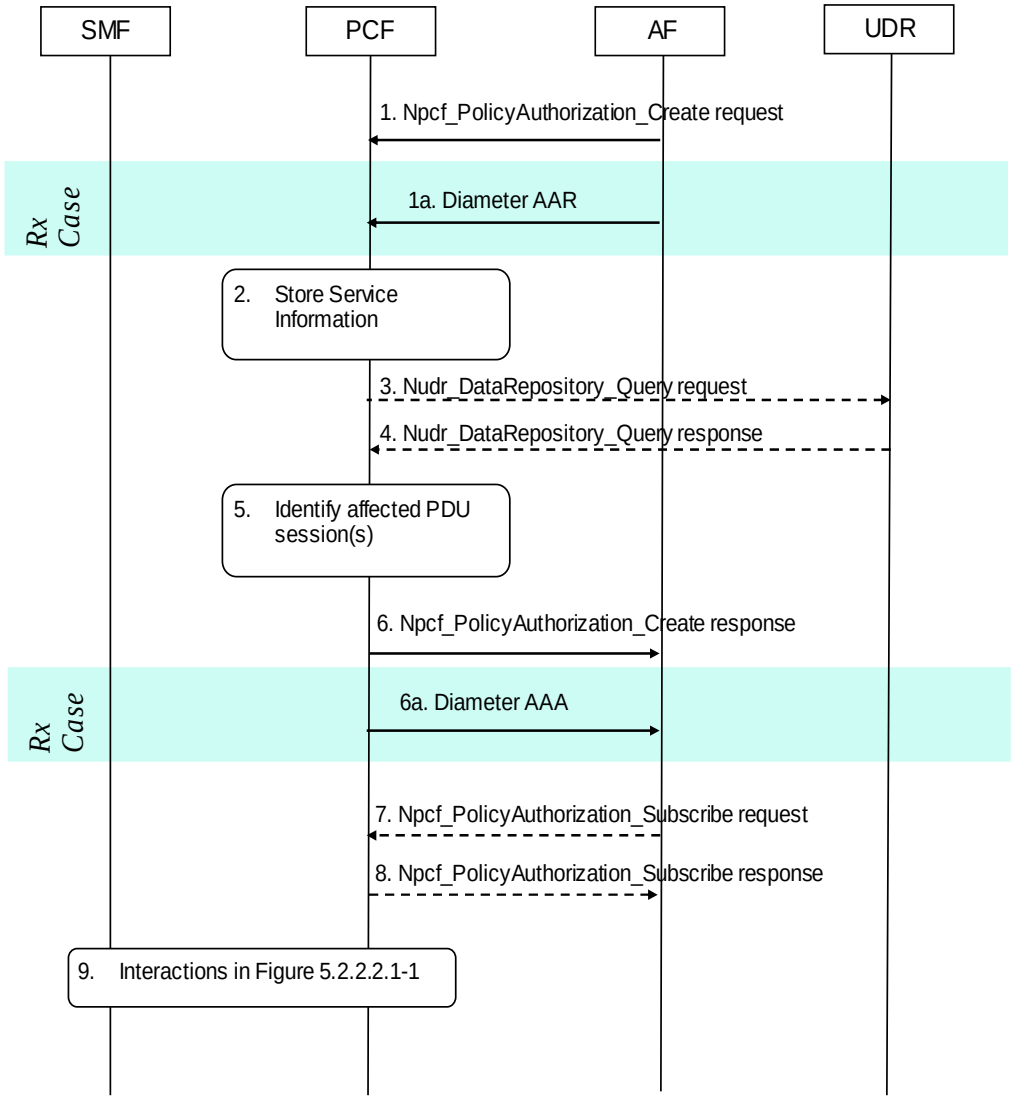


Figure 5.2.2.2.2.1-1: AF Session Establishment triggers PCF-initiated SM Policy Association Modification procedure

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 to the PCF by sending the HTTP POST request to the "Application Sessions" resource. The request operation includes the AF Identifier, the IP address or the MAC address of the UE, the identification of the application session context, the SUPI if available, the GPSI 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.

3-4. If the PCF does not have the subscription data for the SUPI and DNN, it invokes the Nudr_DataRepository_Query service operation to the UDR by sending the HTTP GET request to the "SessionManagementPolicyData" resource. The UDR sends an HTTP "200 OK" response to the PCF with the 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 sends the HTTP GET request to the "IndividualBdtData" resource. The UDR sends an HTTP "200 OK" response to the PCF with the Background Data Transfer policy.

5. 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.

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

   6a. The PCF sends a Diameter AAA to the AF.

7. The AF may invoke the Npcf_PolicyAuthorization_Subscribe service operation by sending the HTTP PUT request to the "Events Subscription" resource to subscribe to events in the PCF. The request includes the events that subscribes and 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].

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

9. 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.

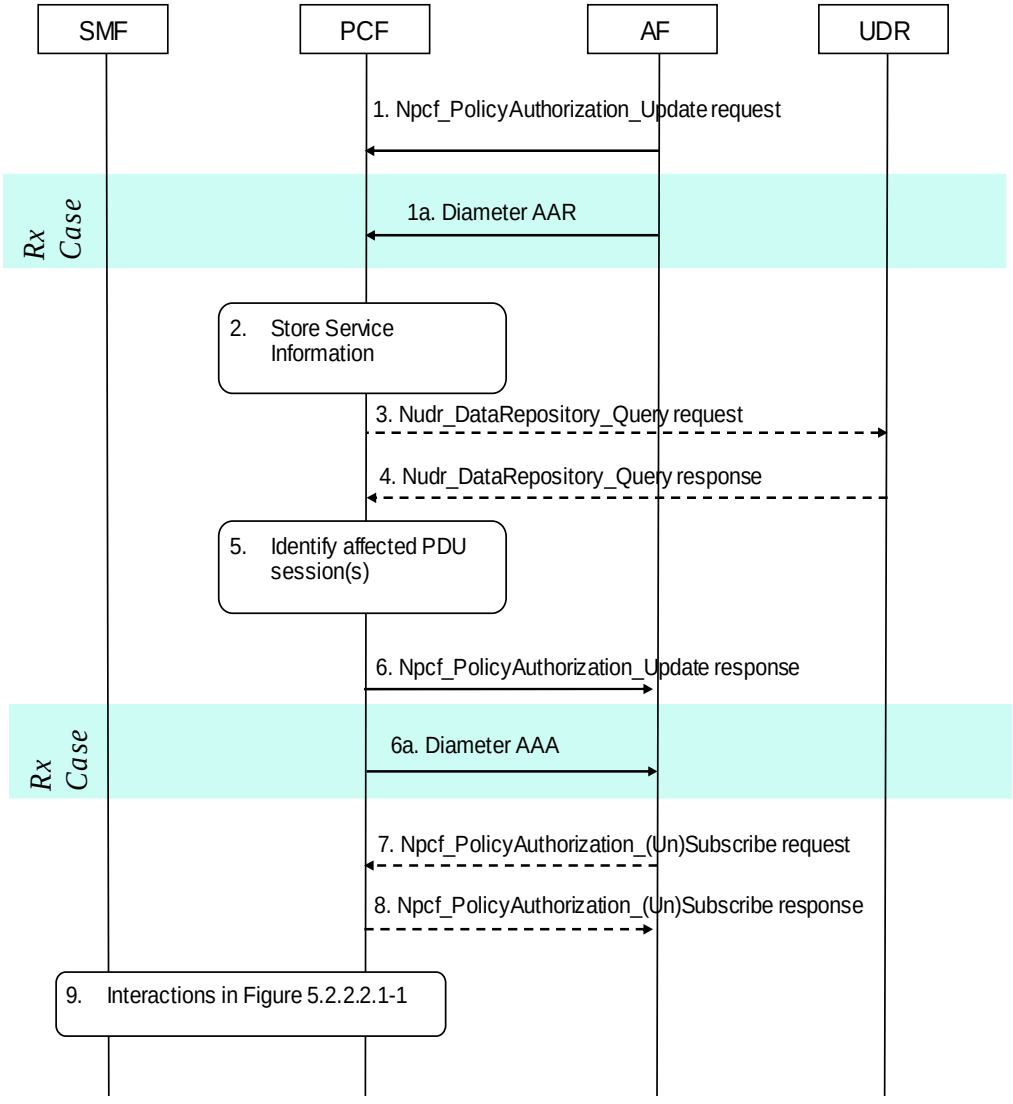


Figure 5.2.2.2.2-1: AF Session Modification triggers PCF-initiated SM Policy Association Modification procedure

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 to the PCF by sending the HTTP PATCH request to the "Individual Application Session Context" resource 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.

3-4. These steps are the same as steps 3-4 in subclause 5.2.2.2.2.1.

5. 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.

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

   6a. The H-PCF sends a Diameter AAA to the AF.

7. 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 "Events Subscription" resource. The HTTP request includes the events that subscribes and may also include 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 "Events Subscription" resource.

8. 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.

9. 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.

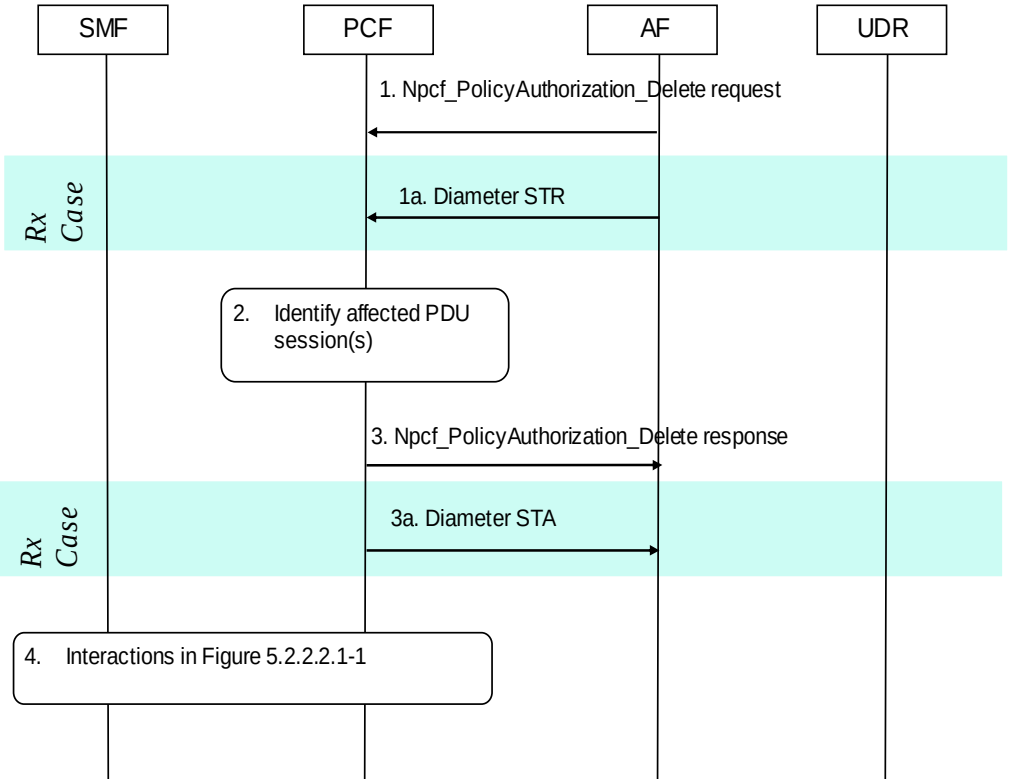


Figure 5.2.2.2.2.3-1: AF Session Termination triggers PCF-initiated SM Policy Association Modification procedure

1. The AF sends the Npcf_PolicyAuthorization_Delete service operation by sending the HTTP POST request to the "Individual Application Session Context" resource to request the removal of the AF application session. The request may include the events to subscribe 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.

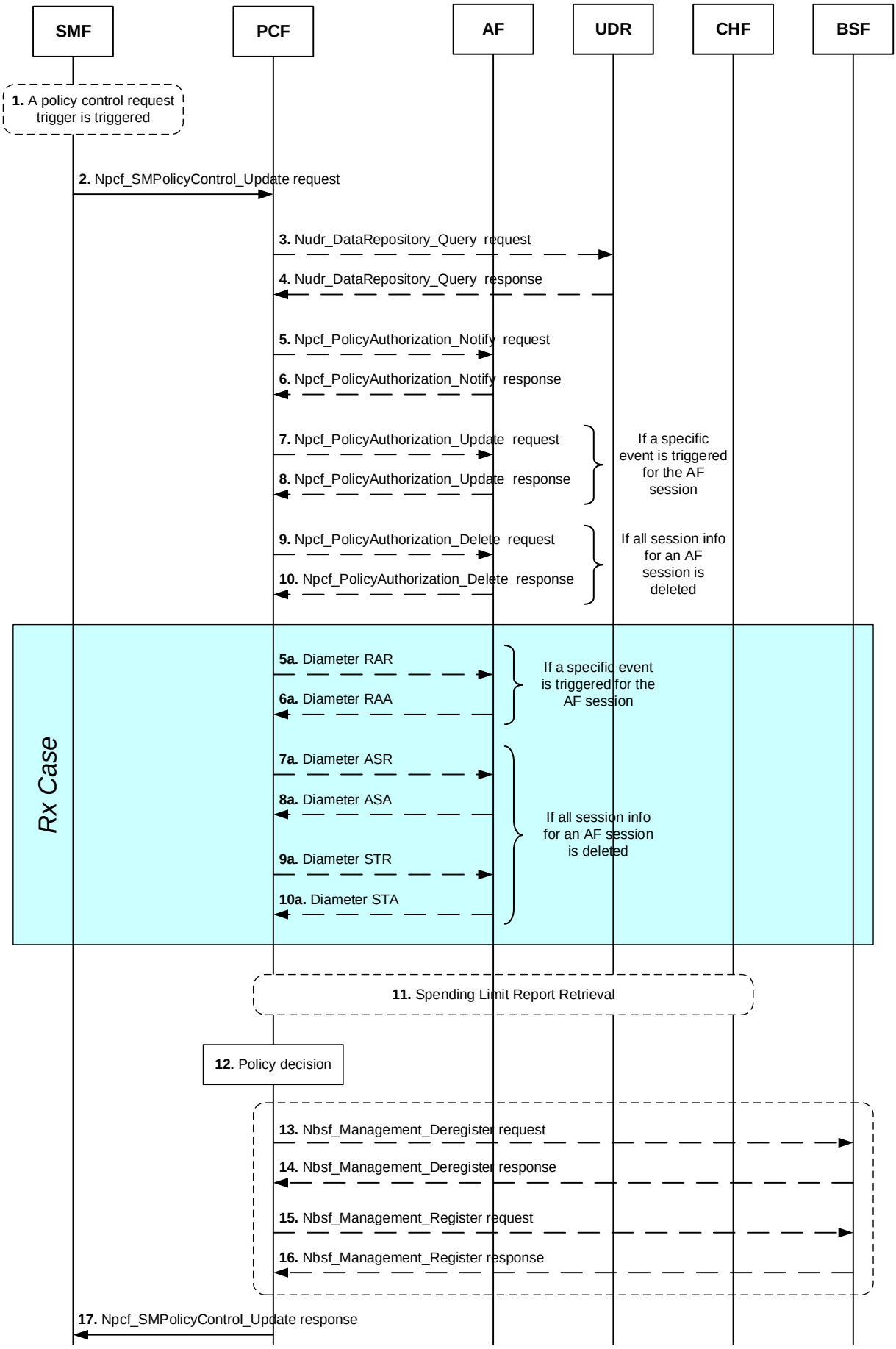


Figure 5.2.2.3-1: SMF-initiated SM Policy Association Modification procedure

1. The SMF detects a policy control request trigger condition is met.

2. The SMF invokes the Npcf_SMPolicyControl_Update service operation to the PCF by sending the HTTP POST request to the "Individual SM Policy" resource 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 invokes the Nudr_DataRepository_Query service operation to the UDR by sending the HTTP GET request to the "SessionManagementPolicyData" resource to fetch the information.

4. The UDR sends an HTTP "200 OK" response to the PCF with the subscription related information containing the information about the allowed service(s) and PCC Rules information.

5. 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.

   5a. 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.

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

   6a. The AF replies with a Diameter RAA and may provide updated service information within.

7. The AF may invoke the Npcf_PolicyAuthorization_Update service operation to the PCF by sending the HTTP PATCH request to the "Individual Application Session Context" resource including the modified service information.

8. The PCF sends an HTTP "200 OK" or an HTTP "204 No Content" response to the AF.

9. If the PCF indicates in step 5 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 to the "Individual Application Session Context" resource to terminate the AF session. The request may include the events to subscribe to.

10. 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.

    7a-10a. If all service data flows for an AF session are deleted, the AF session is terminated.

11. 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.

12. The PCF makes a policy decision. The PCF may determine that updated or new policy information needs to be sent to the SMF in step 17.

13. If the IP address is released for the IP PDU session or the MAC address is not used anymore for the Ethernet PDU session and the binding information has been previously registered in the BSF, the PCF invokes the Nbsf_Management_Deregister service operation by sending an HTTP DELETE request to the BSF to delete binding information as detailed in subclause 8.5.3.

14. The PCF receives an HTTP "204 No Content" response from the BSF as detailed in subclause 8.5.3.

15. If a new IP address is allocated for the IP PDU session or a new MAC address is used for the Ethernet PDU session and the BSF is to be used, the PCF invokes the Nbsf_Management_Register service operation by sending an HTTP POST request to create the binding information in the BSF as detailed in subclause 8.5.2.

16. The PCF receives an HTTP "201 Created" response from the BSF with the created binding information as detailed in subclause 8.5.2.

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

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).

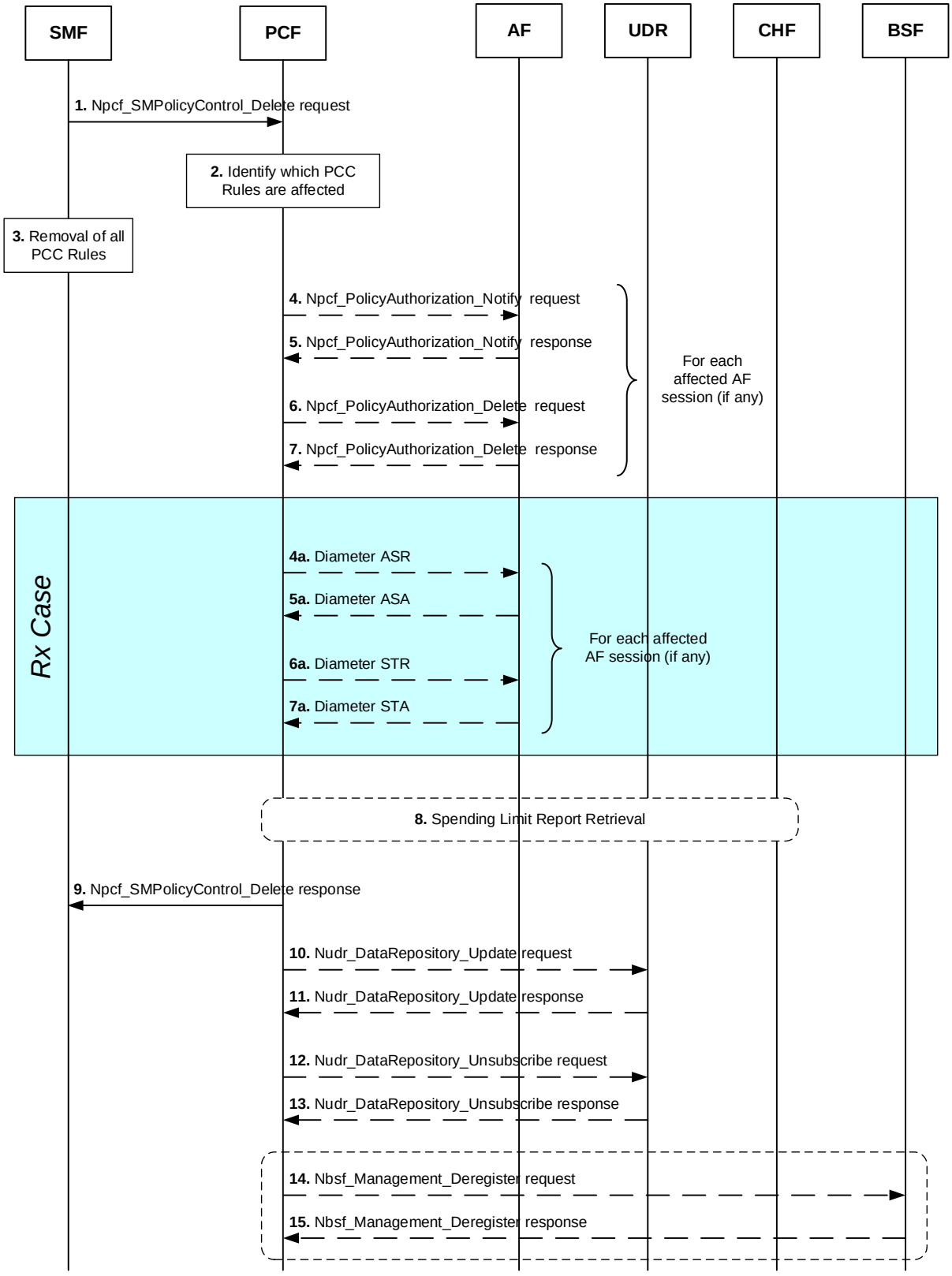


Figure 5.2.3.1-1:SMF-initiated SM Policy Association Termination procedure

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, steps 10 - step 13 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 to the "Individual SM Policy" resource 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}/terminate" 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 "Individual Application Session Context" resource. The request may include the events to subscribe 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 needs 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 subclause 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 subclause 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 invokes the Nudr_DataRepository_Update service operation by sending the HTTP PATCH request to the "SessionManagementPolicyData" resource to store the remaining usage allowance in the UDR, if all PDU sessions of the user to the same DNN are terminated.

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

12-13. To unsubscribe the notification of the PDU session related data modification from the UDR, the PCF invokes the Nudr_DataRepository_Unsubscribe service operation by sending the HTTP DELETE request to the "IndividualPolicyDataSubscription" resource if it has subscribed such notification. The UDR sends an HTTP "204 No Content" response to the PCF.

    Additionally, to unsubscribe the notification of the AF influence data from the UDR, the PCF invokes the Nudr_DataRepository_Unsubscribe service operation by sending the HTTP DELETE request to the "Individual Influence Data Subscription" resource if it has subscribed such notification. The UDR sends an HTTP "204 No Content" response to the PCF.

14. In the case that binding information has been previously registered in the BSF the PCF invokes the Nbsf_Management_Deregister service operation by sending an HTTP DELETE request to the BSF to delete binding information as detailed in subclause 8.5.3.

15. The PCF receives an HTTP "204 No Content response from the BSF as detailed in subclause 8.5.3.

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.

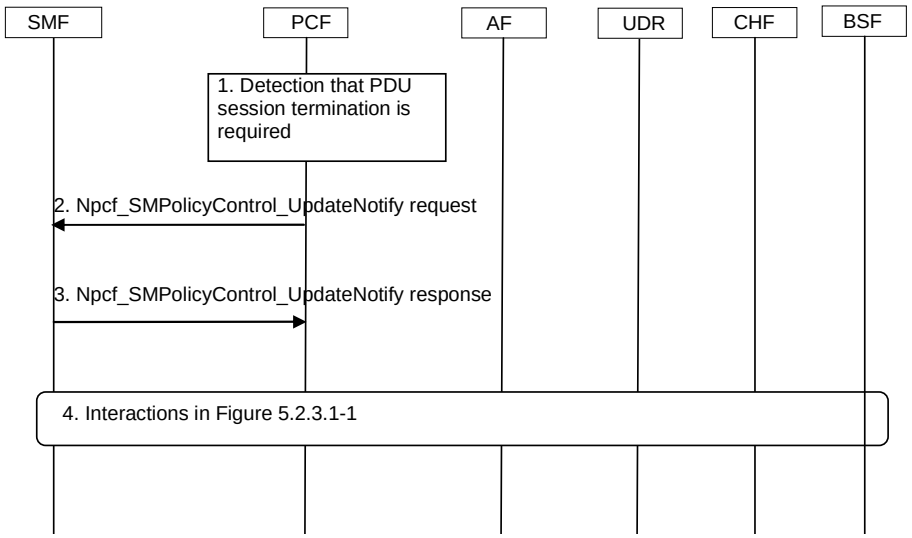


Figure 5.2.3.2-1: PCF-initiated SM Policy Association Termination procedure

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/BSF 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.

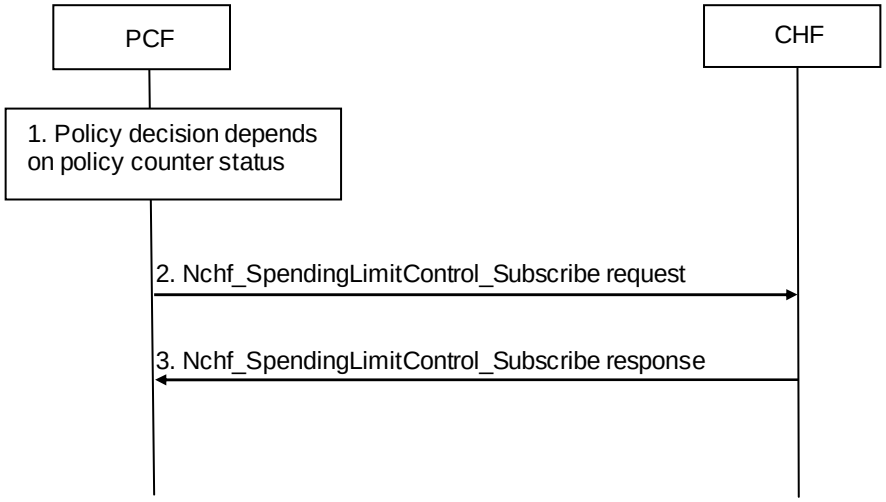


Figure 5.3.2-1: Initial Spending Limit Report Request procedure

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 the Nchf_SpendingLimitControl_Subscribe service operation to the CHF by sending the HTTP POST request to the "Spending Limit Retrieval Subscriptions" resource if such reporting is not established for the subscriber. The request operation includes the subscriber Id "SUPI", the notification URI and optionally the list of policy counter identifier(s).
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.

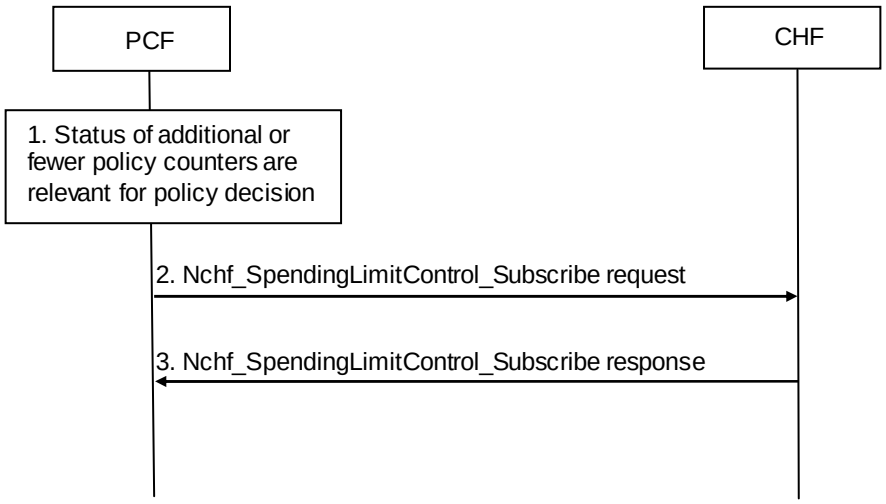


Figure 5.3.3-1: Intermediate Spending Limit Report Request procedure

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 the Nchf_SpendingLimitControl_Subscribe service operation to the CHF by sending the HTTP PUT request to the "Individual Spending Limit Retrieval Subscription" resource. The request operation may include an updated list of policy counter identifier(s) that overrides the previously stored list of policy counter identifier(s) and a notification URI.

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.

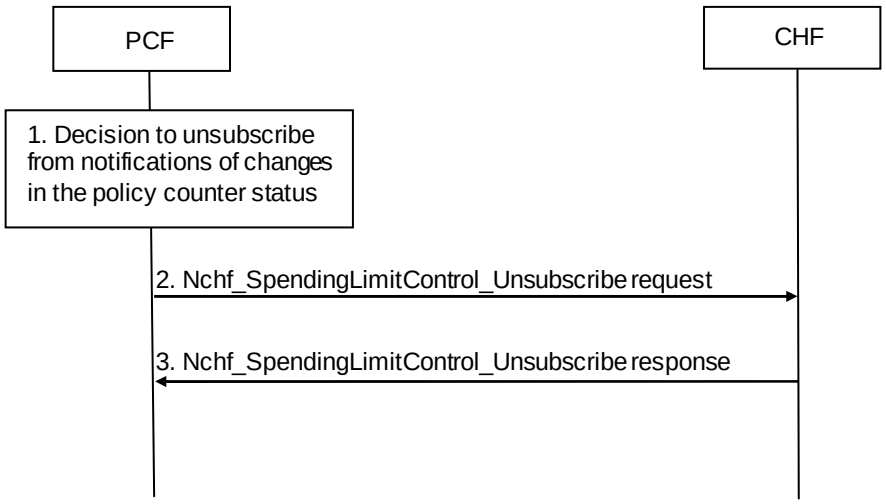


Figure 5.3.4-1: Final Spending Limit Report Request procedure

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 to the CHF by sending the HTTP DELETE request to the "Individual Spending Limit Retrieval Subscription" resource 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.

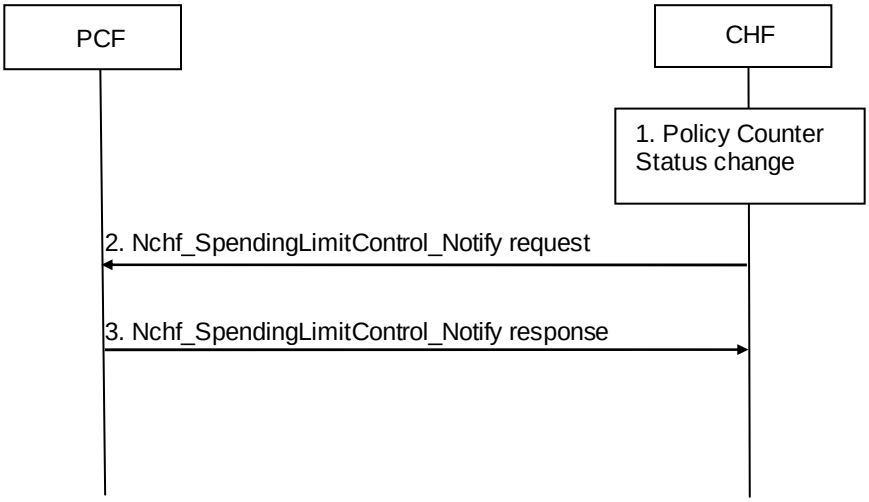


Figure 5.3.5-1: Spending Limit Report procedure

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 "{notifURI}/notify " as the request URI to the PCF associated with each affected PDU session. The request operation includes the subscriber Id "SUPI" 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.

5.3.6 Subscription termination request by CHF

This clause describes the signalling flow for the CHF to report the removal of the subscriber to every PCF.

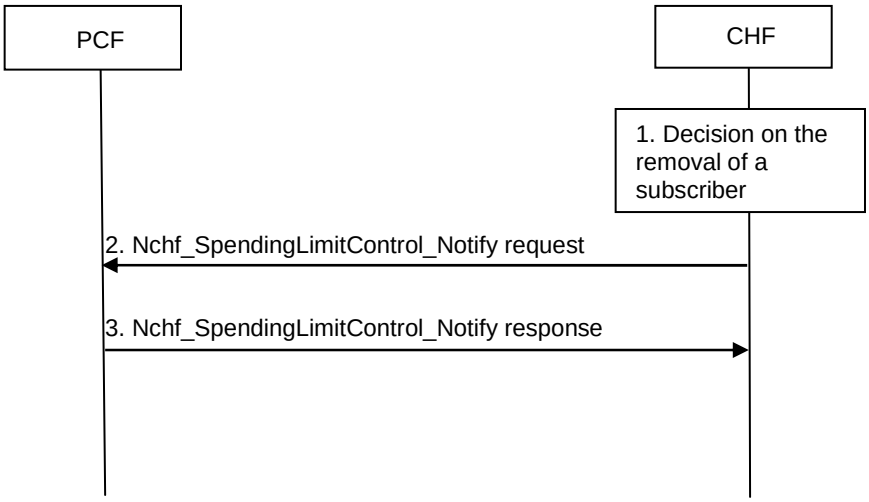


Figure 5.3.6-1: Subscription Termination Request procedure

1. When the CHF decides that a subscriber is removed it may report the removal to the PCF.

2. The CHF may invoke the Nchf_SpendingLimitControl_Notify service operation by sending the HTTP POST request with "{notifURI}/terminate" as request URI to the PCF. The request operation shall include the subscriber Id "SUPI" and in the subscription termination information "removed subscriber" as Event Information.

3. The PCF removes the subscription to notification of all policy counter statuses for a subscriber identified by the subscriber Id, makes applicable policy decisions and acknowledges the Nchf_SpendingLimitControl_Notify service operation.

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 to/unsubscribe from 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.

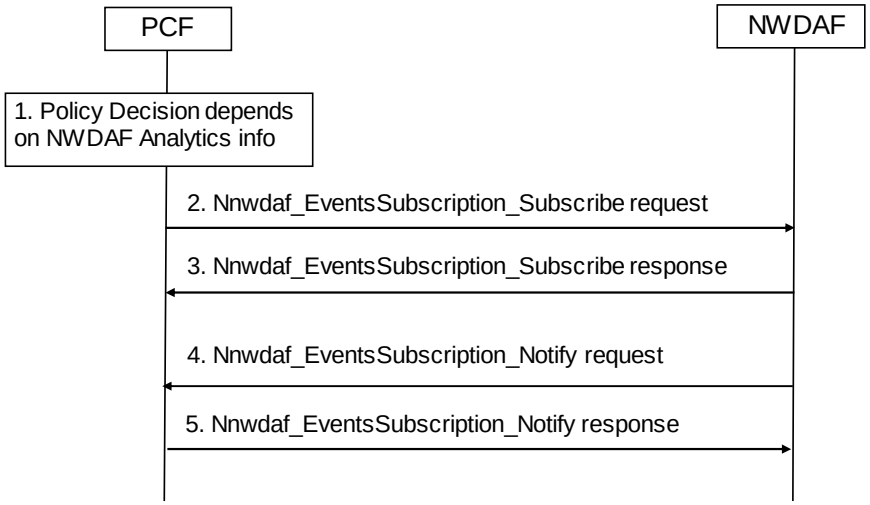


Figure 5.4.2-1: Network data analytics Subscribe procedure

1. The PCF makes policy decisions depend on load level information.

2. In order to subscribe to load level information of network slice instance(s) from NWDAF, the PCF invokes Nnwdaf_EventsSubscription_Subscribe service operation by sending an HTTP POST request with Resource URI of the resource "NWDAF Events Subscriptions". The request includes the subscribed events and may include the identifier of network slice instance(s), event notification method.

   In order to update the existing subscription, the PCF invokes Nnwdaf_EventsSubscription_Subscribe service operation by sending an HTTP PUT request with Resource URI of the resource "Individual NWDAF Event Subscription".

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".

4. If the NWDAF observes the event(s) that PCF has subscribed to, the NWDAF invokes Nnwdaf_EventsSubscription_Notify service operation to report the event(s) by sending an HTTP POST request with {notificationURI} as Notification URI.

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

NOTE 1: For details of Nnwdaf_EventsSubscription_Subscribe/Notify service operations refer to 3GPP TS 29.520 [11].

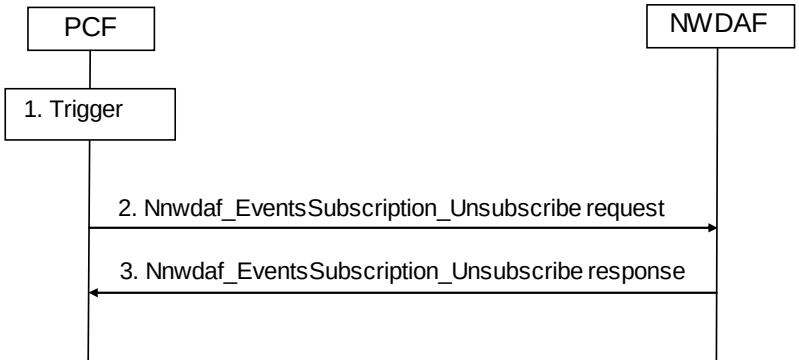


Figure 5.4.2-2: Network data analytics Unsubscribe procedure

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

2. The PCF invokes Nnwdaf_EventsSubscription_Unsubscribe service operation by sending an HTTP DELETE request with Resource URI of the resource "Individual NWDAF Event Subscription", to the NWDAF to unsubscribe from 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".

NOTE 2: For details of Nnwdaf_EventsSubscription_Unsubscribe service operation refer to 3GPP TS 29.520 [11].

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.

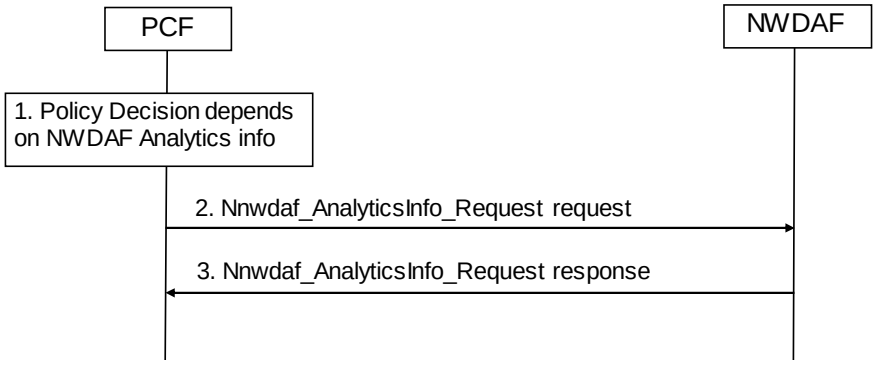


Figure 5.4.3-1: Network data analytics info request procedure

1. The PCF makes policy decisions depend on load level information of network slice instance(s), especially for one time usage.

2. The PCF invokes Nnwdaf_AnalyticsInfo_Request service operation by sending an HTTP GET request with Resource URI of the resource "NWDAF Analytics", 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".

NOTE: For details of Nnwdaf_AnalyticsInfo_Request service operation refer to 3GPP TS 29.520 [11].

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 PFD 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.

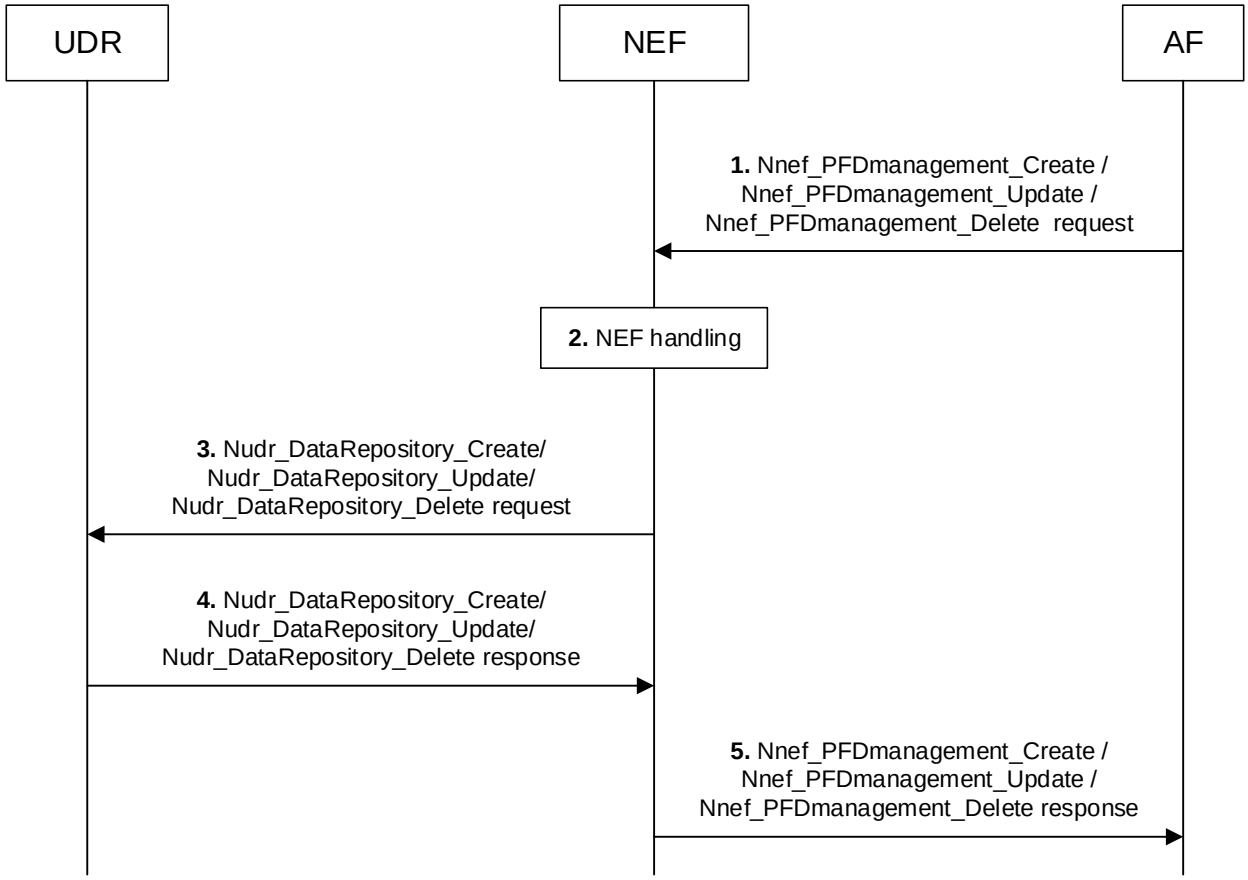


Figure 5.5.2.1-1: AF-initiated PFDF management procedure

1. To create PFDs resources for one or more application identifier(s), the AF invokes the Nnef_PFDmanagement_Create service operation to the NEF by sending the HTTP POST request to the resource "Individual PFD Management Transaction".

To update the PFDs for an existing individual transaction, the AF invokes the Nnef_PFDmanagement_Update service operation by sending the HTTP PUT request to the resource "Individual PFD Management Transaction".

To update the PFDs for an existing Application Identifier, the AF invokes the Nnef_PFDmanagement_Update service operation by sending the HTTP PUT or PATCH request to the resource "Individual Application PFD Management".

To remove the PFDs for an existing individual transaction "Individual PFD Management Transaction", the AF invokes the Nnef_PFDmanagement_Delete service operation by sending the HTTP DELETE request to the resource "Individual PFD Management Transaction".

To remove the PFDs for an existing individual application, the AF invokes the Nnef_PFDmanagement_Delete service operation by sending the HTTP DELETE request to the resource "Individual Application PFD Management".

NOTE 1: For details of Nnef_PFDmanagement_Create/Update/Delete service operations refer to 3GPP TS 29.522 [24].

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 PFD creation was requested in step 1, the NEF shall invoke the Nudr_DataRepository_Create service operation by sending an HTTP PUT request message to the resource "Individual PFD Data".

   - if PFD update was requested in step 1, the NEF shall invoke the Nudr_DataRepository_Create and/or Nudr_DataRepository_Update service operation by sending an HTTP PUT request message to the resource "Individual PFD Data", and/or invoke the Nudr_DataRepository_Delete service operation by sending an HTTP DELETE request message to the resource "Individual PFD Data".

   - if PFD removal was requested in step 1, the NEF shall invoke the Nudr_DataRepository_Delete service operation by sending an HTTP DELETE request message to the resource "Individual PFD Data".

NOTE 2: PFD creation/update/removal in step 1 can include PFD management request for multiple applications, but the UDR service for PFD management only supports one application at a time.

NOTE 3: For details of Nudr_DataRepository_Create/Update/Delete service operations refer to 3GPP TS 29.519 [12].

4. The UDR shall send the HTTP response message to the NEF correspondingly.

5. The NEF sends Nnef_PFDManagement_Create/Update/Delete Response to the AF.

5.5.2.2 PFD 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) provisioned by the PFDF 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).

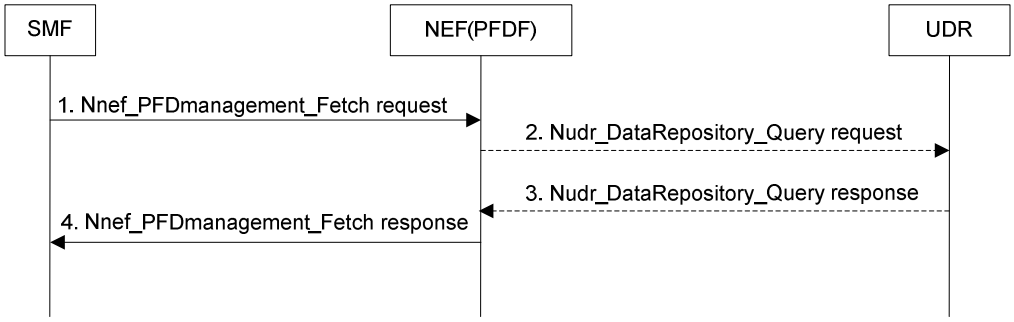


Figure 5.5.2.2.1-1: PFD retrieval by SMF

1. In order to retrieve the PFDs of individual application identifier, the SMF shall invoke Nnef_PFDmanagement_Fetch service operation by sending an HTTP GET request message to the resource "Individual application PFD".

   In order to retrieve the PFDs of all application identifiers, the SMF shall invoke the Nnef_PFDmanagement_Fetch service operation by sending an HTTP GET request message to the resource "PFD of applications".

   In order to retrieve the PFDs of collection of application identifiers, the SMF shall invoke the Nnef_PFDmanagement_Fetch service operation by sending an HTTP GET request message to the resource "PFD of applications" with query parameters indicating the requested application identifiers.

NOTE 1: For details of Nnef_PFDmanagement_Fetch service operation refer to 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 to the resource "Individual PFD Data" as specified in 3GPP TS 29.519 [12].

NOTE 2: The SMF in step 1 can include PFD management request for multiple applications, but the UDR service for PFD management only supports one application at a time.

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

4. The NEF (PFDF) sends the HTTP GET response message "200 OK" 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.

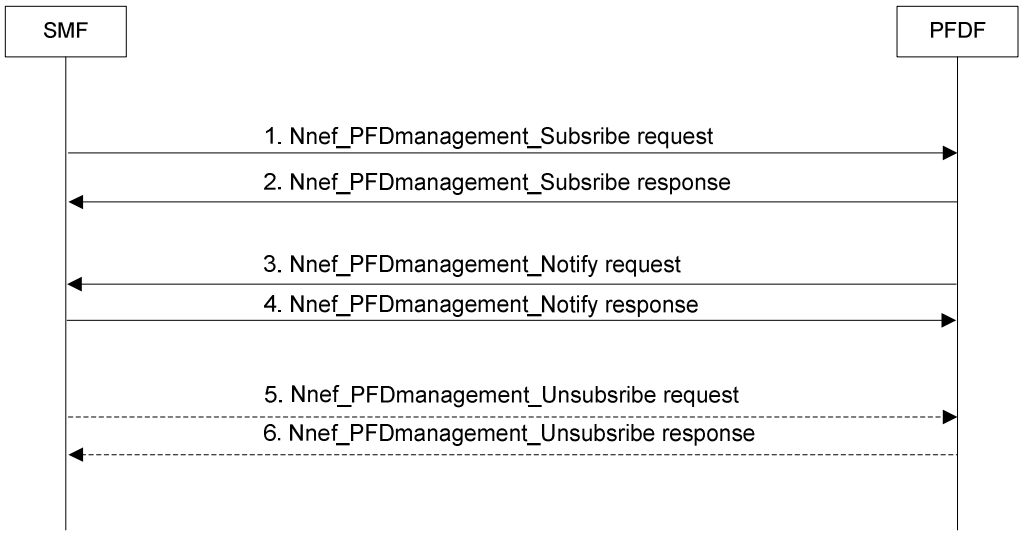


Figure 5.5.2.2.2-1: PFDF management in the SMF

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 resource "PFD subscriptions". The HTTP POST request includes a notification URI to indicate to the PFDF where to send notifications when events occur. If the subscription is accepted, he PFDF shall send the POST response message a "201 Created" 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 notification URI "{notifyUri}/notify". The SMF replies to the PFDF with an HTTP POST response message "204 No Content" indicating the successful provisioning of all PFDs or "200 OK" containing failed application identifier(s).

5-6. The SMF may initiate Nnef_PFDmanagement_Unsubscribe service operation to remove the subscription by sending an HTTP DELETE request message to the resource "Individual PFD subscription". The PFDF replies to the SMF with an HTTP DELETE response message "204 No Content".

NOTE: For details of Nnef_PFDmanagement_Subscribe/Notify/Unsubscribe service operations refer to 3GPP TS 29.551 [25].

5.5.3 Traffic influence procedures

5.5.3.1 General

As described in 3GPP TS 23.501 [2] subclause 5.6.7, an AF may send requests to influence SMF routing decisions for User Plane traffic of PDU Sessions. The AF may also provide in its request subscriptions to SMF events (e.g. UP path change).

The following cases are included in this clause:

AF requests targeting an individual UE address: such requests are routed (by the AF or by the NEF) to an individual PCF using the BSF or by configuration as described in subclause 5.5.3.2.

NOTE 1: Such requests target an on-going PDU Session. Whether the AF needs to use the NEF or not depends on local deployment.

AF requests targeting PDU Sessions that are not identified by an UE address: For such requests the AF shall contact the NEF and the NEF stores the AF request information in the UDR. PCF(s) that have subscribed to the modification of the AF request information receive a corresponding notification from the UDR. This is described in subclause 5.5.3.3.

NOTE 2: Such requests can target on-going or future PDU Sessions.

NOTE 3: The 5GC functions used in the following procedures are assumed to all belong to the same PLMN (HPLMN in non-roaming case or VPLMN in the case of a PDU Session in LBO mode).

NOTE 4: AF requests invoked from an AF located in the HPLMN for home routed roaming scenario are not supported.

5.5.3.2 AF requests targeting an individual UE address

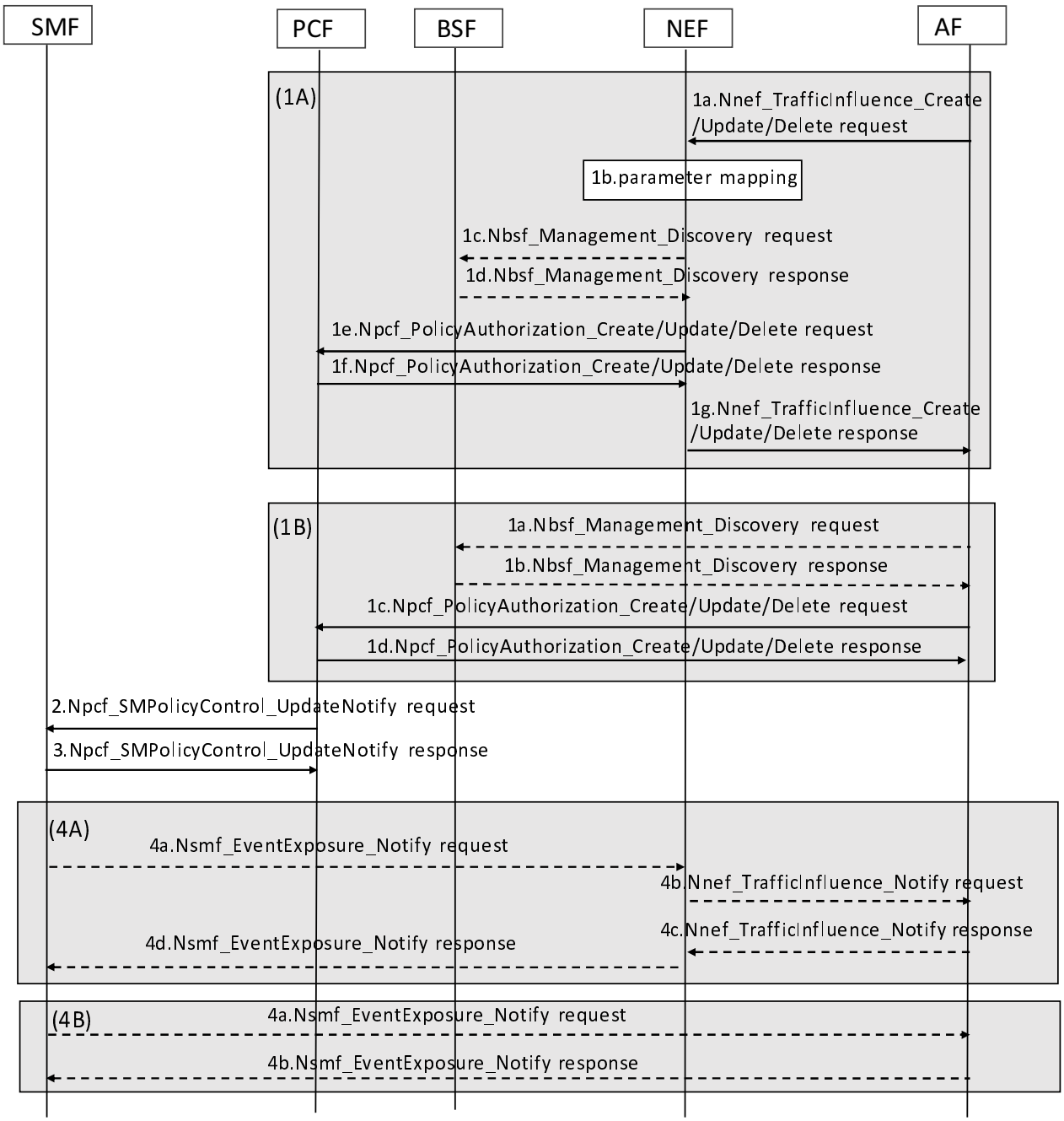


Figure 5.5.3.2-1: Processing AF requests to influence traffic routing for Sessions identified by an UE address

1A. The AF sends the AF request to PCF via the NEF.

1a-1b. These steps are the same as steps 1-2 in Figure 5.5.3.3-1.

1c-1d. If the PCF address is not available on the NEF based on local configuration, the NEF invokes the Nbsf_Management_Discovery service operation, specified in subclause 8.5.4, to obtain the selected PCF ID for the ongoing PDU session identified by the individual UE address in the AF request.

1e-1f. The NEF forwards the AF request to the PCF.

When receiving the Nnef_TrafficInfluence_Create request in step 1a, the NEF invokes the Npcf_PolicyAuthorization_Create service operation by sending the HTTP POST request to the "Application Sessions" resource as described in subclause 5.2.2.2.2.1.

When receiving the Nnef_TrafficInfluence_Update request in step 1a, the NEF invokes the Npcf_PolicyAuthorization_Update service operation by sending the HTTP PATCH request to the "Individual Application Session Context" resource as described in subclause 5.2.2.2.2.2.

When receiving the Nnef_TrafficInfluence_Delete request in step 1a The NEF invokes the Npcf_PolicyAuthorization_Delete service operation by sending the HTTP POST request to the "Individual Application Session Context" resource as described in subclause 5.2.2.2.2.3.

1g The NEF sends the HTTP response message to the AF correspondingly.

1B.The AF sends the AF request to PCF directly.

1a-1b. If the PCF address is not available on the AF based on local configuration, the AF invokes the Nbsf_Management_Discovery service operation, as specified in subclause 8.5.4, to obtain the selected PCF ID for the ongoing PDU session identified by the individual UE address in its request.

1c-1d. To create a new AF request, the AF invokes the Npcf_PolicyAuthorization_Create service operation by sending the HTTP POST request to the "Application Sessions" resource as described in subclause 5.2.2.2.2.1.

To update an existing AF request, the AF invokes the Npcf_PolicyAuthorization_Update service operation by sending the HTTP PATCH request to the "Individual Application Session Context" resource as described in subclause 5.2.2.2.2.2.

To remove an existing AF request, the AF invokes the Npcf_PolicyAuthorization_Delete service operation by sending the HTTP POST request to the "Individual Application Session Context" resource as described in subclause 5.2.2.2.2.3.

2-3. Upon receipt of the AF request, the PCF invokes the Npcf_SMPolicyControl_UpdateNotify service operation to update the SMF with corresponding PCC rule(s) by sending the HTTP POST request to the resource URI "{Notification URI}/update" as described in subclause 5.2.2.2.1. If the AF subscribes to UP Path change event, the PCF includes the related subscription information within the corresponding PCC rule(s) as specified in TS 29.512 [9].

- For the case of 4A, the PCF includes in the PCC rule(s) the Notification URI pointing to the NEF and the Notification Correlation ID assigned by NEF (i.e. AF Transaction Internal ID).

- For the case of 4B, the PCF includes in the PCC rule(s) the Notification URI pointing to the AF and the Notification Correlation ID assigned by AF (i.e. AF Transaction ID).

If the AF unsubscribes from UP Path change event, the PCF removes the related subscription information from the corresponding PCC rule(s) as specified in 3GPP TS 29.512 [9].

4A. In case of 1A, if the SMF observes PDU Session related event(s) that AF has subscribed to, the SMF invokes Nsmf_EventExposure_Notify to the AF via the NEF by sending an HTTP POST request. When receiving the Nsmf_EventExposure_Notify service operation, the NEF performs information mapping (e.g. AF Transaction Internal ID to AF Transaction ID, SUPI to GPSI, etc.), and invokes the Nnef_TrafficInfluence_Notify service operation to forward the notification to the AF. The step is the same as steps 7-10 in Figure 5.5.3.3-1.

4B. In case of 1B, if the SMF observes PDU Session related event(s) that AF has subscribed to, the SMF invokes Nsmf_EventExposure_Notify to the AF directly by sending an HTTP POST request to the resource URI "{notifUri}", and the AF sends a "204 No Content" response to the SMF.

5.5.3.3 AF requests targeting PDU Sessions not identified by an UE address

If the AF traffic influence request affects future PDU session, the traffic influence procedure is performed as depicted in Figure 5.5.3.3-1.

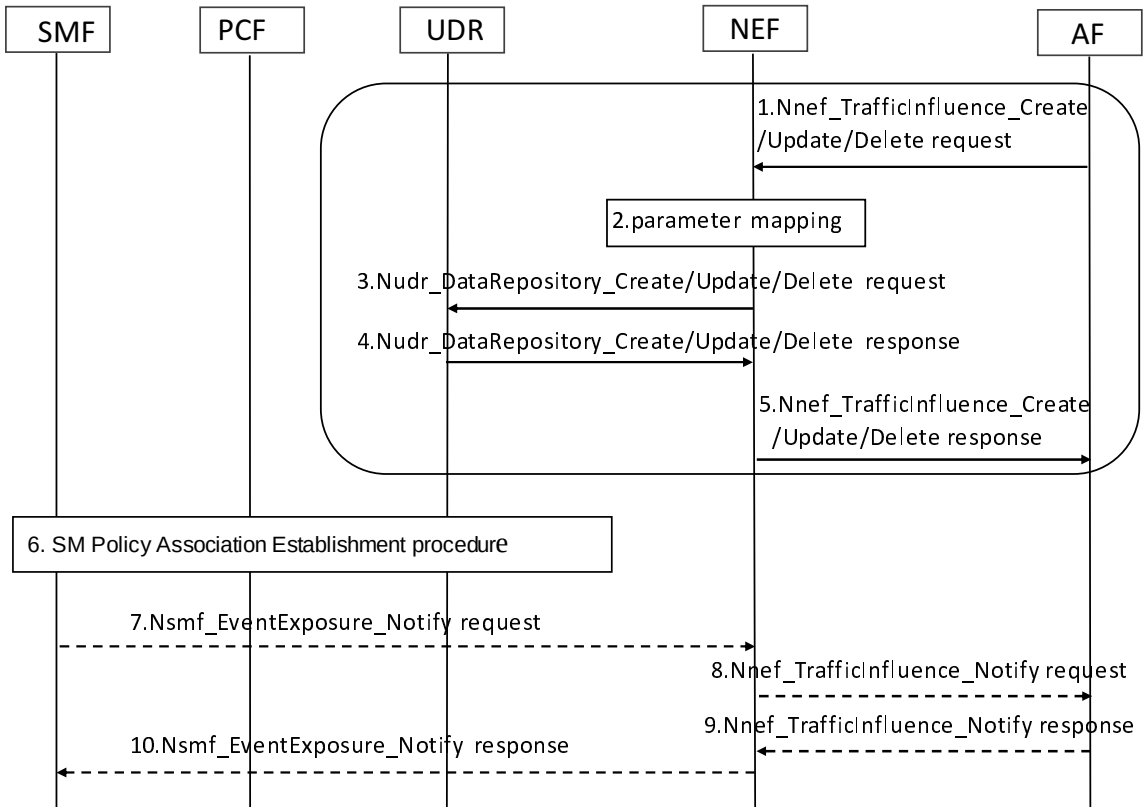


Figure 5.5.3.3-1: Processing AF requests to influence traffic routing for Sessions not identified by an UE address, affecting future PDU session

1. To create a new AF request, the AF invokes the Nnef_TrafficInfluence_Create service operation to the NEF by sending the HTTP POST request to the "Traffic Influence Subscription" resource .

   To update an existing AF request, the AF invokes the Nnef_TrafficInfluence_Update service operation by sending the HTTP PUT or PATCH request to the "Individual Traffic Influence Subscription" resource.

   To remove an existing AF request, the AF invokes the Nnef_TrafficInfluence_Delete service operation by sending the HTTP DELETE request to the "Individual Traffic Influence Subscription" resource.

NOTE 1: For details of Nnef_TrafficInfluence_Create/Update/Delete service operations refer to 3GPP TS 29.522 [24].

2. Upon receipt of the AF request, the NEF authorizes it and then performs the mapping from the information provided by the AF into information needed by the 5GC as described in 3GPP TS 23.501 [2] and 3GPP TS 23.502 [3].

3-4. When receiving the Nnef_TrafficInfluence_Create request, the NEF invokes the Nudr_DataRepository_Create service operation to store the AF request information in the UDR by sending the HTTP PUT request to the "Individual Influence Data" resource, and the UDR sends a "201 Created" response.

   When receiving the Nnef_TrafficInfluence_Update request, the NEF invokes the Nudr_DataRepository_Update service operation to modify the AF request information in the UDR by sending the HTTP PATCH/PUT request to the resource "Individual Influence Data", and the UDR sends a "200 OK" or "204 No Content" response accordingly.

   When receiving the Nnef_TrafficInfluence_Delete request, the NEF invokes the Nudr_DataRepository_Delete service operation to delete the AF requirements from the UDR by sending the HTTP DELETE request to the "Individual Influence Data" resource, and the UDR sends a "204 No Content" response.

NOTE 2: For details of the Nudr_DataRepository_Create/Update/Delete service operations refer to 3GPP TS 29.519 [12].

5. The NEF sends the HTTP response message to the AF correspondingly.

6. The PCF retrieves the stored AF request in the UDR by invoking the Nudr_DataRepository_Query service operation during SM Policy Association Establishment procedure (see subclause 5.2.1).

   The PCF generates the PCC rule(s) based on the AF request and provides it to the SMF. If the AF subscribes to UP Path change event, the PCF includes the Notification URI pointing to the NEF and the Notification Correlation ID assigned by NEF (i.e. AF Transaction Internal ID) within the corresponding PCC rule(s) as specified in 3GPP TS 29.512 [9]. If the AF unsubscribes from UP Path change event, the PCF removes the related subscription information from the corresponding PCC rule(s) as specified in 3GPP TS 29.512 [9].

7. If the SMF observes PDU Session related event(s) that AF has subscribed to, the SMF invokes the Nsmf_EventExposure_Notify service operation to the NEF by sending an HTTP POST request to the resource URI "{notifUri}".

8. When receiving the Nsmf_EventExposure_Notify service operation, the NEF performs information mapping (e.g. AF Transaction Internal ID to AF Transaction ID), and invokes the Nnef_TrafficInfluence_Notify service operation to forward the notification to the AF by sending the HTTP request to the resource URI "notificationDestination" as specified in TS 29.522 [24].

9. The AF sends an HTTP "204 No Content" response to the NEF.

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

If the AF traffic influence request affects ongoing PDU session, the traffic influence procedure is performed as depicted in Figure 5.5.3.3-2.

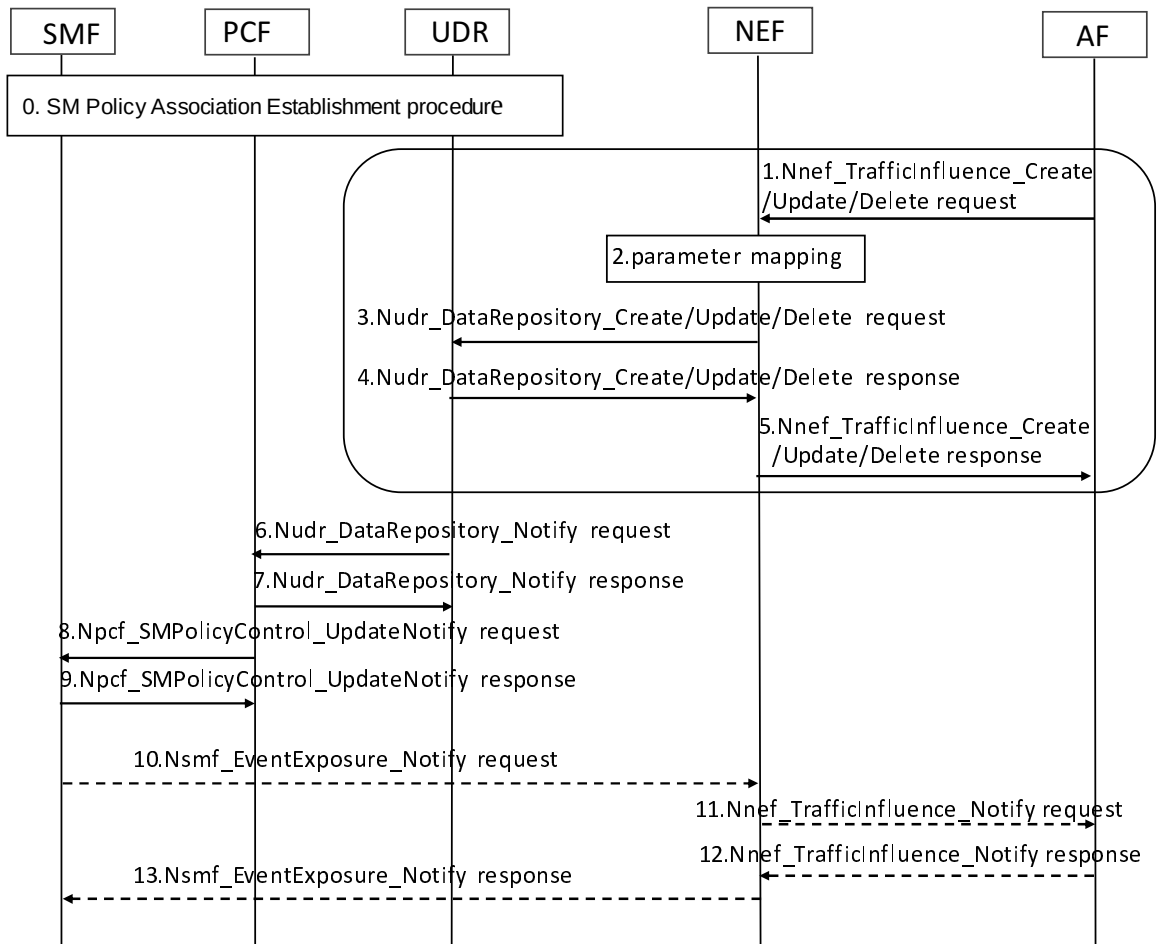


Figure 5.5.3.3-2: Processing AF requests to influence traffic routing for Sessions not identified by an UE address, affecting ongoing PDU session

0. The PCF subscribes to the changes of traffic influence data in the UDR during SM Policy Association procedure (see subclause 5.2.1).

1-5. These steps are the same as steps 1-5 in Figure 5.5.3.3-1.

6-7. The UDR invokes the Nudr_DataRepository_Notify service operation to PCF(s) that have subscribed to modifications of AF requests by sending the HTTP POST request to the resource URI "{notificationUri}", and the PCF sends a "204 No Content" response to the UDR.

8-9. Upon receipt of the AF request from the UDR, the PCF determines if existing PDU Sessions are potentially impacted by the AF request. For each of these PDU Sessions, the PCF invokes the Npcf_SMPolicyControl_UpdateNotify service operation to update the SMF with corresponding PCC rule(s) by sending the HTTP POST request to the resource URI "{Notification URI}/update" as described in subclause 5.2.2.2.1.

If the AF subscribes to UP Path change event, the PCF includes the Notification URI pointing to the NEF and the Notification Correlation ID (i.e. AF Transaction Internal ID) within the corresponding PCC rule(s) as specified in 3GPP TS 29.512 [9]. If the AF unsubscribes from UP Path change event, the PCF removes the related subscription information from the corresponding PCC rule(s) as specified in 3GPP TS 29.512 [9].

10-13. These steps are the same as steps 7-10 in Figure 5.5.3.3-1.

5.5.4 Negotiation for future background data transfer procedure

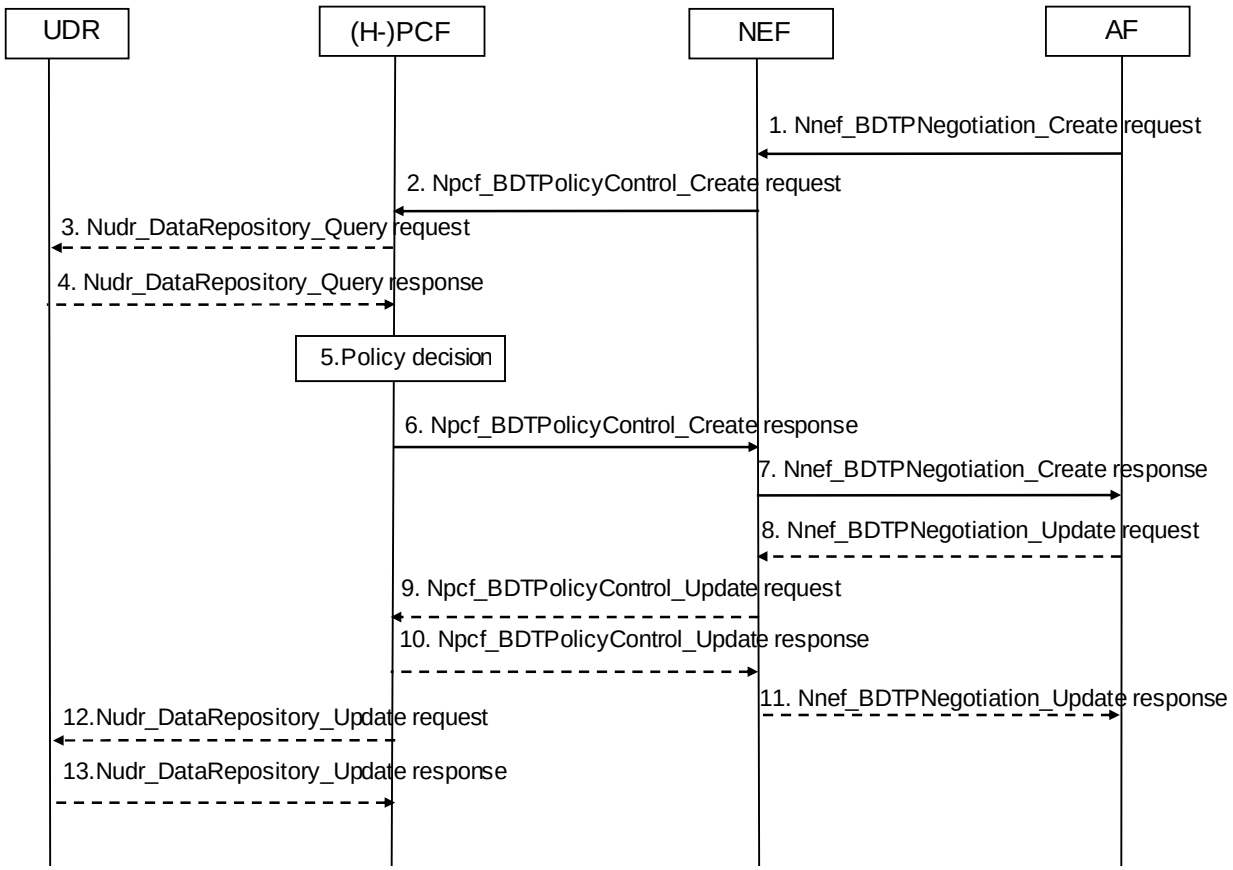


Figure 5.5.4-1: Negotiation for future background data transfer procedure

1. The AF invokes the Nnef_BDTPNegotiation_Create service operation by sending an HTTP POST request to the resource "BDT Subscription" 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 either as a geographical area (e.g. a civic address or shapes), or an area of interest that includes a list of TAs and/or list of NG-RAN nodes and/or a list of cell identifiers. When the AF provides a geographical area, then the NEF maps it based on local configuration into a short list of TAs and/or NG-RAN nodes and/or cells identifiers that is provided to the (H-)PCF.

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 "BDT policies". The request operation includes the ASP identifier, the volume of data to be transferred per UE, the expected number of UEs, the desired time window, and optionally the network area information (list of TAIs and/or NG-RAN nodes and/or cells identifiers).

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

3-4. The (H-) PCF may invoke the Nudr_DataRepository_Query service operation by sending an HTTP GET request to the resource "BdtData", to request from the UDR all stored transfer policies. The UDR sends an HTTP "200 OK" response to the (H-) PCF.

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.

5. 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, network area information and load status estimation for the desired time window).

6. 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.

7. The NEF sends a "201 Created" response to forward the received transfer policies to the AF. If the NEF received only one background transfer policy from the (H) PCF, steps 8-11 are not executed and the flow proceeds to step 12. Otherwise, the flow proceeds to step 8.

8. The AF invokes the Nnef_BDTPNegotiation_Update service operation by sending an HTTP PATCH request to the resource "Individual BDT Subscription" to provide the NEF with the selected background data transfer policy.

9. The NEF invokes the Npcf_BDTPolicyControl_Update service operation by sending an HTTP PATCH request to the resource "Individual BDT policy" to provide the (H-)-PCF with the selected background data transfer policy.

10. The (H-) PCF sends an HTTP PATCH response message to the NEF.

11. The NEF sends an HTTP PATCH response message to the AF.

12-13. If the (H-)PCF does not locally store the transfer policy, it invokes the Nudr_DataRepository_Update service operation by sending an HTTP PUT request to the resource "IndividualBdtData", to store for the provided ASP identifier the new transfer policy together with the associated background data transfer reference ID, the volume of data per UE, the expected number of UEs and if available the corresponding network area information in the UDR. The UDR sends an HTTP "201 Created" response to the (H-)PCF.

NOTE 4: For details of Nnef_BDTPNegotiation_Create/Update service operations refer to 3GPP TS 29.522 [24].

NOTE 5: For details of Npcf_BDTPolicyControl_Create/Update service operations refer to 3GPP TS 29.554 [26].

NOTE 6: For details of Nudr_DataRepository_Query/Update service operations refer to 3GPP TS 29.519 [12] and 3GPP TS 29.504 [27].

5.6 UE Policy Association Management

5.6.1 UE Policy Association Establishment

5.6.1.1 General

The procedures in this subclause are performed when the UE initially registers with the network, when the UE registers with 5GS during the UE moving from EPS to 5GS and if there is no existing UE Policy Association or when the new AMF establishes the UE Policy Association with the new PCF during AMF relocation.

NOTE 1: For details of the Nudr_DataRepository_Query/Update/Subscribe service operations refer to 3GPP TS 29.519 [12].

NOTE 2: For details of the Npcf_UEPolicyControl_Create/Update service operations refer to 3GPP TS 29.525 [31].

NOTE 3: For details of the Namf_Communication_N1N2MessageTransfer/N1N2MessageSubscribe/ N1MessageNotify service operations refer to 3GPP TS 29.518 [32].

5.6.1.2 Non-roaming

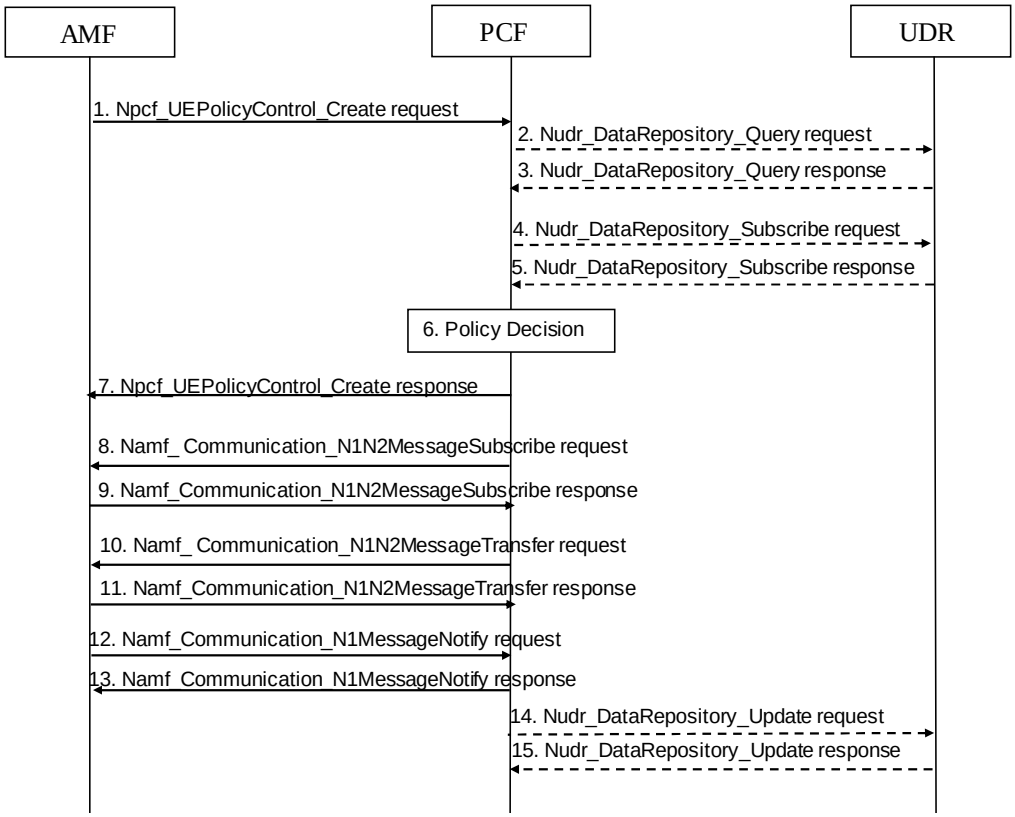


Figure 5.6.1.2-1: UE Policy Association Establishment procedure - Non-roaming

1. The AMF receives the registration request from the AN. Based on local policy, the AMF selects to contact the PCF to create the UE policy association with the PCF and to retrieve the UE policy. The AMF invokes the Npcf_UEPolicyControl_Create service operation by sending an HTTP POST request to the "UE Policy Associations" resource. The request includes the parameters as defined in subclause 4.2.2.1 of 3GPP TS 29.525 [31].

2. If the PCF does not have the subscription data or the latest list of UPSIs for the UE, it invokes the Nudr_DataRepository_Query service operation to the UDR by sending an HTTP GET request to the "UEPolicySet" resource.

3. The UDR sends an HTTP "200 OK" response to the PCF with the latest UPSIs and its content, and/or the subscription data.

4. The PCF may request notifications from the UDR on changes in the subscription information, and in this case, the PCF shall invoke the Nudr_DataRepository_Subscribe service operation by sending an HTTP POST request to the "PolicyDataSubscriptions" resource.

5. The UDR sends an HTTP "201 Created" response to acknowledge the subscription from the PCF.

6. The PCF determines whether and which UE policy has to be provisioned or updated as defined in subclause 4.2.2.2.1 of 3GPP TS 29.525 [31], and can determine applicable Policy Control Request Trigger(s).

In addition, the PCF checks if the size of determined UE policy exceeds a predefined limit.

NOTE: NAS messages from AMF to UE do not 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 UE policy information is included in a single Namf_Communication_N1N2MessageTransfer service operation and messages 10 to 13 are thus executed one time.

- If the size exceeds the predefined limit, the PCF splits the UE policy information in smaller logical independent UE policy information fragments and ensures the size of each is under the predefined limit. Each UE policy information fragment will be then sent in separated Namf_Communication_N1N2MessageTransfer service operations and messages 10 to 13 are thus executed several times, one time for each UE policy information fragment.

7. The PCF sends an HTTP "201 Created" response to the AMF with the Policy Control Request Trigger(s) if applicable.

8. To subscribe to notifications of N1 message for UE Policy Delivery Result, the PCF invokes Namf_Communication_N1N2MessageSubscribe service operation to the AMF by sending the HTTP POST method with the URI of the "N1N2 Subscriptions Collection for Individual UE Contexts" resource.

9. The AMF sends an HTTP "201 Created" response to the PCF.

10. If the PCF determines to provision or update the UE policy in step 6, the PCF sends the UE policy to the UE via the AMF by invoking the Namf_Communication_N1N2MessageTransfer service operation.

11. The AMF sends a response to the Namf_Communication_N1N2MessageTransfer service operation.

12. When receiving the UE Policy container, the AMF forwards the response of the UE to the PCF using Namf_Communication_N1MessageNotify service operation.

13. The PCF sends a response to the Namf_Communication_N1MessageNotify service operation.

14-15. The PCF maintains the latest list of UE policy sections delivered to the UE (in step 8) and updates the UE policy information for the subscriber including the latest list of UPSIs and its content in the UDR by invoking the Nudr_DataRepository_Update service operation.

- If there is no UE policy information retrieved in step 3, the PCF sends an HTTP PUT request to the "UEPolicySet" resource, and the UDR sends an HTTP "201 Created" response.

- Otherwise, the PCF sends an HTTP PUT/PATCH request to the "UEPolicySet" resource, and the UDR sends an HTTP "200 OK" or "204 No Content" response accordingly.

5.6.1.3 Roaming

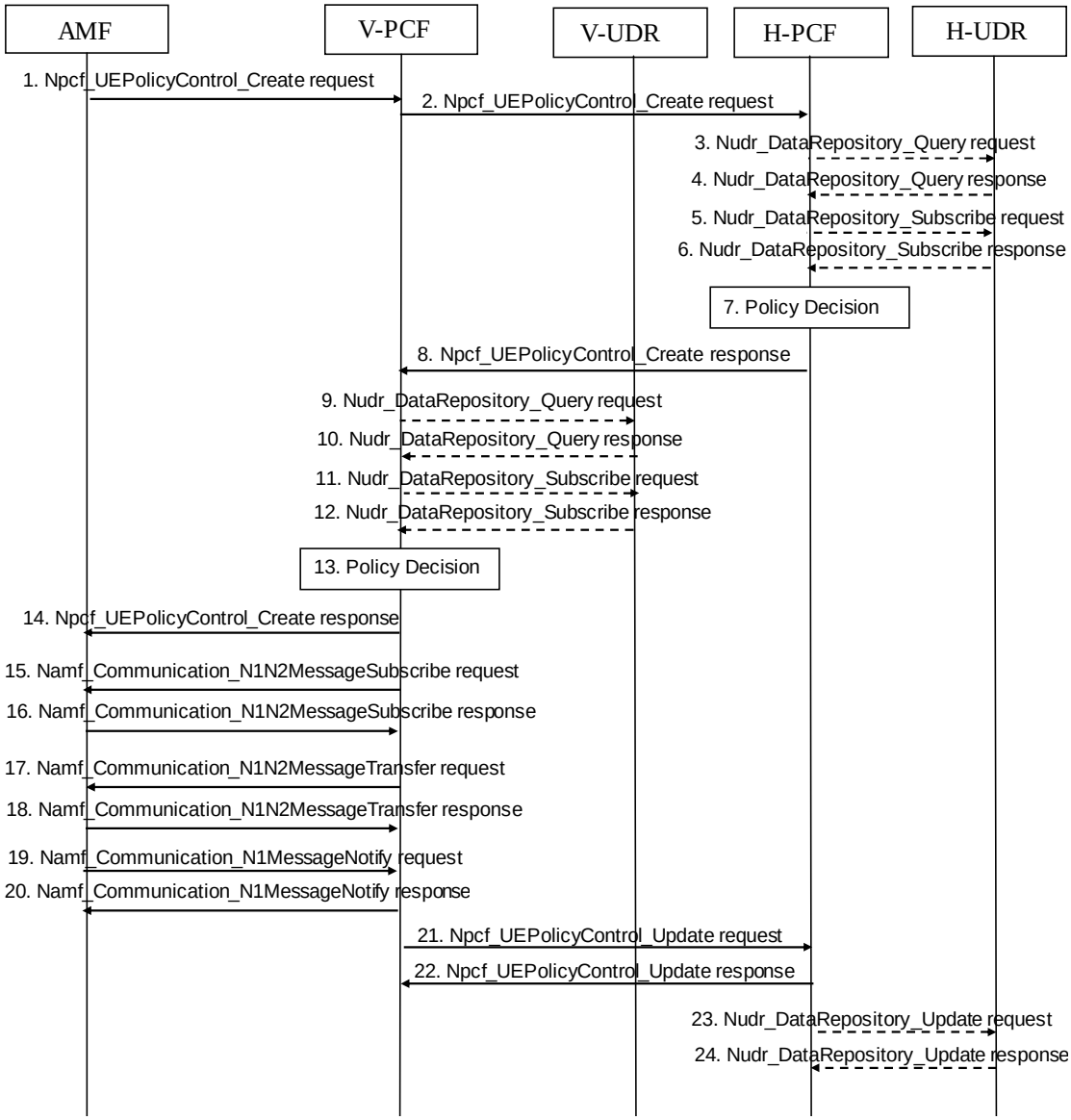


Figure 5.6.1.3-1: UE Policy Association Establishment procedure - Roaming

1. The AMF receives the registration request from the AN. Based on local policy, the AMF decides to establish UE Policy Association with the V-PCF. The AMF invokes the Npcf_UEPolicyControl_Create service operation by sending an HTTP POST request to the "UE Policy Associations" resource. The request includes the parameters as defined in subclause 4.2.2.1 of 3GPP TS 29.525 [31].

2. The V-PCF invokes the Npcf_UEPolicyControl_Create service operation by sending an HTTP POST request to the "UE Policy Associations" resource to forward the information received from AMF to the H-PCF. The request includes the parameters received in step 1. The V-PCF also provides the H-PCF the Notification URI where to send a notification when the policy is updated.

3-6. These steps are the same as steps 2-5 in subclause 5.6.1.2.

7. The H-PCF determines whether and which UE policy has to be provisioned or updated as defined in subclause 4.2.2.2.1 of 3GPP TS 29.525 [31], and may determine applicable Policy Control Request Trigger(s).

   In addition, the H-PCF checks if the size of determined UE policy exceeds a predefined limit.

NOTE 1: NAS messages from AMF to UE do not exceed the maximum size limit allowed in NG-RAN (PDCP layer), so the predefined size limit in H-PCF is related to that limitation.

If the size is under the limit then the UE policy information is included in Npcf_UEPolicyControl_Create response service operation.

- If the size exceeds the predefined limit, the H-PCF splits the UE policy information in smaller logical independent UE policy information fragments and ensures the size of each is under the predefined limit. One fragment will be sent in Npcf_UEPolicyControl_Create response service operation, and others will be sent by initiating the PCF-initiated UE Policy Association Modification procedure specified in subclause 5.6.2.2.3.

8. The H-PCF sends an HTTP "201 Created" response to the V-PCF with the decided UE policy and Policy Control Request Trigger(s) if available.

9. The V-PCF invokes Nudr_DataRepository_Query service operation to the UDR by sending an HTTP GET request to the "PlmnUePolicySet" resource to retrieve the list of UPSIs and its content stored in the V-UDR for the PLMN ID of this UE. Alternatively, the V-PCF can have this information configured locally.

NOTE 2: The UPSI list and content stored/configured for a PLMN ID can be structured according to e.g. location areas (e.g. TAs, PRAs). The V-PCF can then provide UPSIs and its content only if they correspond to the current UE location.

10. The V-UDR sends an HTTP "200 OK" response to the V-PCF with the UE policy information.

11. The V-PCF may request notifications from the V-UDR on changes in UE policy information, and in this case, the PCF shall invoke the Nudr_DataRepository_Subscribe service operation by sending an HTTP POST request to the "PolicyDataSubscriptions" resource.

12. The V-UDR sends an HTTP "201 Created" response to acknowledge the subscription from the V-PCF.

13. The V-PCF determines whether and which UE policy has to be provisioned or updated as defined in subclause 4.2.2.2.1 of 3GPP TS 29.525 [31], and may determine applicable Policy Control Request Trigger(s).

    In addition, the V-PCF checks if the size of determined UE policy exceeds a predefined limit.

NOTE 3: NAS messages from AMF to UE do not exceed the maximum size limit allowed in NG-RAN (PDCP layer), so the predefined size limit in V-PCF is related to that limitation.

- If the size is under the limit then the UE policy information is included in a single Namf_Communication_N1N2MessageTransfer service operation and messages 17 to 22 are thus executed one time.

- If the size exceeds the predefined limit, the V-PCF splits the UE policy information in smaller logical independent UE policy information fragments and ensures the size of each is under the predefined limit. Each UE policy information fragment will be then sent in separated Namf_Communication_N1N2MessageTransfer service operations and messages 17 to 22 are thus executed several times, one time for each UE policy information fragment.

14. The V-PCF sends an HTTP "201 Created" response to the AMF with the Policy Control Request Trigger(s) if available.

15. To subscribe to notifications of N1 message for UE Policy Delivery Result, the V-PCF invokes Namf_Communication_N1N2MessageSubscribe service operation to the AMF by sending the HTTP POST method with the URI of the "N1N2 Subscriptions Collection for Individual UE Contexts" resource.

16. The AMF sends an HTTP "201 Created" response to the V-PCF.

17. The V-PCF invokes the Namf_Communication_N1N2MessageTransfer service operation to send the policy decided locally in step 13 and to forward the policy received from the H-PCF in step 8.

18. The AMF sends a response to the Namf_Communication_N1N2MessageTransfer service operation.

19. When receiving the UE Policy container for the result of the UE policy, the AMF forwards the response of the UE to the V-PCF using Namf_Communication_N1MessageNotify service operation.

20. The V-PCF sends a response to the Namf_Communication_N1MessageNotify service operation.

21. Upon receipt of the UE Policy container belonging to the H-PLMN in step 19, the V-PCF invokes the Npcf_UEPolicyControl_Update service operation by sending an HTTP POST request to the "Individual UE Policy Association" resource to forward the response of the UE to the H-PCF.

22. The H-PCF sends an HTTP "200 OK" response to the V-PCF.

23-24. The H-PCF maintains the latest list of UE policy information delivered to the UE and updates UE policy including the latest list of UPSIs and its content in the H-UDR by invoking the Nudr_DataRepository_Update service operation.

- If there is no UE policy information retrieved in step 4, the H-PCF sends an HTTP PUT request to the "UEPolicySet" resource, and the UDR sends an HTTP "201 Created" response.

- Otherwise, the H-PCF sends an HTTP PUT/PATCH request to the "UEPolicySet" resource, and the H-UDR sends an HTTP "200 OK" or "204 No Content" response accordingly.

5.6.2 UE Policy Association Modification

5.6.2.1 UE Policy Association Modification initiated by the AMF

5.6.2.1.1 General

The procedures in this subclause are performed when a Policy Control Request Trigger condition is met or when the new AMF establishes the UE Policy Association with the old PCF during AMF relocation.

NOTE 1: For details of the Nudr_DataRepository_Update service operation refer to 3GPP TS 29.519 [12].

NOTE 2: For details of the Npcf_UEPolicyControl_Update/UpdateNotify service operations refer to 3GPP TS 29.525 [31].

NOTE 3: For details of the Namf_Communication_N1N2MessageTransfer/N1MessageNotify service operations refer to 3GPP TS 29.518 [32].

5.6.2.1.2 Non-roaming

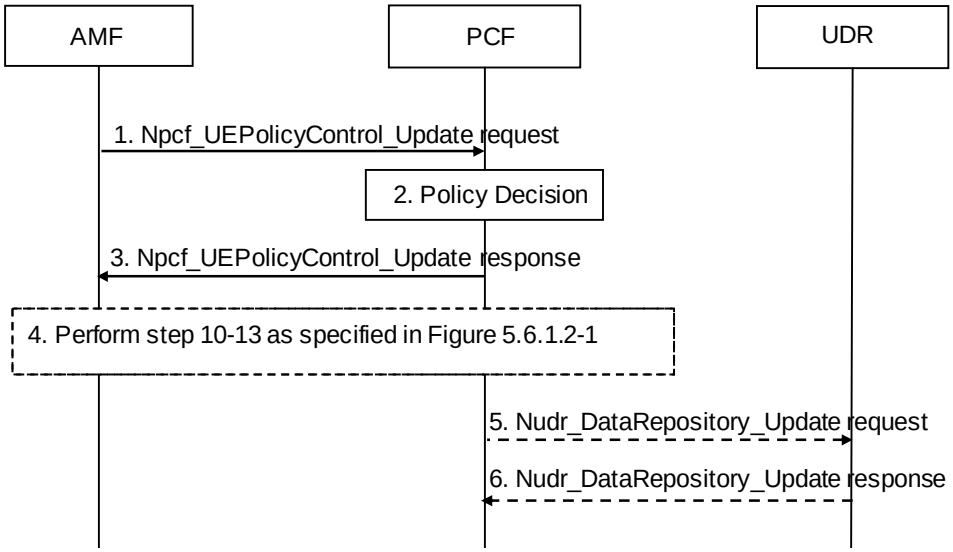


Figure 5.6.2.1.2-1: AMF-initiated UE Policy Association Modification procedure – Non-roaming

1. When the AMF detects a Policy Control Request Trigger condition is met or when the new AMF decides to establish the UE Policy Association with the old PCF during AMF relocation, it invokes the Npcf_UEPolicyControl_Update service operation to the PCF by sending an HTTP POST request to the "Individual UE Policy Association" resource with information on the conditions that have changed.

2. The PCF makes the policy decision including the applicable updated Policy Control Request Trigger(s) and/or updated UE Policy. The PCF checks if the size of determined UE policy exceeds a predefined limit the same as step 6 in subclause 5.6.1.2.

3. The PCF sends an HTTP "200 OK" response to the AMF with the applicable updated Policy Control Request Trigger(s).

4. If the PCF decided to update the UE policy in step 2, steps 10-13 as specified in Figure 5.6.1.2-1 are executed.

5-6. If the PCF decided to update the UE policy in step 2, the PCF maintains the latest list of UE policy information delivered to the UE and updates UE policy including the latest list of UPSIs and its content in the UDR by invoking the Nudr_DataRepository_Update service operation. The PCF sends an HTTP PUT/PATCH request to the "UEPolicySet" resource, and the UDR sends an HTTP "204 No Content" response.

5.6.2.1.3 Roaming

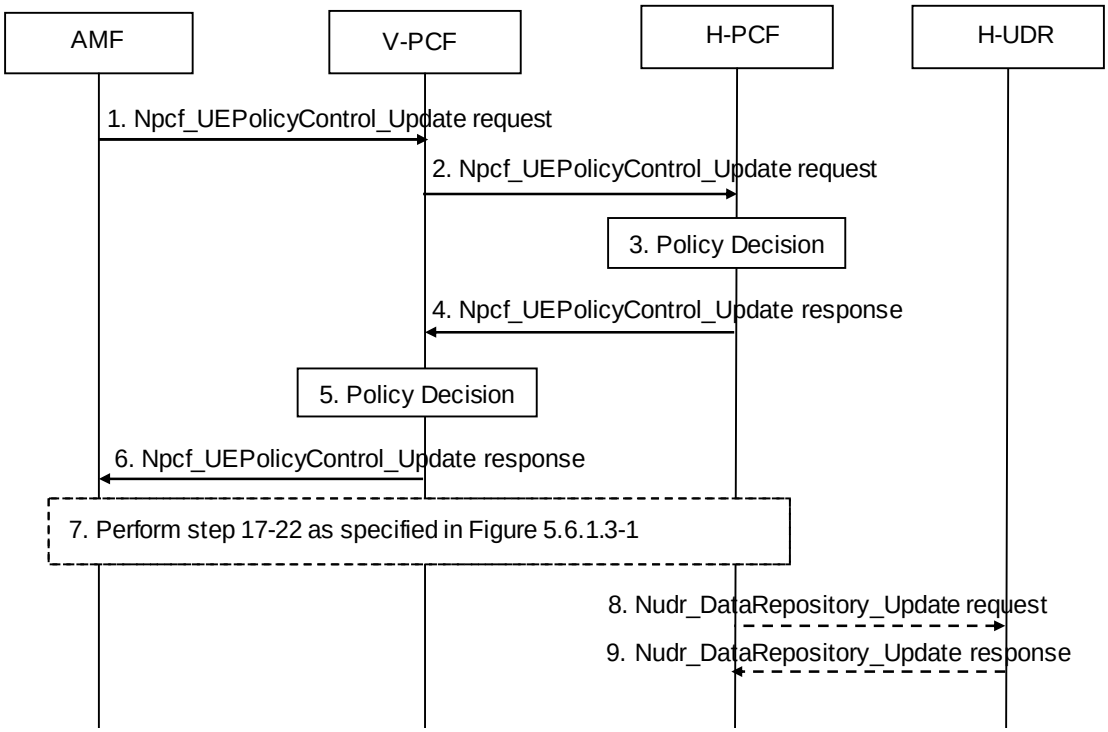


Figure 5.6.2.1.3-1: AMF-initiated UE Policy Association Modification procedure - Roaming

1. When the AMF detects a Policy Control Request Trigger condition is met or when the new AMF decides to establish the UE Policy Association with the old PCF during AMF relocation, it invokes the Npcf_UEPolicyControl_Update service operation to the V-PCF by sending an HTTP POST request to the "Individual UE Policy Association" resource with information on the conditions that have changed.

2. The V-PCF forwards the information received from AMF in step 1 to the H-PCF by sending an HTTP POST request to the "Individual UE Policy Association" resource if the H-PCF has subscribed the notification.

3. The H-PCF makes the policy decision including the applicable updated Policy Control Request Trigger(s) and/or updated UE Policy.

   In addition, the H-PCF checks if the size of determined UE policy exceeds a predefined limit.

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

- If the size is under the limit then the UE policy information is included in Npcf_UEPolicyControl_Update response service operation.

- If the size exceeds the predefined limit, the H-PCF splits the UE policy information in smaller logical independent UE policy information fragments and ensures the size of each is under the predefined limit. One fragment will be sent in Npcf_UEPolicyControl_Update response service operation, and others will be then sent by initiating the PCF-initiated UE Policy Association Modification procedure specified in subclause 5.6.2.2.3.

4. The H-PCF sends an HTTP "200 OK" response to the V-PCF with the updated policy information decided in step 3.

5. The V-PCF makes the policy decision including the applicable updated Policy Control Request Trigger(s) and/or updated UE Policy. The V-PCF checks if the size of determined UE policy exceeds a predefined limit the same as step 13 in subclause 5.6.1.3.

6. The V-PCF sends an HTTP "200 OK" response to the AMF with the applicable updated Policy Control Request Trigger(s).

7. If the V-PCF decided to update the UE policy in step 5 or the V-PCF received the UE Policy in step 4, steps 17-22 as specified in Figure 5.6.1.3-1 are executed.

8-9. If the H-PCF decided to update the UE policy in step 3, the H-PCF maintains the latest list of UE policy information delivered to the UE and updates UE policy including the latest list of UPSIs and its content in the H-UDR by invoking the Nudr_DataRepository_Update service operation. The PCF sends an HTTP PUT/PATCH request to the "UEPolicySet" resource, and the UDR sends an HTTP "204 No Content" response.

5.6.2.2 UE Policy Association Modification initiated by the PCF

5.6.2.2.1 General

The procedures in this subclause are performed when the UE policy is changed.

NOTE 1: For details of the Nudr_DataRepository_Update service operation refer to 3GPP TS 29.519 [12].

NOTE 2: For details of the Npcf_UEPolicyControl_UpdateNotify service operation refer to 3GPP TS 29.525 [31].

NOTE 3: For details of the Namf_Communication_N1N2MessageTransfer/N1MessageNotify service operations refer to 3GPP TS 29.518 [32].

5.6.2.2.2 Non-roaming

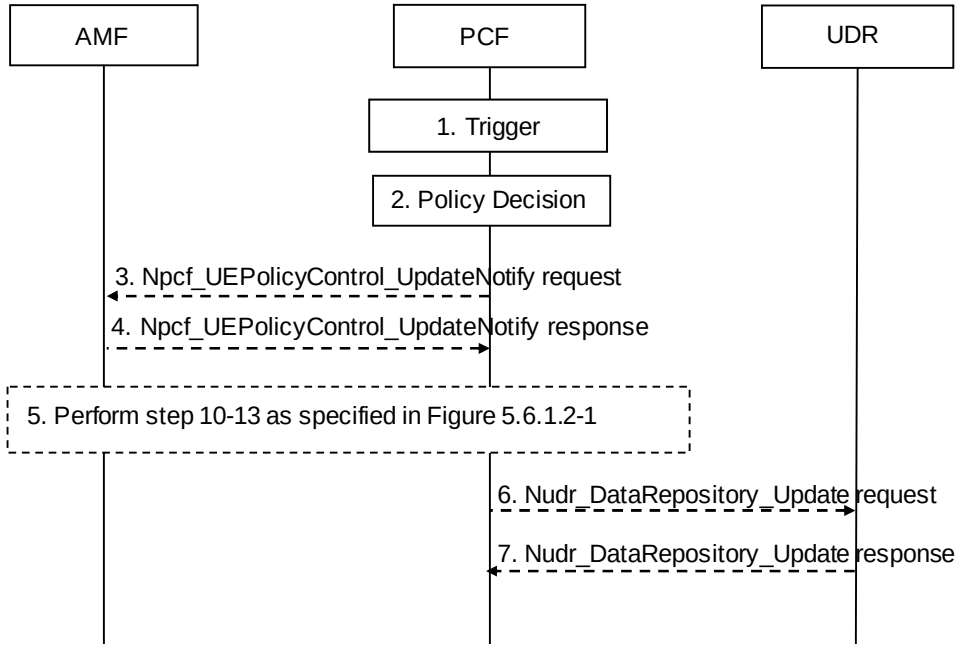


Figure 5.6.2.2.2-1: PCF-initiated UE Policy Association Modification procedure – Non-roaming

1. The PCF receives an external trigger, e.g. the subscriber policy data of a UE is changed or application detection, or the PCF receives an internal trigger, e.g. operator policy is changed, to re-evaluate UE policy decision for a UE.

2. The PCF makes the policy decision including the applicable updated Policy Control Request Trigger(s) and/or updated UE Policy. The PCF checks if the size of determined UE policy exceeds a predefined limit the same as step 6 in subclause 5.6.1.2.

3. If the PCF decided to update the Policy Control Request Trigger(s) in step 2, the V-PCF shall invoke the Npcf_UEPolicyControl_UpdateNotify service operation by sending an HTTP POST request to the resource URI "{Notification URI}/update".

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

5. If the PCF decided to update the UE policy in step 2, steps 10-13 as specified in Figure 5.6.1.2-1 are executed.

6-7. If the PCF decided to update the UE policy in step 2, steps 5-6 in subclause 5.6.2.1.2 are executed.

5.6.2.2.3 Roaming

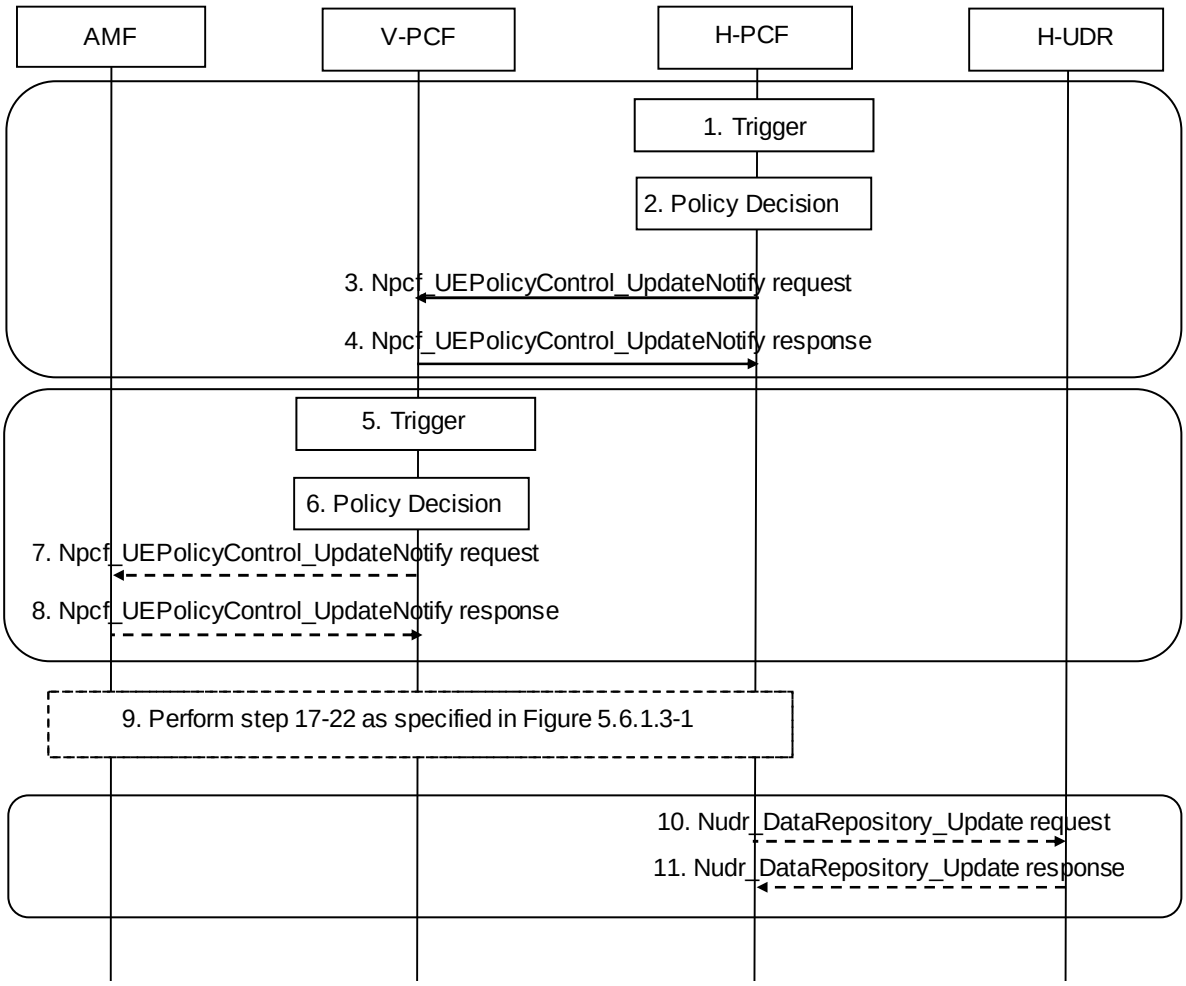


Figure 5.6.2.2.3-1: PCF-initiated UE Policy Association Modification procedure – Roaming

If the H-PCF receives a trigger, steps 1 to 4 and 10 to 11 are executed and steps 5 to 8 are omitted.

If the V-PCF receives a trigger, steps 1 to 4 and 10 to 11 are omitted and steps 5 to 8 are executed.

1. The H-PCF receives an external trigger, e.g. the subscriber policy data of a UE is changed, or the PCF receives an internal trigger, e.g. operator policy is changed, to re-evaluate UE policy decision for a UE.

2. The H-PCF makes the policy decision including the applicable updated Policy Control Request Trigger(s) and/or updated UE Policy.

   In addition, the H-PCF checks if the size of determined UE policy exceeds a predefined limit.

NOTE 1: NAS messages from AMF to UE do not exceed the maximum size limit allowed in NG-RAN (PDCP layer), so the predefined size limit in H-PCF is related to that limitation.

- If the size is under the limit then the UE policy information is included in a single Npcf_UEPolicyControl_UpdateNotify service operation and messages 3 to 4 are thus executed one time.

- If the size exceeds the predefined limit, the PCF splits the UE policy information in smaller logical independent UE policy information fragments and ensures the size of each is under the predefined limit. Each UE policy information fragment will be then sent in separated Npcf_UEPolicyControl_UpdateNotify service operations and messages 3 to 4, and 9 are thus executed several times, one time for each UE policy information fragment.

3. The H-PCF invokes the Npcf_UEPolicyControl_UpdateNotify service operation by sending an HTTP POST request to the resource URI "{Notification URI}/update" with the updated UE policy and/or Policy Control Request Trigger(s) if applicable.

4. The V-PCF sends an HTTP "204 No Content" response to the H-PCF.

5. The V-PCF receives an external trigger, e.g. operator policy in the V-UDR for the PLMN ID of this UE is changed, or the V-PCF receives an internal trigger, e.g. local policy is changed, to re-evaluate UE policy decision for a UE.

6. The V-PCF makes the policy decision including the applicable updated Policy Control Request Trigger(s) and/or updated UE Policy.

   In addition, the V-PCF checks if the size of determined UE policy and received UE policy from H-PCF in step 3 exceeds a predefined limit.

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

- If the size is under the limit then the UE policy information is included in a single Namf_Communication_N1N2MessageTransfer service operation and message 9 is thus executed one time.

- If the size exceeds the predefined limit, the V-PCF splits the UE policy information in smaller logical independent UE policy information fragments and ensures the size of each is under the predefined limit. Each UE policy information fragment will be then sent in separated Namf_Communication_N1N2MessageTransfer service operations and message 9 is thus executed several times, one time for each UE policy information fragment.

7. If the V-PCF needs to update the Policy Control Request Trigger(s) or forward the Policy Control Request Trigger(s) received from the H-PCF in step 3, the V-PCF shall invoke the Npcf_UEPolicyControl_UpdateNotify service operation by sending an HTTP POST request to the resource URI "{Notification URI}/update".

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

9. If the V-PCF decided to update the UE policy in step 6 or the V-PCF received the UE Policy in step 3, steps 17-22 as specified in Figure 5.6.1.3-1 are executed.

10-11. If the H-PCF decided to update the UE policy in step 2, the steps 8-9 in subclause 5.6.2.1.3 are executed.

5.6.3 UE Policy Association Termination

5.6.3.1 UE Policy Association Termination initiated by the AMF

5.6.3.1.1 General

This procedure is performed when the UE deregisters from the network, when the UE deregisters from 5GS during the UE moving from 5GS to EPS or when the old AMF removes the UE Policy Association during AMF relocation.

NOTE 1: For details of the Nudr_DataRepository_Unsubscribe service operation refer to 3GPP TS 29.519 [12].

NOTE 2: For details of the Npcf_UEPolicyControl_Delete service operation refer to 3GPP TS 29.525 [31].

NOTE 3: For details of the Namf_Communication_N1N2MessageUnsubscribe service operation refer to 3GPP TS 29.518 [32].

5.6.3.1.2 Non-roaming

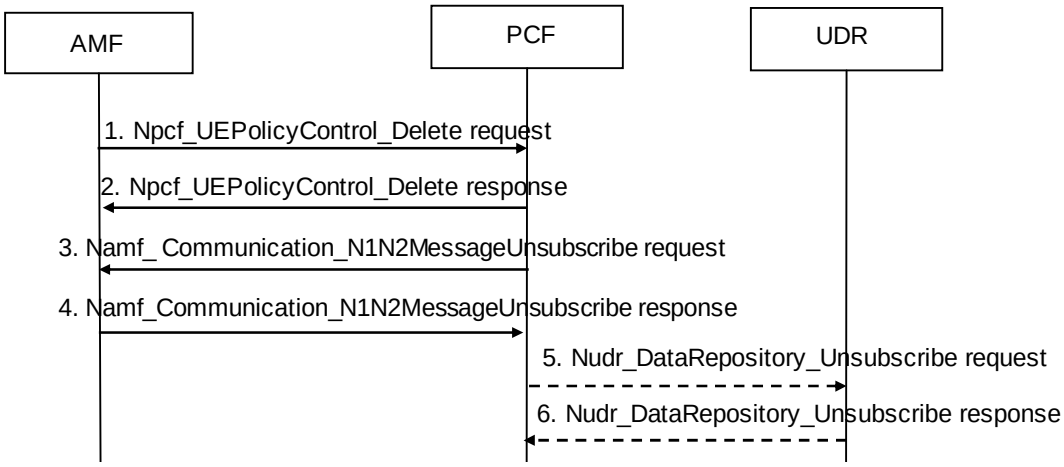


Figure 5.6.3.1.2-1: AMF-initiated UE Policy Association Termination procedure – Non-roaming

1. The AMF invokes the Npcf_UEPolicyControl_Delete service operation by sending the HTTP DELETE request to the "Individual UE Policy Association" resource to delete the policy context in the PCF.
2. The PCF removes the policy context for the UE and sends an HTTP "204 No Content" response to the AMF.
3. To unsubscribe to notifications of N1 message for UE Policy Delivery Result, the PCF invokes Namf_Communication_N1N2MessageUnsubscribe service operation to the AMF by sending the HTTP DELETE method with the URI of the "N1N2 Individual Subscription" resource.
4. The AMF sends an HTTP "204 No Content" response to the PCF.
5. The PCF unsubscribes the notification of subscriber policy data modification from the UDR by invoking Nudr_DataRepository_Unsubscribe service operation by sending the HTTP DELETE request to the "IndividualPolicyDataSubscription" resource if it has subscribed such notification.
6. The UDR sends an HTTP "204 No Content" response to the PCF.

5.6.3.1.3 Roaming

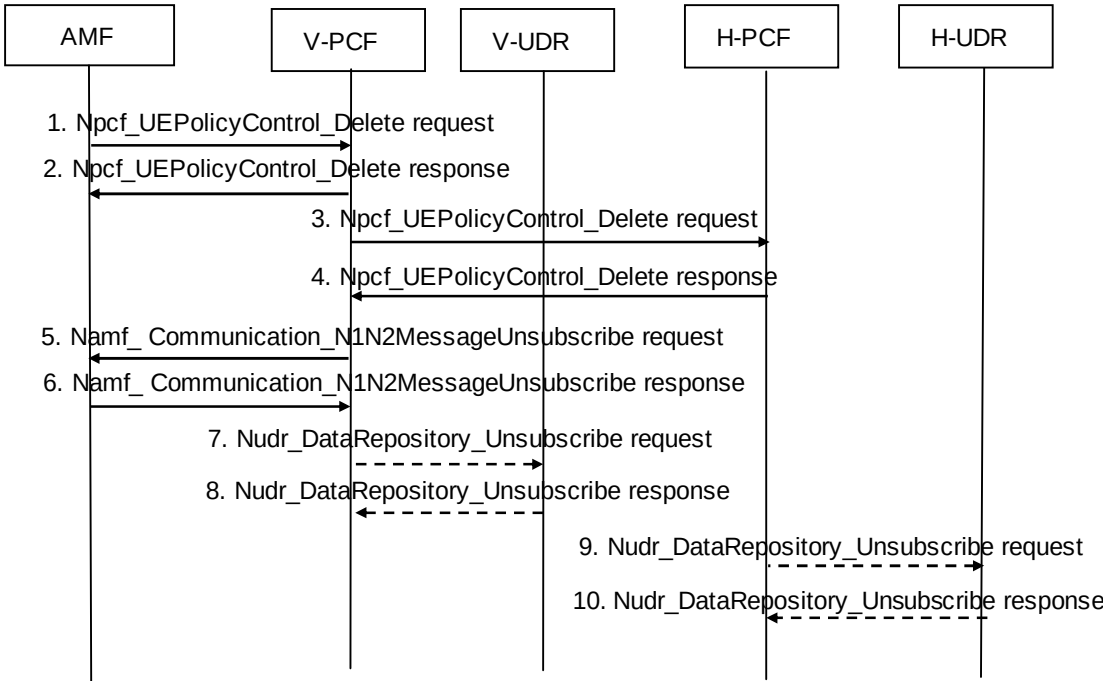


Figure 5.6.3.1.3-1: AMF-initiated UE Policy Association Termination procedure – Roaming

1. The AMF invokes the Npcf_UEPolicyControl_Delete service operation by sending the HTTP DELETE request to the "Individual UE Policy Association" resource to delete the policy context in the V-PCF. The V-PCF interacts with the H-PCF.
2. The V-PCF removes the policy context for the UE and sends an HTTP "204 No Content" response to the AMF.
3. The V-PCF invokes the Npcf_UEPolicyControl_Delete service operation by sending the HTTP DELETE request to the "Individual UE Policy Association" resource to delete the policy context in the H-PCF.
4. The H-PCF removes the policy context for the UE and sends an HTTP "204 No Content" response to the V-PCF.
5. To unsubscribe to notifications of N1 message for UE Policy Delivery Result, the V-PCF invokes Namf_Communication_N1N2MessageUnsubscribe service operation to the AMF by sending the HTTP DELETE method with the URI of the "N1N2 Individual Subscription" resource.
6. The AMF sends an HTTP "204 No Content" response to the V-PCF.
7. The V-PCF invokes the Nudr_DataRepository_Unsubscribe service operation by sending the HTTP DELETE request to the "IndividualPolicyDataSubscription" resource to unsubscribes the notification from the V-UDR on changes in UE policy information if it has subscribed such notification.
8. The V-UDR sends an HTTP "204 No Content" response to the V-PCF.
9. The H-PCF unsubscribes the notification of subscriber policy data modification from the H-UDR by invoking Nudr_DataRepository_Unsubscribe service operation by sending the HTTP DELETE request to the "IndividualPolicyDataSubscription" resource if it has subscribed such notification.
10. The H-UDR sends an HTTP "204 No Content" response to the H-PCF.

5.6.3.2 UE Policy Association Termination initiated by the PCF

5.6.3.2.1 General

This procedure is performed when the (H-)UDR notifies the (H-)PCF that the policy profile is removed.

NOTE 1: For details of the Nudr_DataRepository_Notify service operation refer to 3GPP TS 29.519 [12].

NOTE 2: For details of the Npcf_UEPolicyControl_UpdateNotify/Delete service operations refer to 3GPP TS 29.525 [31].

NOTE 3: For details of the Namf_Communication_N1N2MessageUnsubscribe service operation refer to 3GPP TS 29.518 [32].

5.6.3.2.2 Non-roaming

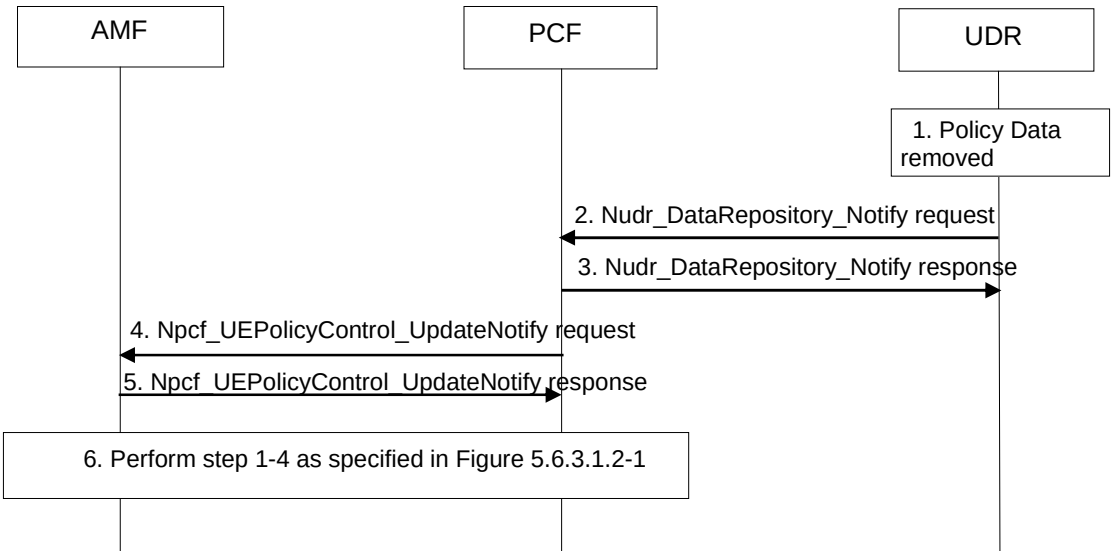


Figure 5.6.3.2.2-1: PCF-initiated UE Policy Association Termination procedure – Non-roaming

1. The subscriber policy control data is removed from the UDR.
2. The UDR invokes the Nudr_DataRepository_Notify service operation by sending the HTTP POST request to resource URI "{notificationUri}" to notify the PCF that the policy profile is removed if PCF has subscribed such notification.
3. The PCF sends HTTP "204 No Content" response to confirm reception and the result to UDR.
4. The PCF may, depending on operator policies, invoke the Npcf_UEPolicyControl_UpdateNotify service operation to the AMF of the removal of the UE policy control information by sending the HTTP POST request to the resource URI "{Notification URI}/terminate".

   Alternatively, the PCF may decide to maintain the UE 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. Steps 1 to 4 as specified in Figure 5.6.3.1.2-1 are executed.

5.6.3.2.3 Roaming

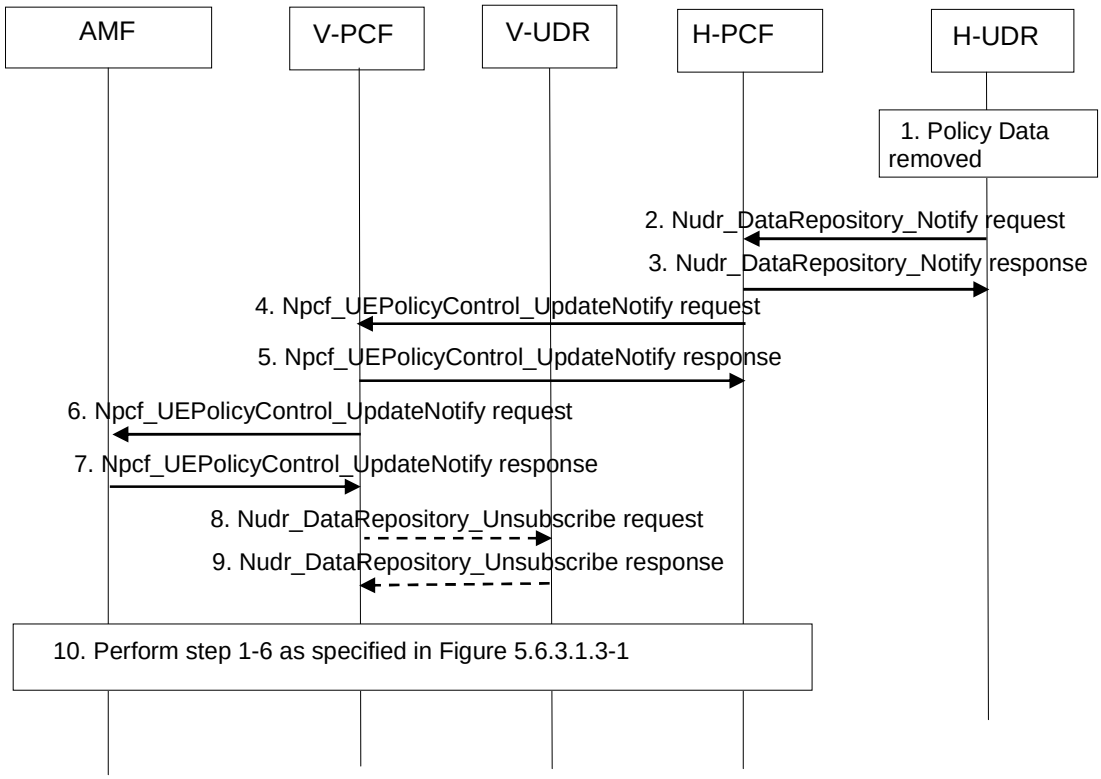


Figure 5.6.3.2.3-1: PCF-initiated UE Policy Association Termination procedure – Roaming

1. The subscriber policy control data is removed from the H-UDR.
2. The H-UDR invokes the Nudr_DataRepository_Notify service operation by sending the HTTP POST request to resource URI "{notificationUri}" to notify the H-PCF that the policy profile is removed if H-PCF has subscribed such notification.
3. The H-PCF sends HTTP "204 No Content" response to confirm reception and the result to H-UDR.
4. The H-PCF may, depending on operator policies, invoke the Npcf_UEPolicyControl_UpdateNotify service operation to the AMF of the removal of the UE policy control information by sending the HTTP POST request to the resource URI "{Notification URI}/terminate".

   Alternatively, the H-PCF may decide to maintain the UE Policy Association if a default profile is applied, and then step 4 through 10 are not executed.
5. The AMF sends an HTTP "204 No Content" response to the V-PCF.
6. The V-PCF invokes the Npcf_UEPolicyControl_UpdateNotify service operation to the AMF of the removal of the UE policy control information by sending the HTTP POST request to the resource URI "{Notification URI}/terminate".
7. The AMF sends an HTTP "204 No Content" response to the V-PCF.
8. The V-PCF invokes the Nudr_DataRepository_Unsubscribe service operation by sending the HTTP DELETE request to the "IndividualPolicyDataSubscription" resource to unsubscribe the notification from the V-UDR on changes in UE policy information if it has subscribed such notification.
9. The V-UDR sends an HTTP "204 No Content" response to the V-PCF.
10. Steps 1 to 6 as specified in Figure 5.6.3.1.3-1 are executed.

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 address. If IPv6 address is received from the AF, the association is done by comparing the /128 IPv6 address with the IPv6 prefix of the PDU session using the longest prefix match.

   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.

d) The IPv4 address domain identity if available in the "ipDomain" attribute.

NOTE 2: The "ipDomain" attribute is helpful when within a network slice instance, there are several separate IP address domains, with SMF/UPF(s) that allocate Ipv4 IP addresses out of the same private address range to UE PDU Sessions. The same IP address can thus be allocated to UE PDU sessions served by SMF/UPF(s) in different address domains. If one PCF controls several SMF/UPF(s) in different IP address domains, the UE IP address is thus not sufficient for the session binding. An AF can serve UEs in different IP address domains, either by having direct IP interfaces to those domains, or by having interconnections via NATs in the user plane between the UPF and the AF. If a NAT is used, the AF obtains the IP address allocated to the UE PDU session via application level signalling and supplies it for the session binding to the PCF in the "ueIpv4" attribute. The AF supplies an "ipDomain" attribute denoting the IP address domain behind the NAT in addition. The AF can derive the appropriate value from the source address (allocated by the NAT) of incoming user plane packets. The value provided in the "ipDomain" attribute is operator configurable.

e) The S-NSSAI if available.

NOTE 3: The S-NSSAI is helpful in the scenario where multiple network slice instances are deployed in the same DNN, and the same IPv4 address may be allocated to UE PDU sessions in different network slice instances. If one PCF controls several network slices, each network slice in different IP address domains, the UE IP address is not sufficient for the session binding. The AF supplies the S-NSSAI denoting the network slice instance that allocated the IPv4 address of the UE PDU session. How the AF derives S-NSSAI is out of the scope of this specification.

Session Binding applies for PDU sessions of IP type. It may also apply to Ethernet PDU session type but only when especially allowed by PCC related policy control request trigger. In the case of Ethernet PDU session, session binding does not apply to AF requests sent over Rx.

NOTE 4: For the Ethernet PDU session, the PCF needs to provision "UE MAC_CH" trigger to the SMF.

NOTE 5: Refer to 3GPP TS 29.213 [30] for the session binding between the IP type PDU session and the AF request sent over Rx.

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.

NOTE: The PCC rule authorization is not applicable to the Unstructured type PDU session.

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 selected QoS flow shall have the same above binding parameters as the one indicated by 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 QoS data decision which the PCC rule refers to includes the "defQosFlowIndication" attribute set to true as defined in subclause 4.2.6.2.10 of 3GPP TS 29.512 [9], the SMF shall bind the PCC rule to the default QoS flow as long as the "defQosFlowIndication" attribute set to true .

If the "defQosFlowIndication" attribute has not been received before during the lifetime of the PCC rule or the "defQosFlowIndication" attribute has been received but set to false (as defined in subclause 4.2.6.2.10 of 3GPP TS 29.512 [9]), 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.

NOTE 3: For PCC rules containing a delay critical GBR 5QI value, the SMF can bind PCC Rules with the same binding parameters to different QoS Flows to ensure that the GFBR of the QoS Flow can be achieved with the Maximum Data Burst Volume of the 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 has previously indicated to the SMF that a PCC rule shall be bound to the default QoS flow by including the "defQosFlowIndication" attribute set to true within the QoS data decision which the PCC rule refers to, but the PCF updates the QoS data decision by including the "defQosFlowIndication" attribute set to false as defined in subclause 4.2.6.2.10 of 3GPP TS 29.512 [9], the SMF shall create the binding between service data flow(s) and the QoS flow which have the same binding parameters.

If the PCC rule is corresponding to the QoS rule requested by the UE as defined in subclause 4.2.4.17 of 3GPP TS 29.512 [9] and a Segregation bit is set as defined in Table 9.11.4.13.1 of 3GPP TS 24.501 [33] in the request from the UE, the SMF should abide by the UE request and bind the PCC rule on a distinct and dedicated QoS Flow e.g. even if an existing QoS Flow can support the requested QoS, but is still allowed to proceed instead with binding the selected SDF(s) on an existing QoS Flow.

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 4: 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 "defQosFlowIndication" attribute set to true.

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

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].

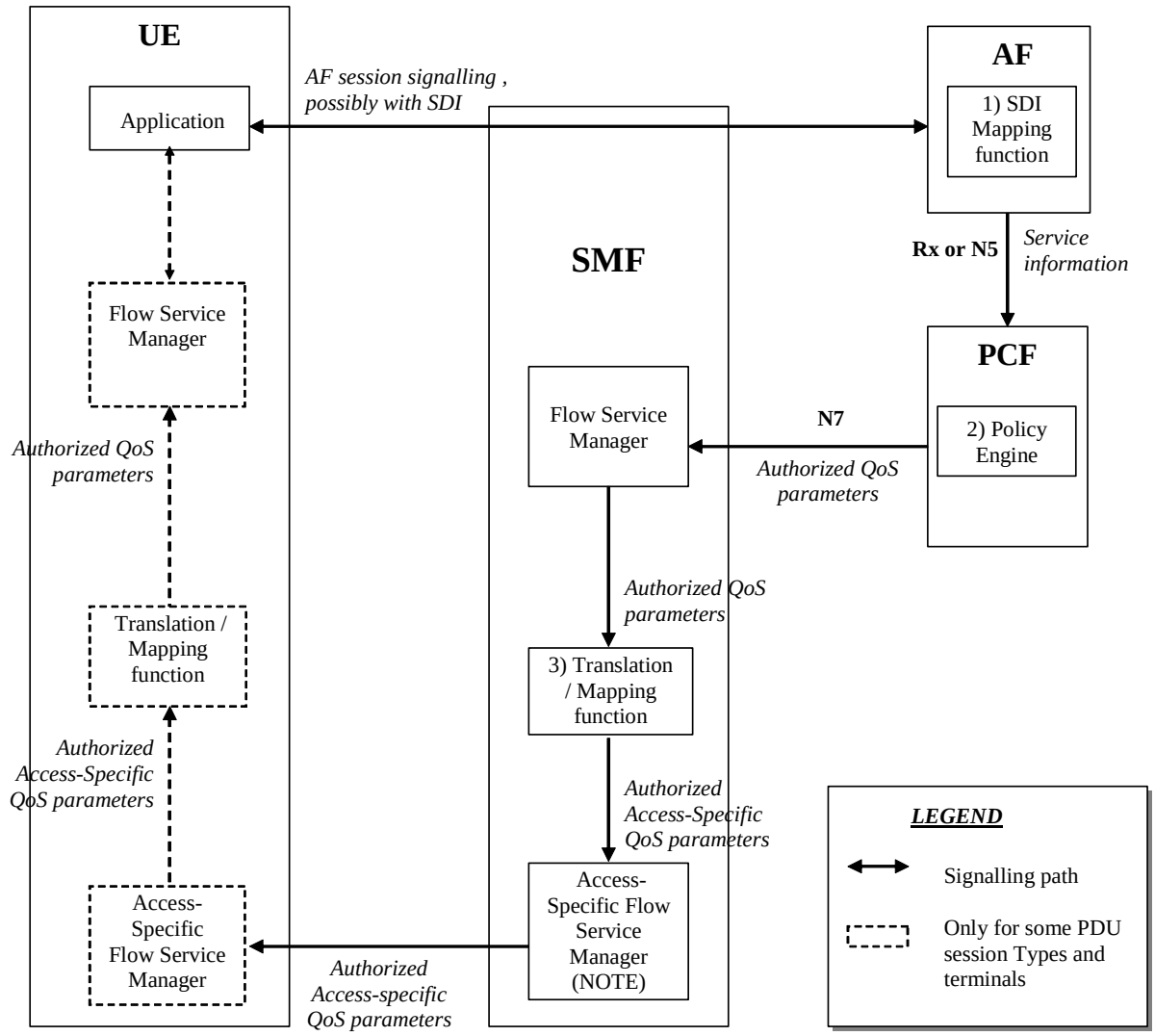
For IMS, the AF may pass service information to the PCF over the Rx interface. The AF derives information about the service from the SDI or from other sources. The mapping is application specific. If SDP (IETF RFC 4566 [16]) is used as SDI, the AF should apply the mapping described in subclause 7.2. If MPD (3GPP TS 26.247 [17]) is used, the AF may apply the mapping described in Annex I 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

7.2.1 Introduction

The mapping described in this clause is mandatory for the P-CSCF and should also be applied by other AFs, if the SDI is SDP.

When a session is initiated or modified the AF shall derive a Media-Component-Description AVP from the SDP Parameters.

7.2.2 AF supporting Rx interface

When the AF interworks with the PCF using the Rx interface, it shall derive a Media-Component-Description AVP from the SDP parameters for each SDP media component using the same mapping rules as defined in subclause 6.2 of 3GPP TS 29.213 [30].

7.2.3 AF supporting N5 interface

No QoS parameter mapping functions at AF is required in this Release.

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 Indication (RQI), 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
	Max_DR_DL:= MAX[0.05 * Maximum DL Requested Bandwidth, RR Bandwidth];
	ENDIF;

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

	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 7 and 14)	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;
	/* 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.
NOTE 14: The PCF may authorize a non-standardized 5QI with explicitly signalled QoS characteristics as defined in subclause 4.2.6.6.3 of 3GPP TS 29.512 [9] or may assign QoS characteristics (e.g. Priority Level, Averaging Window, and Maximum Data Burst Volume) to be used instead of the default QoS characteristics associated with a standardised 5QI value as shown in table 5.7.4-1 in 3GPP TS 23.501 [2].

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

When the AF interworks with the PCF using the N5 interface, the session binding in the PCF shall be associated to an IP session or an Ethernet session, and the PCF shall derive QoS parameters for the related data flows.

Table 7.3.3-1: 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 (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;
	(NOTE 8, 9 and 10)
	ELSE IF afAppId attribute of MediaComponent data type 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 codecs attribute of MediaComponent data type provides Codec information for a codec that is supported by a specific algorithm (NOTE 5) 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 flowUsage attribute of MediaSubComponent data type THEN
	IF fStatus attribute indicates “REMOVED” THEN
	Max_DR_UL:= 0;
	Max_DR_DL:= 0;
	ELSE
	IF Uplink Flow Description is supplied within the fDescs attribute of the MediaSubComponent data type THEN
	IF marBwUl attribute is present THEN
	Max_DR_UL:= marBwUl value;
	ELSE
	Max_DR_UL:= as set by the operator;
	ENDIF;
	ELSE
	Max_DR_UL:= 0;
	ENDIF;
	IF Downlink Flow Description is supplied within the fDescs attribute of the MediaSubComponent data type THEN
	IF marBwDl attribute is present THEN
	Max_DR_DL:= marBwDl value;
	ELSE
	Max_DR_DL:= as set by the operator;
	ENDIF;
	ELSE
	Max_DR_DL:= 0;
	ENDIF;
	ENDIF;
	ELSE /* RTCP IP flow(s) */
	IF fStatus attribute indicates “REMOVED” THEN
	Max_DR_UL:= 0;
	Max_DR_DL:= 0;
	ELSE
	IF Uplink Flow Description is supplied within the fDescs attribute of the MediaSubComponent data type THEN
	IF marBwUl attribute is present within the MediaSubComponent data type THEN
	Max_DR_UL:= marBwUl;
	ELSEIF marBwUl attribute is present within the MediaComponent data type THEN
	Max_DR_UL:= 0.05 * marBwUl value;
	ELSE
	Max_DR_UL:= as set by the operator;
	ENDIF;
	ELSE
	Max_DR_UL:= 0;
	ENDIF;
	IF Downlink Flow Description is supplied within the fDescs attribute of the MediaSubComponent data type THEN
	IF marBwDl attribute is present within the MediaSubComponent data type THEN
	Max_DR_DL:= marBwDl;
	ELSEIF marBwDl attribute is present within the MediaComponent data type THEN
	Max_DR_DL:= 0.05 * marBwDl value;
	ELSE
	Max_DR_DL:= as set by the operator;
	ENDIF;
	ELSE
	Max_DR_DL:= 0;
	ENDIF;
	ENDIF;
	ENDIF;
	ENDIF;

Authorized QoS Parameter	Derivation from service information (NOTE 4)

Authorized Guaranteed Data Rate DL (Gua_DR_DL) and UL (Gua_DR_UL)	IF operator special policy exists THEN
	Gua_DR_UL:= as defined by operator specific algorithm;
	Gua_DR_DL:= as defined by operator specific algorithm;
	
	ELSEIF afAppId attribute of MediaComponent data type 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 codecs attribute of MediaComponent data type provides Codec information for a codec that is supported by a specific algorithm (NOTE 5) THEN
	Gua_DR_UL:= as defined by specific algorithm;
	Gua_DR_DL:= as defined by specific algorithm;
	ELSE
	IF fStatus attribute indicates “REMOVED” THEN
	Max_DR_UL:= 0;
	Max_DR_DL:= 0;
	ELSE
	IF Uplink Flow Description is supplied within the fDescs attribute of the MediaSubComponent data type THEN
	IF mirBwUl attribute is present THEN
	Gua_DR_UL:= mirBwUl value;
	ELSE IF corresponding operator policy exists
	Gua_DR_UL:= as set by the operator;
	ELSE
	Gua_DR_UL:= Max_DR_UL;
	ENDIF;
	ELSE
	Gua_DR_UL:= 0;
	ENDIF;
	IF Downlink Flow Description is supplied within the fDescs attribute of the MediaSubComponent data type THEN
	IF mirBwDl attribute is present THEN
	Gua_DR_DL:= mirBwDl value;
	ELSE IF corresponding operator policy exists
	Gua_DR_DL:= as set by the operator;
	ELSE
	Gua_DR_DL:= Max_DR_DL;
	ENDIF;
	ELSE
	Gua_DR_DL:= 0;
	ENDIF;
	ENDIF;
	ENDIF;

Authorized 5G QoS Identifier (5QI)	IF an operator special policy exists THEN
	5QI:= as defined by operator specific algorithm;
	ELSE IF mpsId attribute 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 codecs attribute of MediaComponent data type 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 the medType attribute of MediaComponent data type is present THEN
	CASE medType value OF
	“audio”: 5QI := 1;
	“video”: 5QI := 2;
	“application”: 5QI := 1 OR 2;
	OTHERWISE: 5QI := 9; /*e.g. for TCP-based generic traffic */
	END;
	ENDIF;
	ENDIF;
	(NOTE 1, 2, 3, 7 and 12)

Authorized QoS Parameter	Derivation from service information (NOTE 4)
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 29.514 [10].	
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: 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 mpsId and resPrio attributes, for deriving the 5QI.	
NOTE 12: The PCF may authorize a non-standardized 5QI with explicitly signalled QoS characteristics as defined in subclause 4.2.6.6.3 of 3GPP TS 29.512 [9] or may assign QoS characteristics (e.g. Priority Level, Averaging Window, and Maximum Data Burst Volume) to be used instead of the default QoS characteristics associated with a standardised 5QI value as shown in table 5.7.4-1 in 3GPP TS 23.501 [2].	

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 medComponents attribute).

If the PCF provides a QoS information associated to a PCC rule it may apply the rules in table 7.3.3-2 to combine the Authorized QoS per service data flow or bidirectional combination of service data flows (as derived according to table 7.3.3-1) 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 7.3.3-2 to combine the Authorized QoS per service data flow or bidirectional combination of service data flows (as derived according to table 7.3.3-1) for all service data flows allowed to be transported within the PDU session. It is recommended that the rules in table 7.3.3-2 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 7.3.3-2.

Table 7.3.3-2: 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 7.3.3-1).
Guaranteed Authorized Data Rate DL and UL	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 7.3.3-1). (NOTE 3)
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	IF an operator special policy exists THEN
	ARP:= as defined by operator specific algorithm;
	ELSE IF mpsId attribute 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)

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 mpsId and resPrio attributes, 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.	

7.4 QoS parameter mapping Functions at SMF

Table 7.4.1: Rules for derivation of the Authorized QoS Parameters per QoS flow from the Authorized QoS Parameters in SMF

Authorized QoS Parameter per QoS flow (NOTE 1)	Derivation from Authorized QoS Parameters
Maximum Authorized Bandwidth DL and UL per QoS flow	Maximum Authorized Bandwidth DL/UL per QoS flow = Sum of Maximum Authorized Data Rate DL/UL for all PCC rules bound to that Qos flow
Guaranteed Authorized Data Rate DL and UL per QoS flow	Guaranteed Authorized Data Rate DL/UL per QoS flow = Sum of Guaranteed Authorized Data Rate DL/UL for all PCC rules bound to that QoS flow
Session-AMBR DL and UL	For all non-GBR QoS flows, Session-AMBR DL/UL is applied.
5QI	5QI from PCC rules having the same value combination of 5QI/ARP/QNC/PL/AW/MDBV is used.
ARP	ARP from PCC rules having the same value combination of 5QI/ARP/QNC/PL/AW/MDBV is used.
QNC	QNC from PCC rules having the same value combination of 5QI/ARP/QNC/PL/AW/MDBV is used.
Priority Level (PL)	PL from PCC rules having the same value combination of 5QI/ARP/QNC/PL/AW/MDBV is used.
Averaging Window (AW)	AW from PCC rules having the same value combination of 5QI/ARP/QNC/PL/AW/MDBV is used. Applicable for GBR QoS flow.
Maximum Data Burst Volume (MDBV)	MDBV from PCC rules having the same value combination of 5QI/ARP/QNC/PL/AW/MDBV is used. Applicable for GBR QoS flow of delay critical type.
RQI	RQI from PCC rules is used per service data flow. Applicable for non-GBR QoS flows.
Maximum Packet Loss Rate DL and UL per QoS flow	Minimum maximum packet loss rate DL/UL among all PCC rules bound to that QoS flow. Applicable for GBR QoS flows.
NOTE: For unstructured PDU session type, only default 5QI and ARP of the QoS Flow associated with the default QoS rule, and Session-AMBR are applicable.	

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.

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.

The AMF may utilize the Nnrf_NFDiscovery service of the NRF to discover the candidate PCF instance(s). In addition, PCF information may also be locally configured on AMF. The AMF selects a PCF instance, or two when roaming, based on the available PCF instances (obtained from the NRF or locally configured in the AMF), depending on operator's policies.

In the non-roaming case, the AMF selects a PCF instance for AM policy association and selects the same PCF instance for UE policy association. In the roaming case, the AMF selects a V-PCF instance for AM policy association and selects the same V-PCF instance for UE policy association.

The following factors may be considered at PCF discovery and selection by the AMF:

- SUPI; the AMF selects a PCF instance based on the SUPI range the UE's SUPI belongs to or based on the results of a discovery procedure with NRF using the UE's SUPI as input for PCF discovery.
- S-NSSAIs.

In the following scenarios, information about the PCF that has been selected by the AMF (e.g. the selected PCF instance Id) can be forwarded to another NF and used instead of performing PCF selection as described above (discovery may still be needed depending on what level of information is sent by the AMF, e.g. the address of the PCF instance may not be present):

- During AMF relocation, the target AMF may receive a resource URI of AM Policy association and/or a resource URI of UE Policy association from the source AMF to enable the target AMF to reuse the same PCF instance (i.e. reuse the resource of the AM Policy association and/or UE Policy association), and the target AMF may decide based on operator policy either to use the same PCF instance or select a new PCF instance.
- In the roaming case, the AMF may, based on operator policies, e.g. roaming agreement, select the H-PCF in addition to the V-PCF for a UE by performing the PCF discovery and selection as described above. The AMF sends the selected H-PCF instance Id to the V-PCF during the UE Policy association establishment procedure.

8.3 PCF discovery and selection by the SMF

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

The SMF may utilize the Nnrf_NFDiscovery service of the Network Repository Function to discover the candidate PCF instance(s). In addition, PCF information may also be locally configured on SMF. The SMF selects a PCF instance based on the available PCF instances (obtained from the NRF or locally configured in the SMF). The following factors may be considered during the PCF selection.

- Local operator policies.
- Selected Data Network Name (DNN).
- S-NSSAI of the PDU session.
- SUPI; the SMF selects a PCF instance based on the SUPI range the UE's SUPI belongs to or based on the results of a discovery procedure with NRF using the UE's SUPI as input for PCF discovery.

The AMF may, based on operator policies, forward the selected PCF instance to the SMF during the PDU Session Establishment procedure to enable the usage of the same PCF instance for the AMF and the SMF. The SMF may decide based on operator policy either to use the same PCF instance or select a new PCF instance. If the same PCF instance is selected by the SMF, the PCF discovery and selection procedure described above is not performed.

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) , S-NSSAI, the IPv4 address domain (if applicable) and the selected PCF address for a certain PDU session. This information is stored internally in the BSF.

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-NSSAI, IPv4 address domain) (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.

   It shall support the functionality of a proxy agent and a redirect agent as defined in IETF RFC 6733 [29]. The mode in which it operates (i.e. proxy or redirect) shall be based on operator's requirements.

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.

This subclause also concerns the BSF procedures over Rx reference point. Subclause 8.5.5 is for the BSF implemented as a Diameter Proxy Agent, and subclause 8.5.6 is for the BSF implemented as a Diameter Redirect Agent.

8.5.2 Binding information Creation

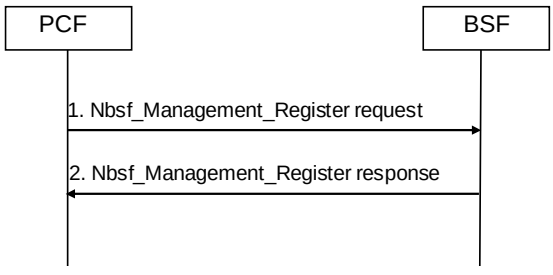


Figure 8.5.2-1: Binding information Creation procedure

1. When an IP address is allocated for the IP 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 Resource URI of the resource "PCF Session Bindings" to store the binding information in the BSF. The binding information provided in the HTTP POST 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.

8.5.3 Binding information Deletion

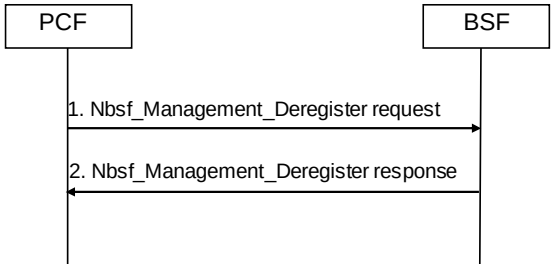


Figure 8.5.3-1: Binding information Deletion procedure

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 Resource URI of the resource "Individual PCF Session Binding" 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 stored binding information.

8.5.4 Binding information Retrieval

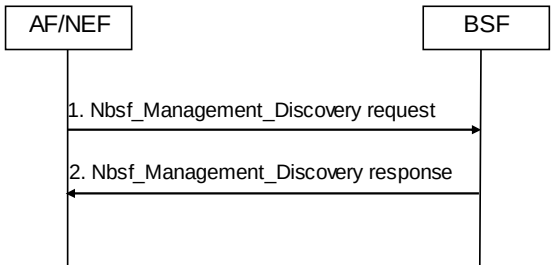


Figure 8.5.4-1: Binding information Retrieval procedure

1. AF/NEF invokes the Nbsf_Management_Discovery service operation by sending the HTTP GET request with Resource URI of the resource "PCF Session Bindings" to the BSF to obtain the address information of the selected PCF for a certain PDU session. The URI query parameters in the HTTP GET request are specified in subclause 4.2.4.2 of TS 29.521 [22].

2. The BSF sends an HTTP "200 OK" response to the AF/NEF with the address information of the selected PCF (FQDN and/or IP address(es) and port information of the selected PCF, or if the PCF supports the Rx interface the Diameter host and realm for the selected PCF).

8.5.5 Proxy BSF

8.5.5.1 General

When the BSF receives a request from an AF, it shall check whether it already has selected a PCF for the Rx session; if it does have a PCF already selected for the Rx session, it shall proxy the request to the corresponding PCF. If the BSF does not have a PCF already selected, it shall select a PCF to handle the Rx session and then proxy the request to the selected PCF.

8.5.5.2 Rx Session Establishment

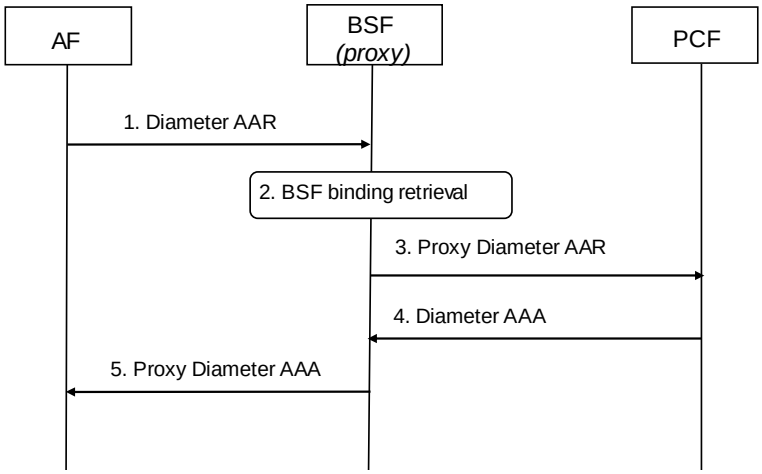


Figure 8.5.5.2-1: Rx Session Establishment procedure using BSF (proxy)

1. A Diameter AAR indicating establishment of an AF session is sent by the AF and received by a BSF (proxy).
2. The BSF (proxy) shall select a PCF from the binding for the AF.
3. The BSF (proxy) proxies the Diameter AAR to the target PCF. The proxied Diameter AAR maintains the same Session-Id AVP value.
4. The PCF returns a Diameter AAA to the BSF (proxy).
5. BSF (proxy) proxies the Diameter AAA to the AF. The proxied Diameter AAA maintains the same Session-Id AVP value.

8.5.5.3 Rx Session Modification

8.5.5.3.1 AF-initiated

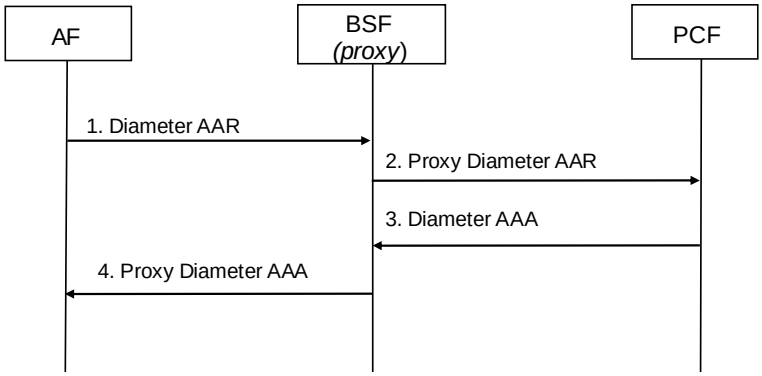


Figure 8.5.5.3.1-1: AF-initiated Rx Session Modification procedure using BSF (proxy)

1. A subsequent Diameter AAR indicating modification of an existing Rx session is sent by the AF and received by the BSF (proxy).
2. The BSF (proxy) proxies the Diameter AAR to the target PCF.
3. PCF returns a Diameter AAA to the BSF (proxy).
4. BSF (proxy) proxies the Diameter AAA to the AF.

8.5.5.3.2 PCF-initiated

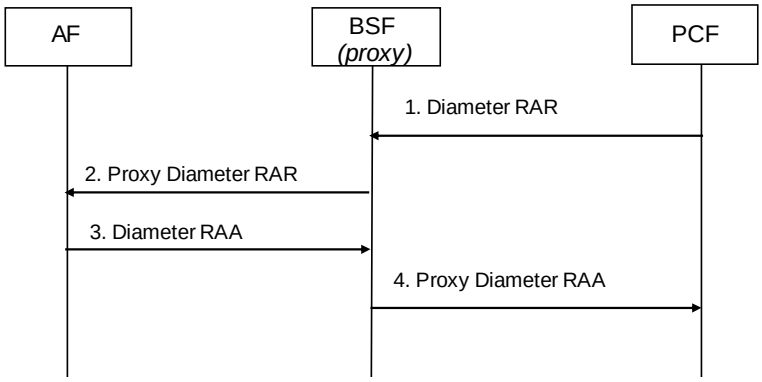


Figure 8.5.5.3.2-1: PCF-initiated Rx Session Modification procedure using BSF (proxy)

1. A PCF-initiated Diameter RAR indicating an Rx specific action is sent to the AF and received by the BSF (proxy).
2. The BSF (proxy) proxies the Diameter RAR to the AF. The proxied Diameter Request maintains the same Session-Id AVP value.
3. AF returns a Diameter RAA to the BSF (proxy).
4. BSF (proxy) proxies the Diameter RAA to the PCF.

8.5.5.4 Rx Session Termination

8.5.5.4.1 AF-initiated

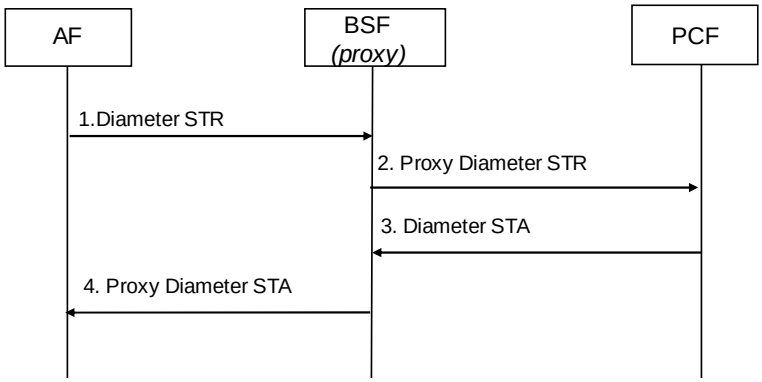


Figure 8.5.5.4.1-1: AF-initiated Rx Session Termination procedure using BSF (proxy)

1. A Diameter STR indicating termination of an Rx session is sent by the AF to the BSF (proxy). The message uses the same Session-Id AVP value of the active Rx session established between the AF and PCF.
2. The BSF (proxy) proxies the Diameter STR to the target PCF. The proxied Diameter Request maintains the same Session-Id AVP value.
3. PCF sends BSF (proxy) a Diameter STA to acknowledge termination of the session.
4. The BSF marks the Rx session terminated and proxies the Diameter STA to the AF. The proxied Diameter Answer maintains the same Session-Id AVP value.

8.5.5.4.2 PCF-initiated

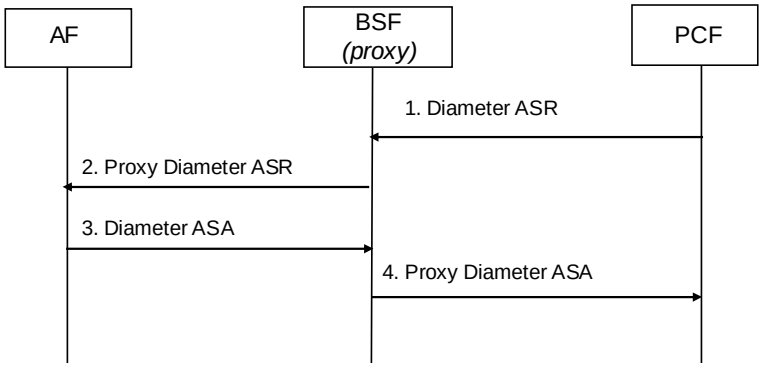


Figure 8.5.5.4.2-1: PCF-initiated Rx Session Termination procedure using BSF (proxy)

1. A PCF-initiated Diameter ASR requesting the termination of an Rx session is sent to the AF and received by the BSF (proxy).
2. The BSF (proxy) proxies the Diameter ASR to the AF. The proxied Diameter ASR maintains the same Session-Id AVP value.
3. AF returns a Diameter ASA to the BSF (proxy).
4. BSF (proxy) proxies the Diameter ASA to the PCF.

8.5.6 Redirect BSF

8.5.6.1 General

A BSF implemented as a Diameter redirect agent shall redirect the received Diameter request message by carrying out the procedures defined in subclause 6.1.7 of IETF RFC 6733 [29]. The Client shall use the value within the Redirect-Host AVP of the redirect response in order to obtain the PCF identity. The BSF may provide the Redirect-Host-Usage AVP in the redirect response to provide a hint to the Client about how the cached route table entry created from the Redirect-Host AVP is to be used as described in subclause 6.13 of IETF RFC 6733 [29].

The BSF may also provide the Redirect-Max-Cache-Time AVP in the redirect response to indicate to the Client the lifetime of the cached route table entry created from the Redirect-Host and Redirect-Host-Usage AVP values as described in subclause 6.14 of IETF RFC 6733 [29].

The BSF clients shall use cached route table entry created from the Redirect-Host, Redirect-Host-Usage and Redirect-Max-Cache-Time AVPs to determine whether BSF interaction is required.

The AF shall contact the BSF on Rx session establishment to retrieve the PCF address. The BSF (redirect) does not need to maintain Diameter sessions and Diameter Base redirect procedures are applicable. Therefore, an AF should not send an Rx session modification or termination request to the BSF.

8.5.6.2 Rx Session Establishment

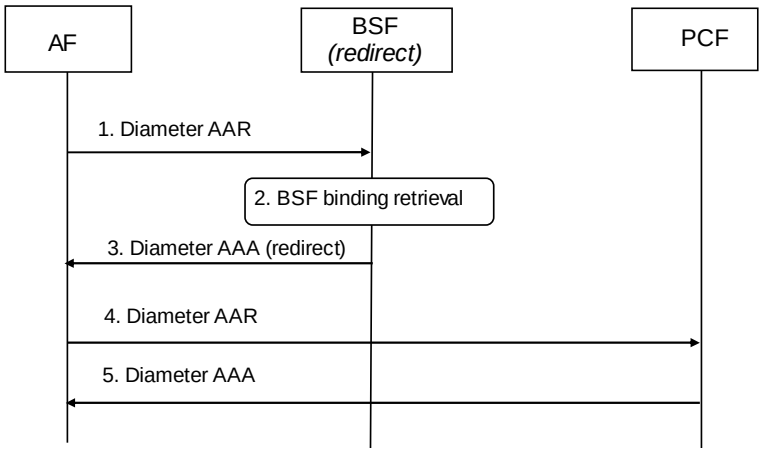


Figure 8.5.6.2-1: Rx Session Establishment procedure using BSF (redirect)

1. A Diameter AAR indicating establishment of a new Rx Diameter session with the PCF is sent by the AF and received by a BSF (redirect).
2. The BSF shall select the PCF from the binding for the AF.
3. The BSF sends a Diameter AAA indicating redirection as defined in IETF RFC 6733 [29]. The target PCF identity is included in the Redirect-Host AVP.
4. The AF re-sends the Diameter AAR of step 1 to the target PCF.
5. PCF returns a Diameter AAA to the AF.

Annex A (informative): DRA and BSF coexistence

During the network migration, DRA and BSF may coexist in operator's network. When the AF sends Rx request to the DRA, the DRA can utilize the Nbsf_Management_Discovery service operation to obtain the relevant PCF address as depicted in figure A-1. The DRA only applies this operation if it has no stored binding information derived from an ongoing Gx session for that subscriber.

NOTE 1: For a UE in the EPC there is a Gx session and the DRA stores the binding information. For a UE in the 5GC the Npcf_SmPolicyControl service is used and the BSF stores the binding information.

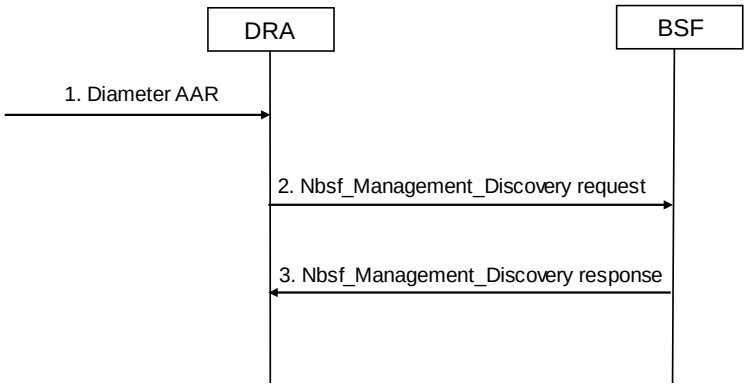


Figure A-1: PCF discovery by DRA via BSF

1. The AF sends a Diameter AAR to the DRA to establish a new Rx diameter session.
2. When receiving the request in step 1, if the DRA has no stored binding information derived from an ongoing Gx session for the subscriber, the DRA invokes the Nbsf_Management_Discovery service operation to the BSF to obtain the selected PCF ID for a certain PDU session.
3. The BSF replies to the DRA with the PCF ID.

NOTE 2: If the DRA has no stored binding information derived from an ongoing Gx session for a subscriber, the DRA needs to request new binding information for each Rx session establishment because the information in the BSF could have changed compared to any previous binding information the DRA requested.

Annex B (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
2018-09	CT#81	CP-182015	0001	2	F	AF traffic routing procedure	15.1.0
2018-09	CT#81	CP-182015	0002	3	F	BSF procedures over Rx	15.1.0
2018-09	CT#81	CP-182015	0003	2	F	Clarification on PCF discovery and selection	15.1.0
2018-09	CT#81	CP-182015	0004	4	F	QoS mapping at AF and PCF	15.1.0
2018-09	CT#81	CP-182015	0005	2	F	remove EN of PCC rule authorization for non-IP cases	15.1.0
2018-09	CT#81	CP-182015	0006	2	F	slice info considered in session binding and PCF selection	15.1.0
2018-09	CT#81	CP-182015	0007	1	B	Solution to IPv4 overlapping	15.1.0
2018-09	CT#81	CP-182015	0008		F	Remove the editor's note for Ethernet	15.1.0
2018-09	CT#81	CP-182015	0009		F	5QI derivation in PCF QoS mapping	15.1.0
2018-09	CT#81	CP-182015	0010		B	SMF QoS mapping	15.1.0
2018-09	CT#81	CP-182035	0011	2	F	Resolving EN for PFD Management	15.1.0
2018-12	CT#82	CP-183205	0012	1	F	Architecture of interworking with AFs supporting Rx interface	15.2.0
2018-12	CT#82	CP-183205	0014	5	F	Correction to AM Policy association procedure	15.2.0
2018-12	CT#82	CP-183205	0015		F	Correction to the PFD retrieval	15.2.0
2018-12	CT#82	CP-183205	0016	1	F	Correction to the PCF discovery and selection	15.2.0
2018-12	CT#82	CP-183205	0017	2	F	Correction to the QoS flow binding	15.2.0
2018-12	CT#82	CP-183205	0018	1	F	PCF Derivation of QoS Parameters	15.2.0
2018-12	CT#82	CP-183205	0019	1	F	Consolidation of Initial Spending Limit Report request	15.2.0
2018-12	CT#82	CP-183205	0020	1	F	Consolidation of Intermediate Spending Limit Report request	15.2.0
2018-12	CT#82	CP-183205	0021	1	F	Consolidation of Spending Limit Report notification	15.2.0
2018-12	CT#82	CP-183205	0022	1	F	Introduction of the subclause "subscription termination request"	15.2.0
2018-12	CT#82	CP-183205	0025	4	F	UE Policy Association procedures	15.2.0
2018-12	CT#82	CP-183205	0026	1	F	updates in clause 5.2 to detail UDR interaction	15.2.0
2018-12	CT#82	CP-183205	0027	3	F	corrections to AF traffic routing procedures	15.2.0
2018-12	CT#82	CP-183205	0028	1	F	BSF only stores binding info locally	15.2.0
2018-12	CT#82	CP-183205	0029	3	F	Correction on BSF and DRA coexistence scenario	15.2.0
2018-12	CT#82	CP-183108	0031	2	F	Correction of SM Policy Establishment and Termination Flows to Include Calls to the BSF	15.2.0
2018-12	CT#82	CP-183205	0032	1	F	Correction of SM Policy Modification Flows to Include Calls to the BSF	15.2.0
2018-12	CT#82	CP-183205	0033		F	Using resource name instead of resoure URI in BSF procedure	15.2.0

2018-12	CT#82	CP-183205	0034	1	F	corrections on PFD management procedure	15.2.0
2018-12	CT#82	CP-183205	0035		F	corrections on NWDA procedure	15.2.0
2018-12	CT#82	CP-183205	0036		F	http details in BDT procedure	15.2.0
2018-12	CT#82	CP-183205	0037		F	Correction to architecture figures	15.2.0
2019-03	CT#83	CP-190115	0039		F	GPSI in AF session establishment	15.3.0
2019-03	CT#83	CP-190134	0040	1	F	SEPPs in roaming architecture	15.3.0
2019-03	CT#83	CP-190115	0041	3	F	Correct PCF-initiated AM policy association termination	15.3.0
2019-03	CT#83	CP-190115	0044		F	Invocation of Nudr_DataRepository_Update service operation for BDT	15.3.0
2019-03	CT#83	CP-190115	0045	1	F	PFD management in the SMF	15.3.0
2019-03	CT#83	CP-190115	0046		F	Invocations of the Nbsf_Management service operations	15.3.0
2019-03	CT#83	CP-190115	0047		F	Corrections on UE policy association procedure	15.3.0
2019-03	CT#83	CP-190115	0051		F	Corrections on AFTrafficRouting procedure	15.3.0
2019-06	CT#84	CP-191075	0052	1	F	Correction on PCF discovery	15.4.0
2019-06	CT#84	CP-191075	0053	1	F	Correction to the QoS flow binding	15.4.0
2019-06	CT#84	CP-191075	0056	2	F	Corrections to AM policy control procedure and UE policy control procedure	15.4.0
2019-06	CT#84	CP-191075	0057	1	F	multiple MANAGE UE POLICY COMMAND messages sent by H-PCF	15.4.0
2019-06	CT#84	CP-191075	0059		F	Remove NSI ID	15.4.0
2019-06	CT#84	CP-191075	0064	1	F	Correction to AM Policy Association Establishment Flow	15.4.0
2019-09	CT#85	CP-192143	0071		F	Session binding for IPv6 addresses	15.5.0
2019-09	CT#85	CP-192143	0075	1	F	Alignment of notification URI name and HTTP reponse code	15.5.0
2019-09	CT#85	CP-192143	0077	1	F	Corrections on NWDA procedures	15.5.0
2019-09	CT#85	CP-192143	0079		F	Corrections on PFD procedure and SM policy procedure	15.5.0
2019-12	CT#86	CP-193185	0084	1	F	Correct AMF behaviour during PCF-initiated AM Policy Association Termination procedure	15.6.0
2019-12	CT#86	CP-193185	0087	1	F	Correction to PCF selection	15.6.0
2019-12	CT#86	CP-193185	0089	1	F	Correction to QoS Mapping	15.6.0

History

Document history		
V15.0.0	June 2018	Publication
V15.1.0	October 2018	Publication
V15.2.0	April 2019	Publication
V15.3.0	April 2019	Publication
V15.4.0	July 2019	Publication
V15.5.0	October 2019	Publication
V15.6.0	January 2020	Publication