ETSI TS 129 513 V17.10.0 (2023-04)

5G;
5G System;
Policy and Charging Control signalling flows and QoS parameter mapping;
Stage 3
(3GPP TS 29.513 version 17.10.0 Release 17)

Reference
RTS/TSGC-0329513vha0

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 - APE 7112B
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° w061004871

Intellectual Property Rights

Essential patents

IPRs essential or potentially essential to normative deliverables may have been declared to ETSI. The declarations pertaining to these essential IPRs, if any, are 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 Directives including the ETSI IPR Policy, no investigation regarding the essentiality of IPRs, 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.

DECT™, **PLUGTESTS™**, **UMTS™** and the ETSI logo are trademarks of ETSI registered for the benefit of its Members. **3GPP™** and **LTE™** are trademarks of ETSI registered for the benefit of its Members and of the 3GPP Organizational Partners. **oneM2M™** logo is a trademark of ETSI registered for the benefit of its Members and of the oneM2M Partners. **GSM**® and the GSM logo are trademarks registered and owned by the GSM Association.

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 https://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, Nnwdaf and Nmbsmf 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].

The stage 2 definition and procedures of PCC for 5G multicast/broadcast services are contained in 3GPP TS 23.247 [54].

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], 3GPP TS 29.554 [26] and 3GPP TS 29.537 [55].

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,| SMF and MB-SMF.

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

The present specification also describes the PCF addressing.

The present specification also describes the Race condition handling.

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] Void

[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".

[34] 3GPP TS 29.122: "T8 reference point for northbound Application Programming Interfaces (APIs)".Non-Access-Stratum (NAS) protocol for 5G System (5GS); Stage 3".

[35] 3GPP TS 24.292: "IP Multimedia (IM) Core Network (CN) subsystem Centralized Services (ICS); Stage 3".

[36] IETF RFC 3556: "Session Description Protocol (SDP) Bandwidth Modifiers for RTP Control Protocol (RTCP) Bandwidth".

[37] IETF RFC 3890: "A Transport Independent Bandwidth Modifier for the Session Description Protocol (SDP)".

[38] IETF RFC 5761: "Multiplexing RTP Data and Control Packets on a Single Port".

[39] IETF RFC 4145: "TCP-Based Media Transport in the Session Description Protocol (SDP)".

[40] IETF RFC 4975: "The Message Session Relay Protocol (MSRP)".

[41] 3GPP TS 24.229: " IP multimedia call control protocol based on Session Initiation Protocol (SIP) and Session Description Protocol (SDP); Stage 3".

[42] IETF RFC 4412: "Communications Resource Priority for the Session Initiation Protocol (SIP)".

[43] IETF RFC 3264: "An Offer/Answer model with the Session Description Protocol (SDP)".

[44] 3GPP TS 23.216: "Single Radio Voice Call Continuity (SRVCC); Stage 2".

[45] 3GPP TS 23.380: "IMS Restoration Procedures".

[46] 3GPP TS 23.221: "Architectural requirements".

[47] 3GPP TS 29.505: "5G System; Usage of the Unified Data Repository Service for Subscription Data; Stage 3".

[48] 3GPP TS 29.552: "5G System; Network Data Analytics signalling follows; Stage 3".

[49] 3GPP TS 29.523: "5G System; Policy Control Event Exposure Service; Stage 3".

[50] 3GPP TS 29.534: "5G System; Access and Mobility Policy Authorization Service; Stage 3".

[51] 3GPP TS 29.510: "5G System; Network function repository services; Stage 3".

[52] 3GPP TS 29.502: "5G System; Session Management Services; Stage 3".

[53] 3GPP TS 29.212: "Policy and Charging Control (PCC); Reference points".

[54] 3GPP TS 23.247: "Architectural enhancements for 5G multicast-broadcast services; Stage 2".

[55] 3GPP TS 29.537: "5G System; Multicast/Broadcast Policy Control Services; Stage 3".

[56] 3GPP TS 29.564: "5G System; User Plane Function Services; Stage 3".

[57] 3GPP TS 23.548: "5G System Enhancements for Edge Computing; Stage 2".

[58] 3GPP TS 29.532: "5G System; 5G Multicast-Broadcast Session Management Services; Stage 3".

3 Definitions, symbols and abbreviations

3.1 Definitions

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

For the purposes of the present document, the following terms and definitions given in 3GPP TS 23.501 [2], clause 3.1 apply:

Onboarding Standalone Non-Public Network

3.2 Abbreviations

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

5GC	5G Core Network
5G DDNMF	5G Direct Discovery Name Management Function
5QI	5G QoS Identifier

5G VN	5G Virtual Network
AF	Application Function
AMBR	Aggregate Maximum Bit Rate
AMF	Access and Mobility Management Function
ARP	Allocation and Retention Priority
AW	Average Window
BDT	Background Data Transfer
BSF	Binding Support Function
CHEM	Coverage and Handoff Enhancements using Multimedia error robustness feature
CHF	Charging Function
DSCP	Differentiated Services Code Point
DN-AAA	Data Network Authentication, Authorization and Accounting
DTS	Data Transport Service
LBO	Local Breakout
MBR	Maximum Bitrate
MBS	Multicast/Broadcast Service
MBSF	Multicast/Broadcast Service Function
MB-SMF	Multicast/Broadcast Session Management Function
MCS	Mission Critical Service
MPD	Media Presentation Description
MPS	Multimedia Priority Service
NEF	Network Exposure Function
NID	Network Identifier
NPLI	Network Provided Location Information
NRF	Network Repository Function
NSSAI	Network Slice Selection Assistance Information
NWDAF	Network Data Analytics Function
ON-SNPN	Onboarding Standalone Non-Public Network
PCC	Policy and Charging Control
PCF	Policy Control Function
PDB	Packet Delay Budget
PER	Packet Error Rate
PDUID	ProSe Discovery UE ID
PFD	Packet Flow Description
PFDF	Packet Flow Description Function
PMIC	Port Management Information Container
PL	Priority Level
ProSe	Proximity Services
ProSeP	5G ProSe Policy
PSA	PDU Session Anchor
PSAP	Public Safety Access Point
P-CSCF	Proxy Call Session Control Function
QNC	QoS Notification Control
QoS	Quality of Service
SCP	Service Communication Proxy
SDP	Session Description Protocol
SEPP	Security Edge Protection Proxy
SMF	Session Management Function
S-NSSAI	Single Network Slice Selection Assistance Information
SNPN	Stand-alone Non-Public Network
SPI	Security Parameter Index
TSC	Time Sensitive Communication
TSCAI	Time Sensitive Communication Assistance Information
TSN	Time Sensitive Networking
UDR	Unified Data Repository
UL CL	UpLink CLassifier
UMIC	User plane node Management Information Container
UPF	User Plane Function
UPSI	UE policy section identifier
URSP	UE Route Selection Policy
V2X	Vehicle-to-Everything
V2XP	Vehicle-to-Everything Policy

4 Reference architecture

The policy framework functionality in 5G is comprised of the functions of the Policy Control Function (PCF), the policy and charging enforcement functionality supported by the 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 Charging Function (CHF), the Unified Data Repository (UDR), the Time Sensitive Communication and Time Synchronization Function (TSCTSF), the Application Function (AF) and the 5G Direct Discovery Name Management Function (5G DDNMF).

The policy framework functionality for multicast-broadcast services in 5G is comprised of the functions of the Policy Control Function (PCF), the Multicast/Broadcast Service Function (MBSF), the Multicast-Broadcast Session Management Function (MB-SMF), the Network Exposure Function (NEF), 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.

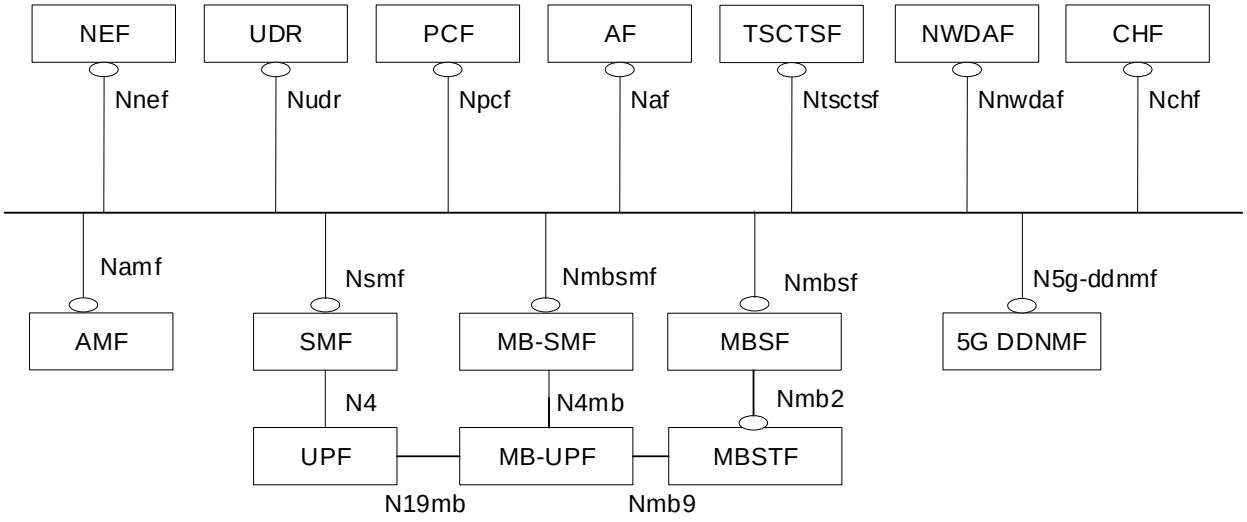


Figure 4.1-1a: Overall non-roaming 5G Policy framework architecture (service based representation)

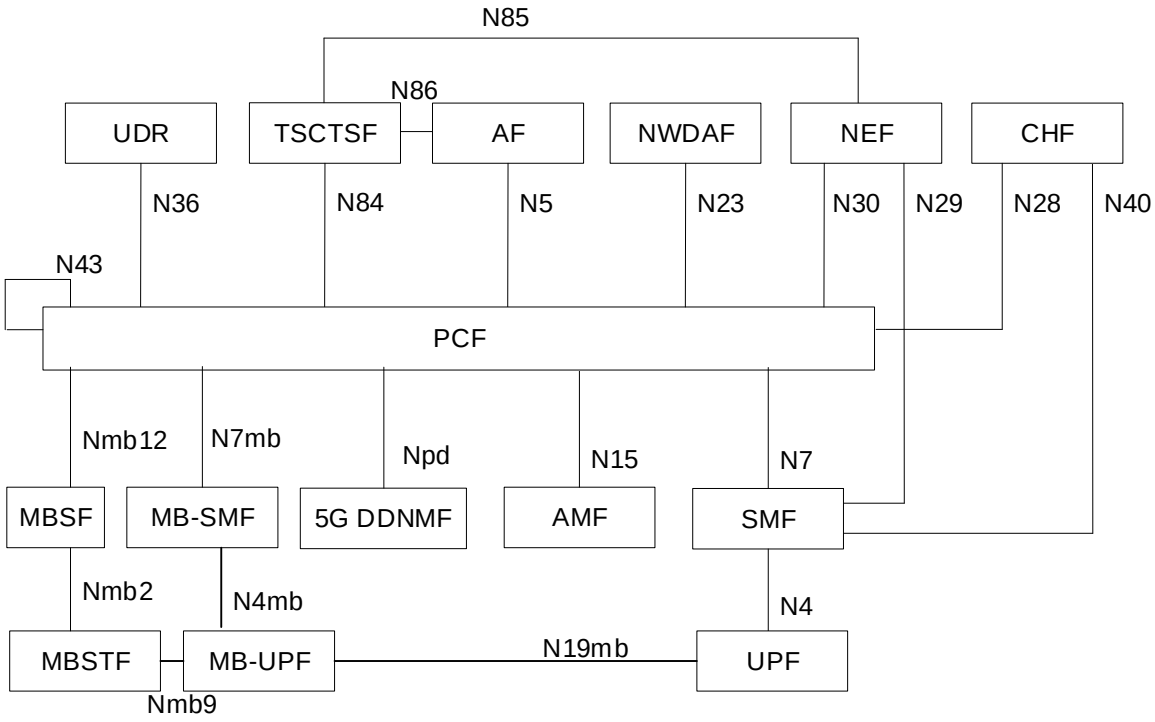


Figure 4.1-1b: Overall non-roaming 5G Policy framework architecture (reference point representation)

NOTE 1: The N4, N4mb, Nmb2, Nmb9 and N19mb interfaces are not part of the Policy Framework architecture but shown in the figures for completeness.

NOTE 2: If an SCP is deployed it can be used for indirect communication between NFs and NF services as described in Annex E of 3GPP TS 23.501 [2].

NOTE 3: MB-SMF, MBSTF, MB-UPF and MBSF apply only when the MBS PCC Architecture as described in 3GPP TS 23.247 [54] is deployed. In this case only the entities shown in that architecture are applicable.

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].

The PCF providing session management policy control for a UE (i.e. PCF for the PDU Session) and the PCF providing non-session management policy control for that UE (i.e. PCF for the UE) may be different PCF instances and the communication between the PCF for the UE and the PCF for the PDU Session is performed over the N43 reference point.

NOTE 3: The roaming scenarios for SNPNs are not supported in this Release.

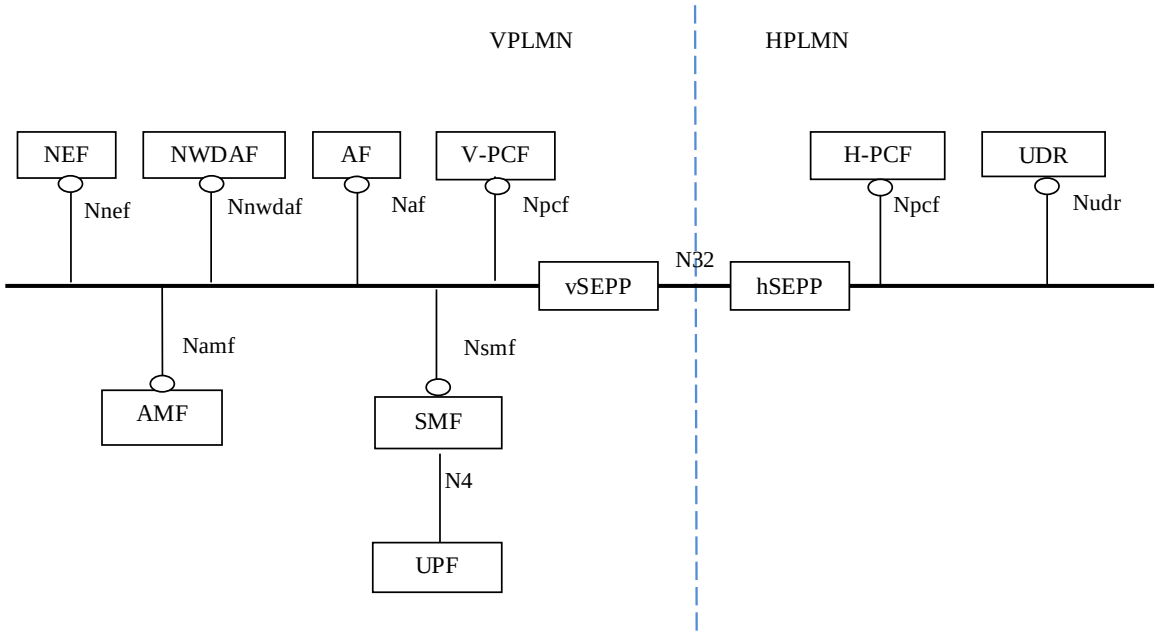


Figure 4.1-2a: Overall roaming policy framework architecture - LBO (service based representation)

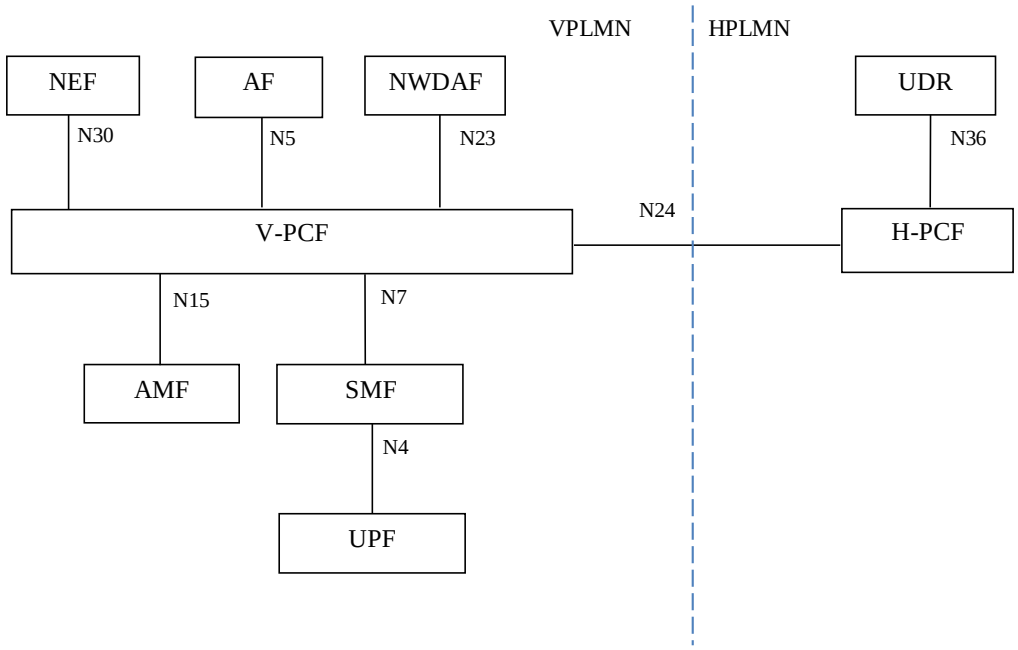


Figure 4.1-2b: Overall roaming policy framework architecture - LBO (reference point representation)

NOTE 4: 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 nor to session management policy data for the UE in the VPLMN 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] clause 5.2.5.

NOTE 5: 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 clause 5.6.7 of 3GPP TS 23.501 [2].

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.

NOTE 8: The Home Routed PDU sessions are not supported for TSC networks in this Release.

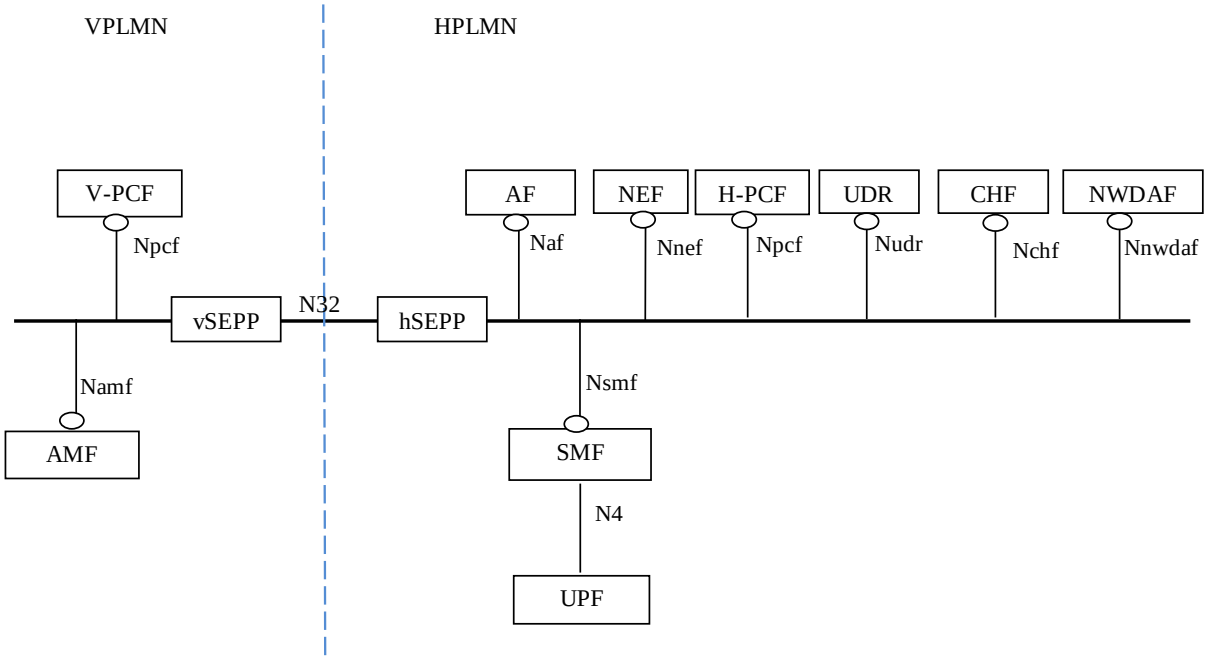


Figure 4.1-3a: Overall roaming policy framework architecture - home routed scenario (service based representation)

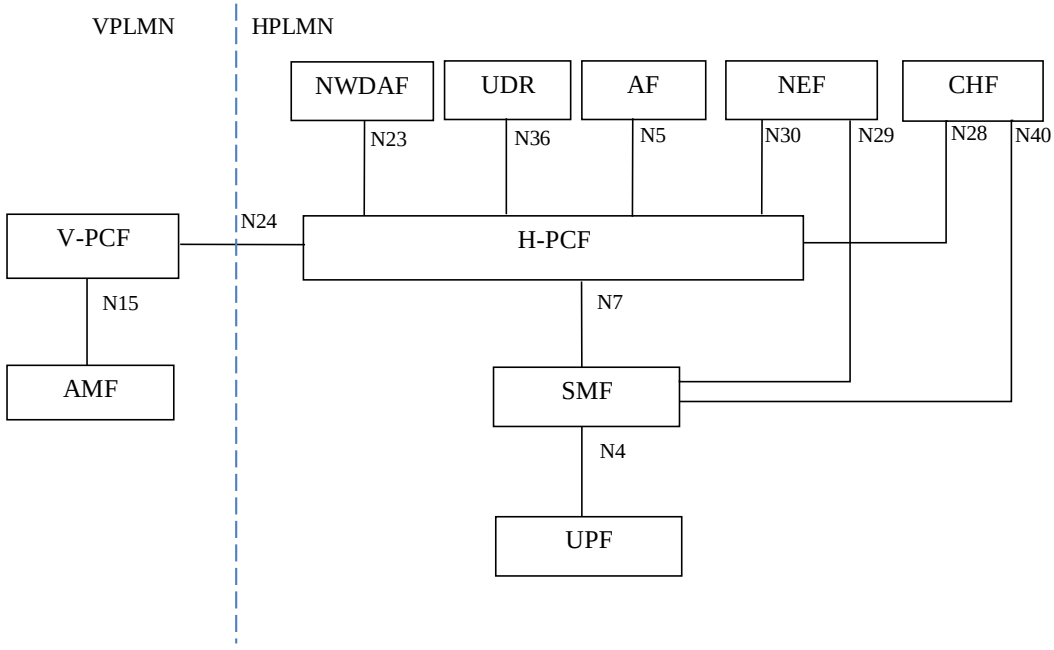


Figure 4.1-3b: Overall roaming policy framework architecture - home routed scenario (reference point representation)

NOTE 9: For the sake of clarity, SEPPs are not depicted in the roaming reference point architecture figures.

NOTE 10: N4 and N32 are not service based interfaces.

NOTE 11: An SCP can be used for indirect communication between NFs and NF services within the VPLMN, within the HPLMN, or in within both VPLMN and HPLMN. For simplicity, the SCP is not shown in the roaming architecture.

NOTE 12: Non-roaming architecture, local breakout roaming architecture and home-routed roaming architecture for interworking between 5GS and EPS are defined in 3GPP TS 23.501 [2]. The signalling flows described in clause 5 apply to this scenario by replacing SMF by the SMF+PGW-C and with the differences applicable to EPC as described in Annex B.3 of 3GPP TS 29.512 [9].

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.

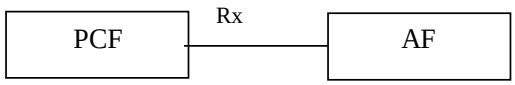


Figure 4.1-4: Interworking between 5G Policy framework and AFs supporting Rx interface

5 Signalling Flows for the Policy Framework

5.0 General

This clause specifies the detailed call flows for the 5G Policy and Charging Control (PCC).

Clauses from 5.1 to 5.6 specify the call flows for PCC with no support of 5G multicast-broadcast services. They include the detailed call flows over Npcf, Nsmf; Namf, Nudr, Nnef; Nchf, Nbsf and Nnwdaf service based interfaces and their relationship with the flow level signalling in the 5G system.

Specific call flows for PCC with support of 5G multicast broadcast services are specified in clause 5.7.

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.

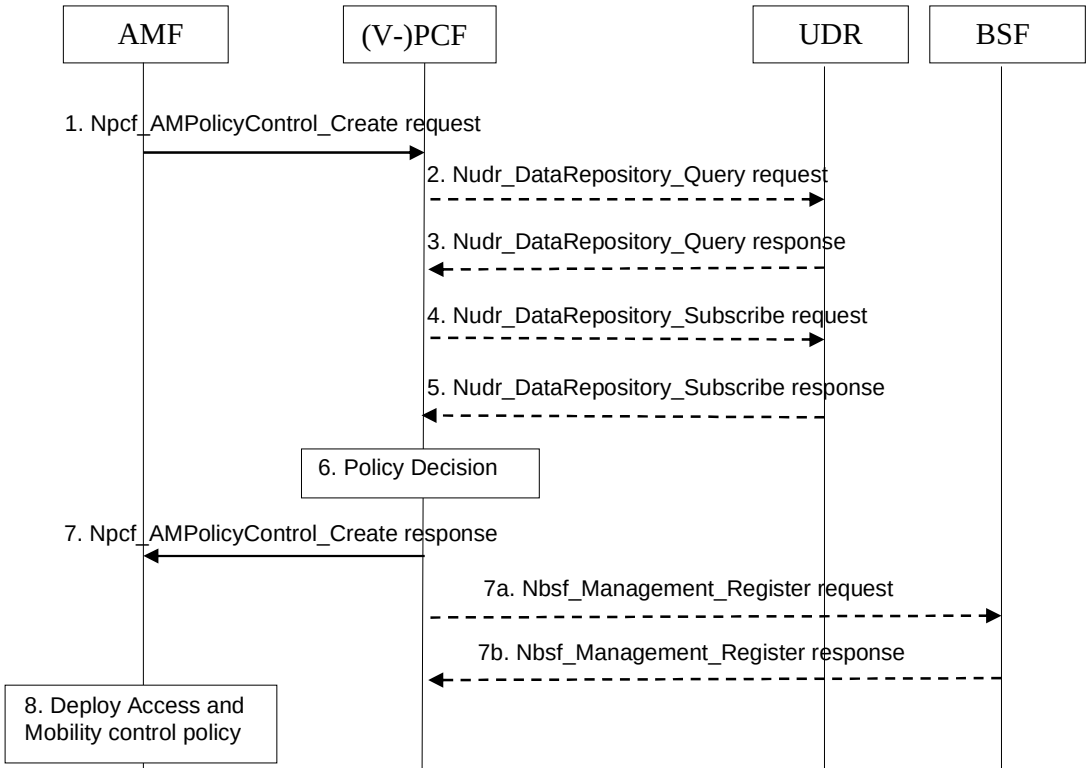


Figure 5.1.1-1: AM Policy Association Establishment procedure

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 clause 8.2 and invokes the Npcf_AMPolicyControl_Create service operation by sending the HTTP POST request to the "AM Policy Associations" resource as defined in clause 4.2.2 and clause 5.3.2.3.1 of 3GPP TS 29.507 [7]. The request operation provides, but is not limited to, the SUPI and the allowed NSSAI if applicable, and if received from the UDM, the Service Area Restrictions, RFSP index, UE-AMBR, a list of UE-Slice-MBR (s), GPSI and a list of Internal Group Identifiers, and may provide the applicable access type(s), the PEI if received in the AMF, the User Location Information if available, the UE Time Zone if available, Serving Network, the applicable RAT type(s), GUAMI of AMF, alternative or backup address(es) or FQDNs of AMF, trace control and configuration parameters information, etc., as defined in clause 4.2.2.1 of 3GPP TS 29.507 [7]. 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 3GPP TS 29.519 [12].

3. The UDR sends an HTTP "200 OK" response to the PCF with the requested subscription data and/or application data in the response message body.

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].

   Additionally, if the PCF and the UDR support dynamically changing AM policies, the PCF may subscribe to the UDR using the Nudr_DataRepository_Subscribe service operation for notifications about AM Influence data changes by sending an HTTP POST request to the "ApplicationDataSubscriptions" 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. If the PCF subscribed to notifications about AM Influence data with the immediate reporting indication set to "true" and matching AM Influence data exists in the UDR, the UDR includes them in the response as specified in 3GPP TS 29.519 [12].

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 clause 4.2.2 of 3GPP TS 29.507 [7], e.g.:

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

   - Policy Control Request Triggers and related policy information.;

   7a. The PCF may register to the BSF as the PCF for the UE (i.e. as the PCF that handles the AM Policy Association of this UE) by sending an HTTP POST request to the "PCF for a UE Bindings" resource of the Nbsf_Management_Register service as described in clause 4.2.2.3 of 3GPP TS 29.521 [22].

   7b. The BSF responds with "201 Created" if the registration of the PCF for the UE was successful.

8. The AMF deploys the Access and Mobility control policy information if received which includes, e.g. 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 when the UE is registered in the 3GPP access.

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. 519 [12]. In this case, the AMF deploys the Access and Mobility control policy information based on the policy retrieved from the UDM if available or the local configuration.

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.

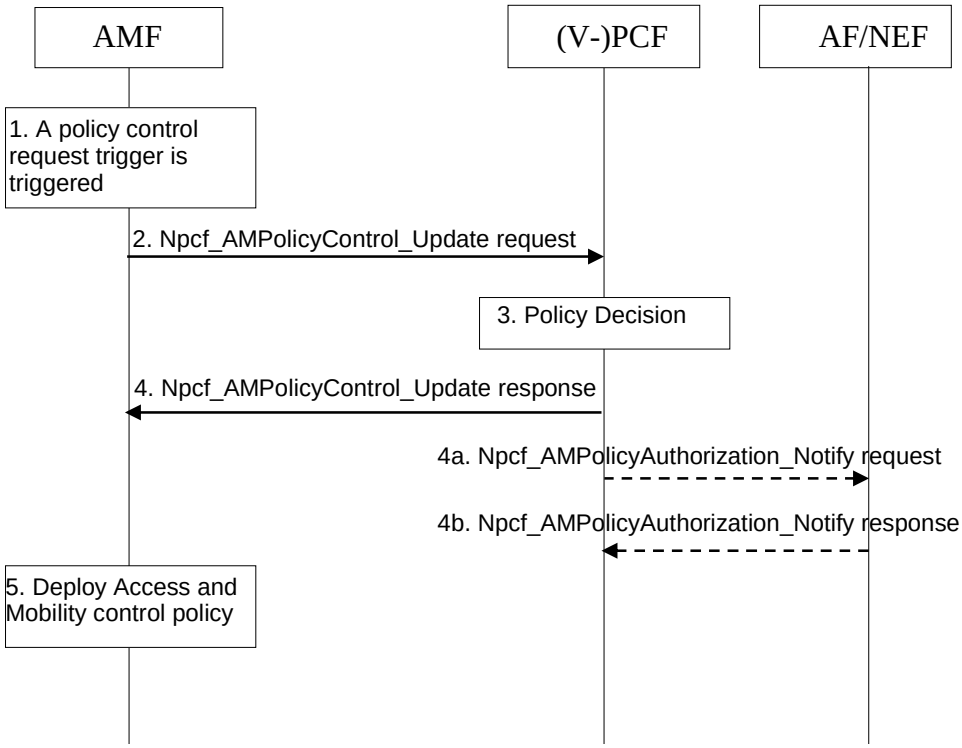


Figure 5.1.2.1.1-1: AMF-initiated AM Policy Association Modification without AMF relocation procedure

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 or other condition is met, e.g. trace control configuration needs to be updated, as defined in clause 4.2.3.1 of 3GPP TS 29.507 [7].

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 as described in clause 4.2.3.3 of 3GPP TS 29.507 [7].

4a. If an AF (either directly or via the NEF) has previously subscribed to events for the AF application AM context (e.g. service area restrictions policy change) as described in 3GPP TS 29.534 [50] clause 4.2.5, the PCF checks if reporting is needed based on the policy decision that was made and may send a respective notification using Npcf_AMPolicyAuthorization_Notify as defined in 3GPP TS 29.534 [50] clause 4.2.7.2 (in addition, a Nnef_AMPolicyAuthorization_Notify request/response may occur between the NEF and the AF if the notification is relayed via the NEF).

4b. The AF (either directly or via the NEF) sends an HTTP "204 No Content" response as defined in 3GPP TS 29.534 [50] clause 4.2.7.2.

5. The AMF deploys the Access and Mobility control policy if received, which includes, e.g. 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 when the UE is registered in the 3GPP access.

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 new AMF.

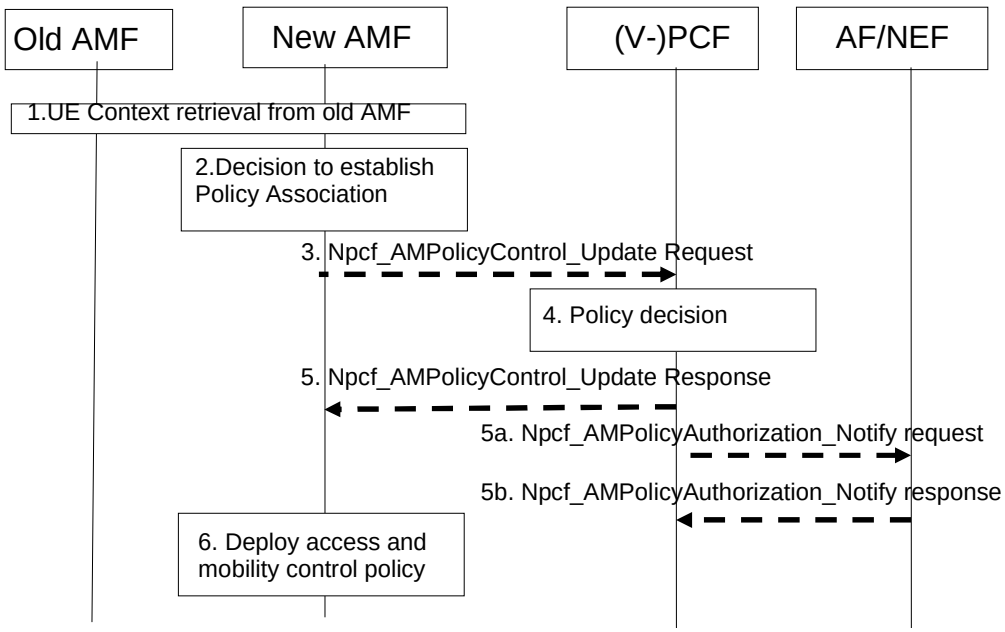


Figure 5.1.2.1.2-1: AMF-initiated AM Policy Association Modification with old PCF during AMF relocation procedure

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 or the same SNPN, the old AMF transfers to the new AMF about the AM Policy Association information including, e.g. 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, and the new alternate or backup IP addresses or FQDN.

4. The (V-)PCF updates the stored information provided by the old AMF with the information provided by the new AMF and makes 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 as described in clause 4.2.3.3 of 3GPP TS 29.507 [7].

5a. If an AF (either directly or via the NEF) has previously subscribed to events for the AF application AM context (e.g. service area restrictions policy change) as described in 3GPP TS 29.534 [50] clause 4.2.5, the PCF checks if reporting is needed based on the policy decision that was made and may send a respective notification using Npcf_AMPolicyAuthorization_Notify as defined in 3GPP TS 29.534 [50] clause 4.2.7.2 (in addition, a Nnef_AMPolicyAuthorization_Notify request/response may occur between the NEF and the AF if the notification is relayed via the NEF).

5b. The AF (either directly or via the NEF) sends an HTTP "204 No Content" response as defined in 3GPP TS 29.534 [50] clause 4.2.7.2.

6. The AMF deploys the Access and Mobility control policy if received, which includes, e.g. 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 when the UE is registered in the 3GPP access.

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.

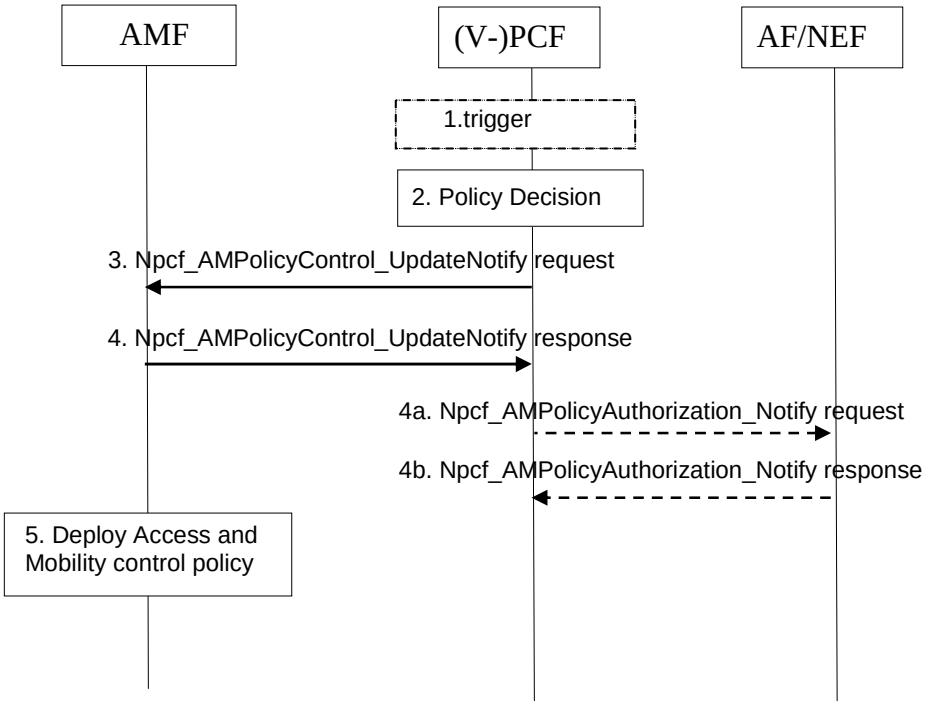


Figure 5.1.2.2-1: PCF-initiated AM Policy Association Modification procedure

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 an AF request to influence AM policies has been received, 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 "{notificationUri}/update" as the callback URI to the AMF that has previously subscribed, as described in clause 4.2.4.2 of 3GPP TS 29.507 [7].

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

4a. If an AF (either directly or via the NEF) has previously subscribed to events for the AF application AM context (e.g. service area restrictions policy change) as described in 3GPP TS 29.534 [50] clause 4.2.5, the PCF checks if reporting is needed based on the policy decision that was made and may send a respective notification using Npcf_AMPolicyAuthorization_Notify as defined in 3GPP TS 29.534 [50] clause 4.2.7.2 (in addition, a Nnef_AMPolicyAuthorization_Notify request/response may occur between the NEF and the AF if the notification is relayed via the NEF).

4b. The AF (either directly or via the NEF) sends an HTTP "204 No Content" response as defined in 3GPP TS 29.534 [50] clause 4.2.7.2.

5. The AMF deploys the Access and Mobility control policy information if received which includes, e.g. 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 when the UE is registered in the 3GPP access.

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.

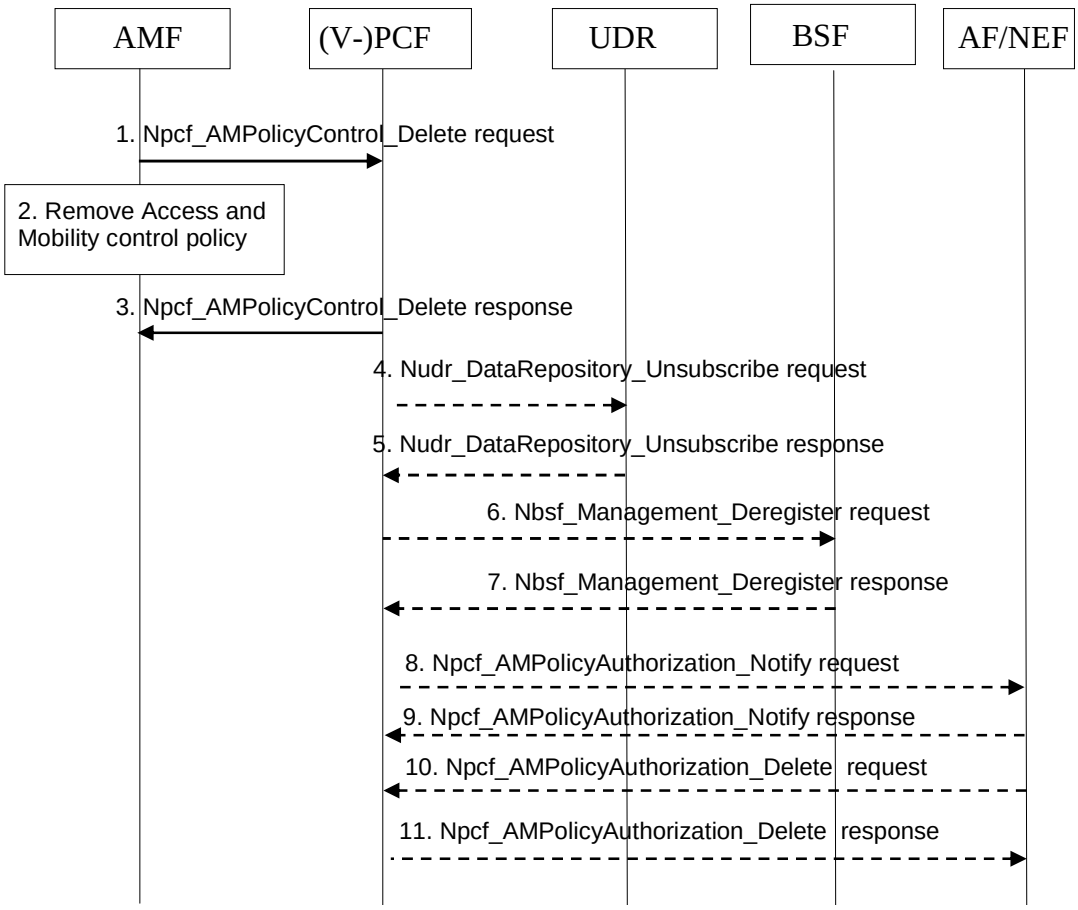


Figure 5.1.3.1-1: AMF-initiated AM Policy Association Termination procedure

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 an HTTP DELETE request to the "IndividualPolicyDataSubscription" resource if it has subscribed such notification. The PCF invokes also the Nudr_DataRepository_Unsubscribe service operation to unsubscribe from notifications about AM Influence data changes at the UDR by sending an HTTP DELETE request to the "IndividualApplicationDataSubscription" resource if it has subscribed such notification.

5. The UDR responds with HTTP "204 No Content" to the PCF.

6. The PCF may also deregister from the BSF as the PCF for the UE (i.e. as the PCF that handles the AM Policy Association of this UE) by sending an HTTP DELETE request to the "Individual PCF for a UE Binding" resource of the Nbsf_Management_Deregister service as described in clause 4.2.3.3 of 3GPP TS 29.521 [22].
7. The BSF responds with "204 No Content" if the deregistration of the PCF for the UE was successful.
8. If there is AF/NEF application AM context associated with the UE, the PCF invokes the Npcf_AMPolicyAuthorization_Notify service operation by sending the HTTP POST request with the {termNotifUri} as the callback URI to the AF/NEF to trigger the AF to request the AF application AM context termination.
9. The AF/NEF sends an HTTP "204 No Content" response to the PCF.
10. The AF/NEF invokes the Npcf_AMPolicyAuthorization_Delete service operation by sending the HTTP POST request to the "Individual Application AM Context" resource.

11 The PCF removes the AF application AM session context and sends an HTTP "204 No Content" response to the AF.

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.

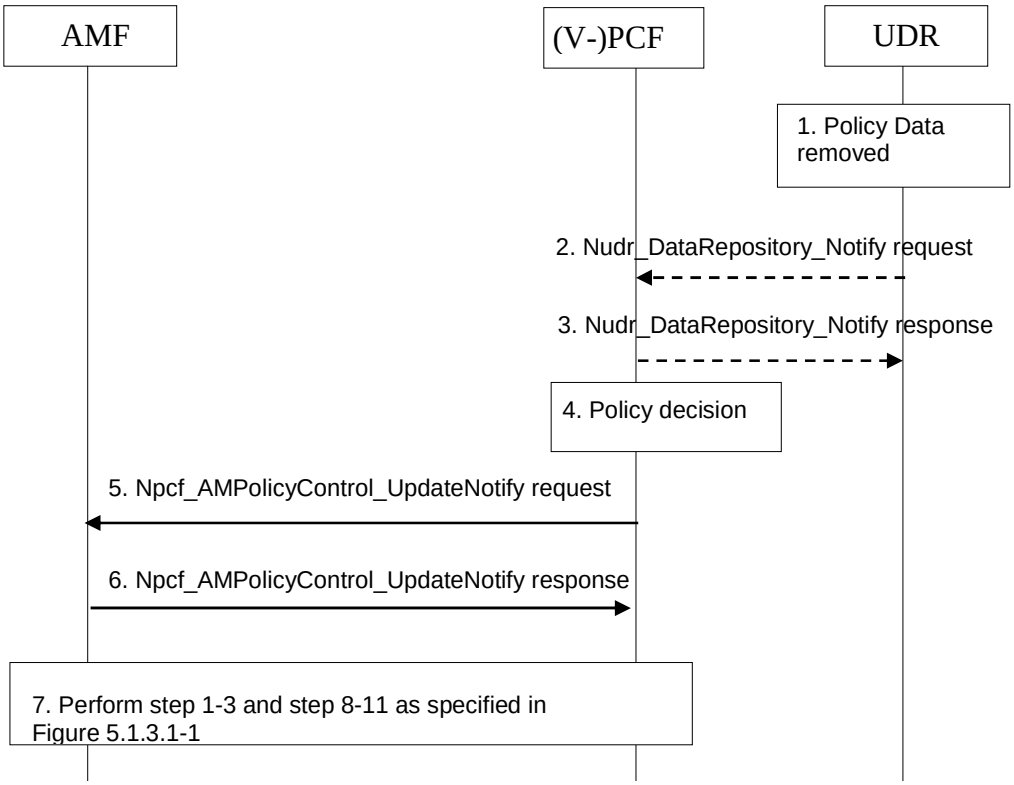


Figure 5.1.3.2-1: PCF-initiated AM Policy Association Termination procedure

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 callback 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, invoke the Npcf_AMPolicyControl_UpdateNotify service operation towards the AMF to notify it of the removal of the Access and Mobility control policy control information by sending an HTTP POST request to the request URI "{notificationUri}/terminate" as described in clause 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 and step 8 through step 11 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.

   - Step 8 through step 11 can be issued at any time after step 4.

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.

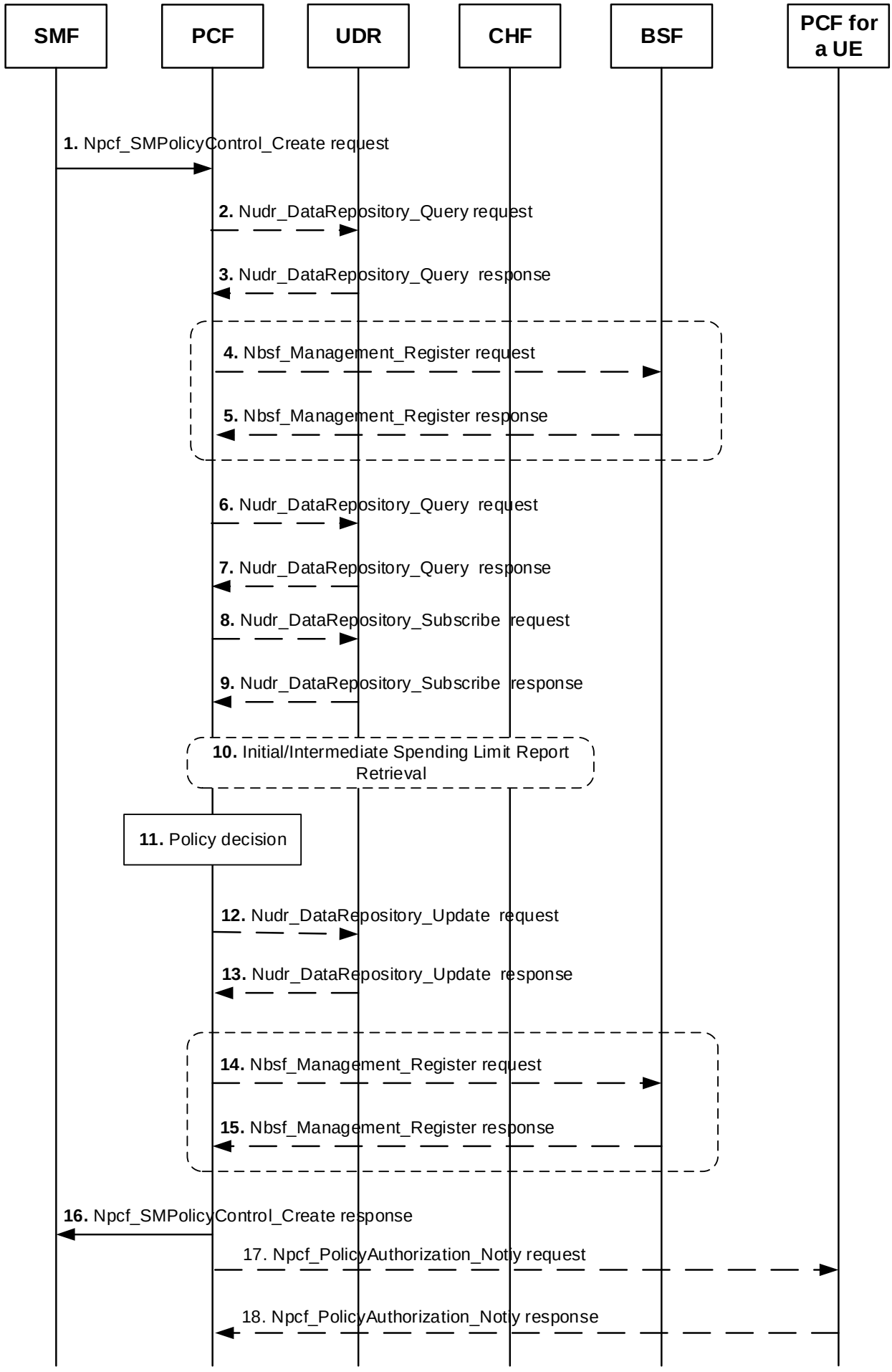

SMF
PCF
UDR
CHF
BSF
PCF for a UE
1. Npcf_SMPolicyControl_Create request
2. Nudr_DataRepository_Query request
3. Nudr_DataRepository_Query response
4. Nbsf_Management_Register request
5. Nbsf_Management_Register response
6. Nudr_DataRepository_Query request
7. Nudr_DataRepository_Query response
8. Nudr_DataRepository_Subscribe request
9. Nudr_DataRepository_Subscribe response
10. Initial/Intermediate Spending Limit Report Retrieval
11. Policy decision
12. Nudr_DataRepository_Update request
13. Nudr_DataRepository_Update response
14. Nbsf_Management_Register request
15. Nbsf_Management_Register response
16. Npcf_SMPolicyControl_Create response
17. Npcf_PolicyAuthorization_Notiy request
18. Npcf_PolicyAuthorization_Notiy response

Figure 5.2.1-1: SM Policy Association Establishment procedure

This procedure concerns 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.

NOTE 1: For LBO roaming case, session management policy data for the UE is not available in the VPLMN and V-PCF uses locally configured information according to the roaming agreement with the HPLMN operator. Therefore, interactions between PCF and UDR in the following procedures do not apply to this scenario.

1. The SMF receives a PDU session establishment request from the UE. The SMF selects the PCF as described in clause 8.3 and invokes the Npcf_SMPolicyControl_Create service operation by sending the HTTP POST request to the "SM Policies" resource as defined in clause 4.2.2.2 of 3GPP TS 29.512 [9]. 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(s), the Access Type (and additional access type, in case of MA PDU session), the IPv4 address or the IPv6 network prefix (if available), the MA PDU session indication and the ATSSS capability, if available, the PEI if received in the SMF, the User Location Information, the UE Time Zone, Serving Network, RAT type, charging information, the Session-AMBR, the DN-AAA authorization profile index if available, one or more framed routes if available, the subscribed default QoS, if available, etc., as defined in clause 4.2.2 of 3GPP TS 29.512 [9]. 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 "PvsSupport" feature defined in 3GPP TS 29.512 [9] is supported and the Onboarding Indication is received these steps are skipped. Otherwise, if PCF does not have the subscription data for the SUPI, DNN and S-NSSAI, 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.

4. If the "ExtendedSamePcf" feature is supported, and based on operator's policies and retrieved data the PCF determines that the same PCF needs to be used for all the SM Policy associations that match a combination of SUPI, DNN and S-NSSAI, and no SM Policy association for the given combination exists, the PCF invokes the Nbsf_Management_Register service operation to check if another PCF exists for the given parameter combination as specified in 3GPP TS 29.512 [9], clause 4.2.2.2.

   If the "ExtendedSamePcf" feature is not supported and the "SamePcf" is supported, and based on operator's policies and retrieved data the PCF determines that the same PCF needs to be used for all the SM Policy associations that match a combination of SUPI, DNN and S-NSSAI, and no SM Policy association for the given combination exists, the PCF invokes the Nbsf_Management_Register service operation to check if another PCF exists for the given parameter combination as specified in 3GPP TS 29.512 [9] clause 4.2.2.2 if the BSF is to be used for PDU session binding and the IP address/prefix or MAC address is received in step 1.

   The PCF includes together with the PCF address information for the Npcf_SMPolicyControl, in case the BSF is to be used for PDU session binding, the PCF address information for the Npcf_PolicyAuthorization and/or Rx, and the UE address, if available.

5. If the PCF receives an HTTP "201 Created" response from the BSF with the created binding information as detailed in clause 8.5.2 and the flow continues in step 6.

   If the PCF receives an HTTP "403 Forbidden" response from the BSF, the PCF replies the SMF as described in 3GPP TS 29.512 [9], clause 4.2.2.2and the flow terminates here.

6-7. If BDT Reference ID(s) is included in the response from the UDR, the PCF shall invoke the Nudr_DataRepository_Query service operation to the UDR to retrieve the Background Data Transfer policy corresponding to the BDT Reference ID(s) by sending the HTTP GET request to the " IndividualBdtData" resource or the "BdtData" collection resource with the URI query parameter "bdt-ref-ids" as specified in 3GPP TS 29.519 [12], and the UDR sends an HTTP "200 OK" response to the PCF with the Background Data Transfer policy.

   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.

Additionally, if the ATSSS feature defined in 3GPP TS 29.512 [9] is supported, and the SDF template of the PCC rule includes an application identifier, the PCF invokes the Nudr_DataRepository_Query service operation to retrieve the stored OS Id(s) supported by the UE from the UDR by sending the HTTP GET request to the "UePolicySet" resource as specified in 3GPP TS 29.519 [12]. The UDR sends an HTTP "200 OK" response with the stored UE Policy data. The PCF determines the application descriptors based on the retrieved OS Id(s), if available, and local configuration, as specified in 3GPP TS 29.512 [9].

Additionally, if the WWC feature defined in 3GPP TS 29.512 [9] is supported, the PCF invokes the Nudr_DataRepository_Query service operation to retrieve the stored IPTV configuration from the UDR by sending the HTTP GET request to the "IPTV Configurations" resource as specified in 3GPP TS 29.519 [12]. The UDR sends an HTTP "200 OK" response with the stored IPTV configuration. The PCF determines Multicast Access Control information (i.e., whether the multicast channel represented by the SDF of the PCC rule is allowed or not) based on the retrieved IPTV configuration as specified in 3GPP TS 29.512 [9].

Additionally, when network slice data rate related policy control is supported by the PCF, the PCF may invoke the Nudr_DataRepository_Query service operation towards the UDR by sending an HTTP GET request targeting the "SlicePolicyControlData" resource as specified in clause 5.2.12 of 3GPP TS 29.519 [12]. The UDR sends an HTTP "200 OK" response to the PCF with the network slice policy control data.

8-9. To request notifications from the UDR on changes in the policy data 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.

Additionally, if the WWC feature defined in 3GPP TS 29.512 [9] is supported, to request notifications from the UDR on changes in the IPTV configuration, the PCF invokes the Nudr_DataRepository_Subscribe service operation by sending an HTTP POST request to the "ApplicationDataSubscriptions" resource. The UDR sends an HTTP "201 Created" response to acknowledge the subscription.

10. If the PCF determines that the policy decision depends on the status of the policy counters available at the CHF, and such reporting is not established for the subscriber, the PCF initiates an Initial Spending Limit Report Retrieval as defined in clause 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 clause 5.3.3.

11. The PCF makes the policy decision to determine the information provided to the SMF.

When the feature "TimeSensitiveNetworking" or "TimeSensitiveCommunication" is supported and the PCF detects that the request relates to TSC traffic based on the received DNN and S-NSSAI, the PCF determines to provide the "TSN_BRIDGE_INFO" policy control request trigger to the SMF.

12-13. If network slice data rate related policy control applies, the (H-)PCF may invoke the Nudr_DataRepository_Update service operation by sending an HTTP PATCH request targeting the "SlicePolicyControlData" resource in order to update the Remaining Maximum Slice Data Rate information.

14. When the "SamePcf" feature is not supported, 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 clause 8.5.2.

When the "SamePcf" feature or the "ExtendedSamePcf" feature is supported, the PCF determines that the same PCF needs to be used for the SM Policy associations of the same DNN, S-NSSAI and SUPI parameter combination, and a SM Policy association already exists for the given parameter combination (i.e., step 4, 5 did not apply) 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 clause 8.5.2, and includes:

- the PCF address for the Npcf_SMPolicyControl service; and

- in the case that the BSF is to be used for PDU session binding, the PCF address for the Npcf_PolicyAuthorization and/or Rx interface, and either the IP address/prefix or MAC address if available.

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

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

17. If the PCF as a PCF for a PDU session receives the callback URI of the PCF for a UE in step 1, the PCF shall send the event of PDU session established to the AF by sending an HTTP POST request to the "{notifUri}/pdu-session" callback URI as defined in clause 4.2.5.22 of 3GPP TS 29.514 [10].

18. The PCF for a UE sends an HTTP "204 No Content" response to the PCF.

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.

NOTE 1: For LBO roaming case, session management policy data for the UE is not available in the VPLMN and V-PCF uses locally configured information according to the roaming agreement with the HPLMN operator. Therefore, interactions between PCF and UDR in the following procedures do not apply to this scenario.

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

NOTE 2: 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.

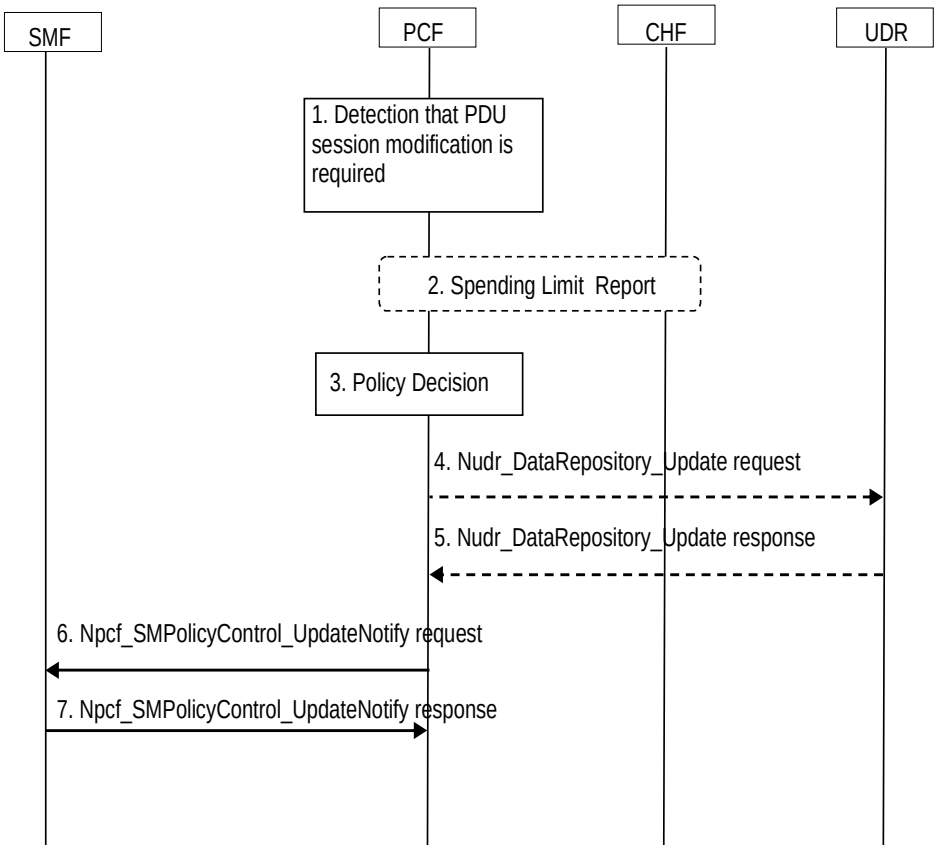


Figure 5.2.2.2.1-1: Interactions between SMF, PCF and CHF for PCF-initiated SM Policy Association Modification procedure

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

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

   - The UDR notifies the PCF about application data change (e.g. change in AF influence data or IPTV configuration data).

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

4-5. If network slice data rate related policy control applies, the (H-)PCF may invoke the Nudr_DataRepository_Update service operation by sending an HTTP PATCH request targeting the "SlicePolicyControlData" resource in order to update the Remaining Maximum Slice Data Rate information.

6. The PCF invokes the Npcf_SMPolicyControl_UpdateNotify service operation by sending the HTTP POST request with "{notificationUri}/update" as the callback URI to the SMF that has previously subscribed. The request operation provides the PDU session ID and the updated policies, as described in clause 4.2.3 of 3GPP TS 29.512 [9].

7. The SMF sends an HTTP "200 OK" or HTTP "204 No Content" 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 1: The NEF acts as an AF to support the network exposure functionality.

For the integration with TSC networks the AF represented in the figures is either the TSN AF (integration with IEEE TSN networks) or the TSCTSF (integration with other TSC networks than IEEE TSN).

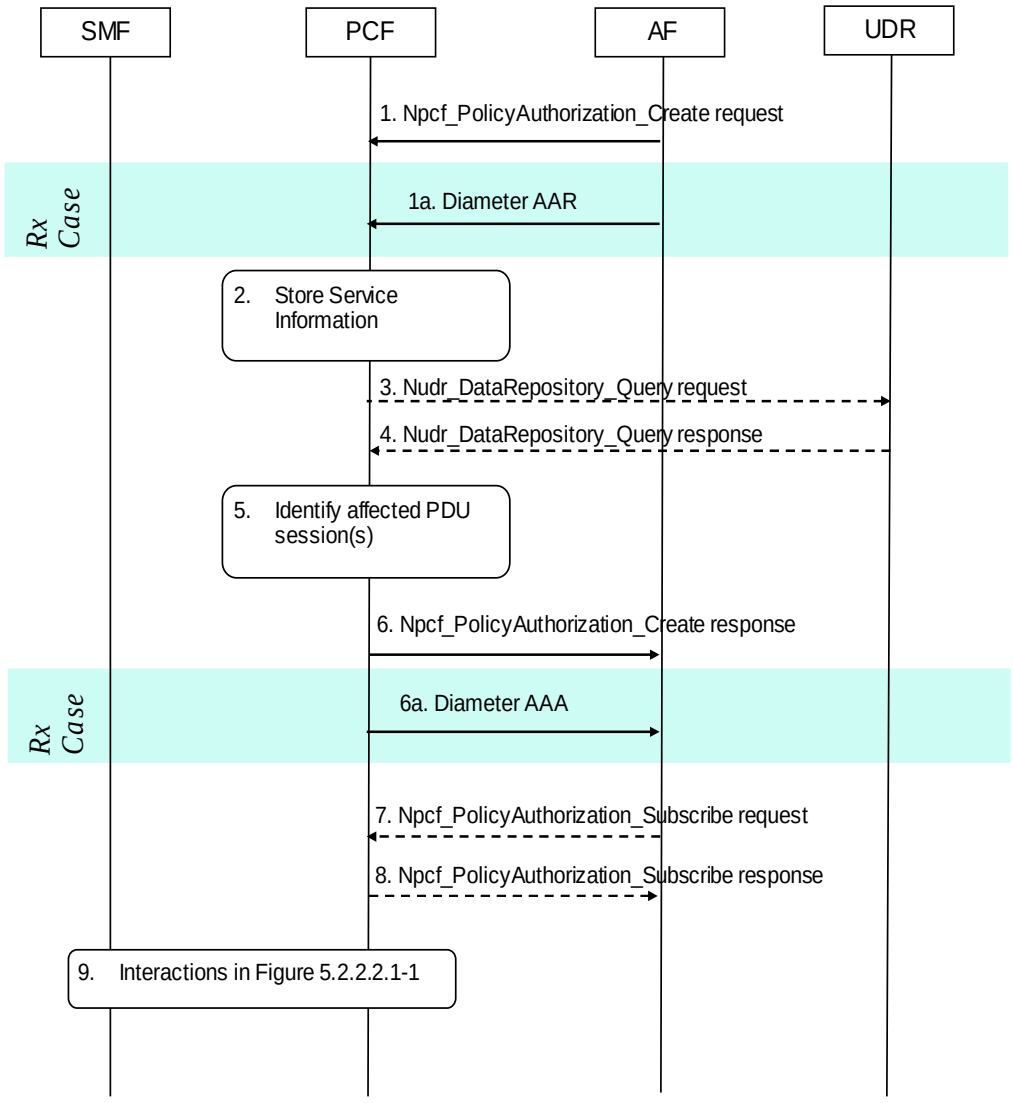


Figure 5.2.2.2.2.1-1: AF Session Establishment triggers PCF-initiated SM Policy Association Modification procedure

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 IP address or the MAC address of the UE, the SUPI if available, the GPSI if available, the DNN if available, the S-NSSAI if available, service information, sponsored data connectivity if applicable, AF application identifier, Priority indicator, etc, as defined in clause 4.2.2.2 of 3GPP TS 29.514 [10]. The request operation may also include the subscription to notifications

on certain user plane events, e.g. subscription to QoS notification control. To invoke MPS for DTS, the AF includes the MPS Action indication as defined in 3GPP TS 29.514 [10].

If the "TimeSensitiveNetworking" or "TimeSensitiveCommunication" feature is supported the TSN AF or TSCTSF may subscribe to notification of DS-TT PMIC and/or NW-TT PMIC(s) and/or UMIC availability. The TSN AF or TSCTSF may also provide TSC Assistance Container and QoS related data and/or a UMIC and/or one or more PMIC(s).

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, DNN and S-NSSAI, 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, when network slice data rate related policy control is supported by the PCF, the PCF may invoke the Nudr_DataRepository_Query service operation towards the UDR by sending an HTTP GET request targeting the "SlicePolicyControlData" resource as specified in clause 5.2.12 of 3GPP TS 29.519 [12]. The UDR sends an HTTP "200 OK" response to the PCF with the network slice policy control 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.

If the AF session is for MPS for DTS invocation, the PCF performs MPS subscription checks if and only if requested by the AF as described in clause 4.4.11 of 3GPP TS 29.214 [18] or as described in clause 4.2.2.12.2 of 3GPP TS 29.514 [10].

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 clause 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.

5.2.2.2.2.2 AF Session Modification

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

NOTE 1: The NEF acts as an AF to support the network exposure functionality.

For the integration with TSC networks the AF represented in the figures is either the TSN AF (integration with IEEE TSN networks) or the TSCTSF (integration with other TSC networks than IEEE TSN).

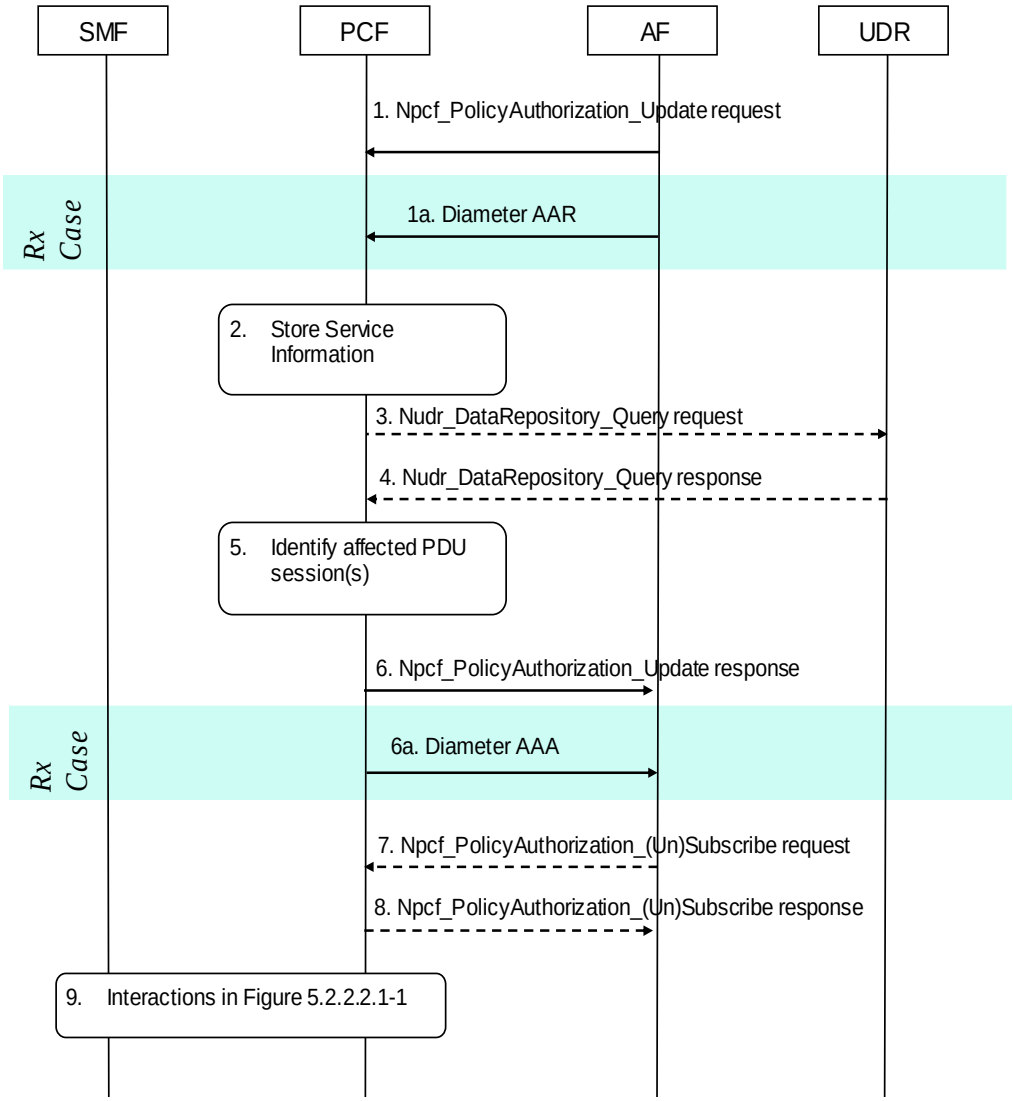


Figure 5.2.2.2.2.2-1: AF Session Modification triggers PCF-initiated SM Policy Association Modification procedure

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 as defined in clause 4.2.3.2 of 3GPP TS 29.514 [10]. The AF may also provide the updated subscription to notifications on user plane events. To invoke/revoke MPS for DTS, the AF includes the MPS Action indication as defined in 3GPP TS 29.514 [10].

   If the "TimeSensitiveNetworking" or "TimeSensitiveCommunication" feature is supported the AF may also update the TSC Assistance Container and QoS related data and/or a UMIC and/or one or more PMIC(s).

   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 clause 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" or HTTP "204 No Content" 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 "200 OK" or 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 AF/NEF requests the PCF to delete the AF application session context.

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

For the integration with TSC networks the AF represented in the figures is either the TSN AF (integration with IEEE TSN networks) or the TSCTSF (integration with other TSC networks than IEEE TSN).

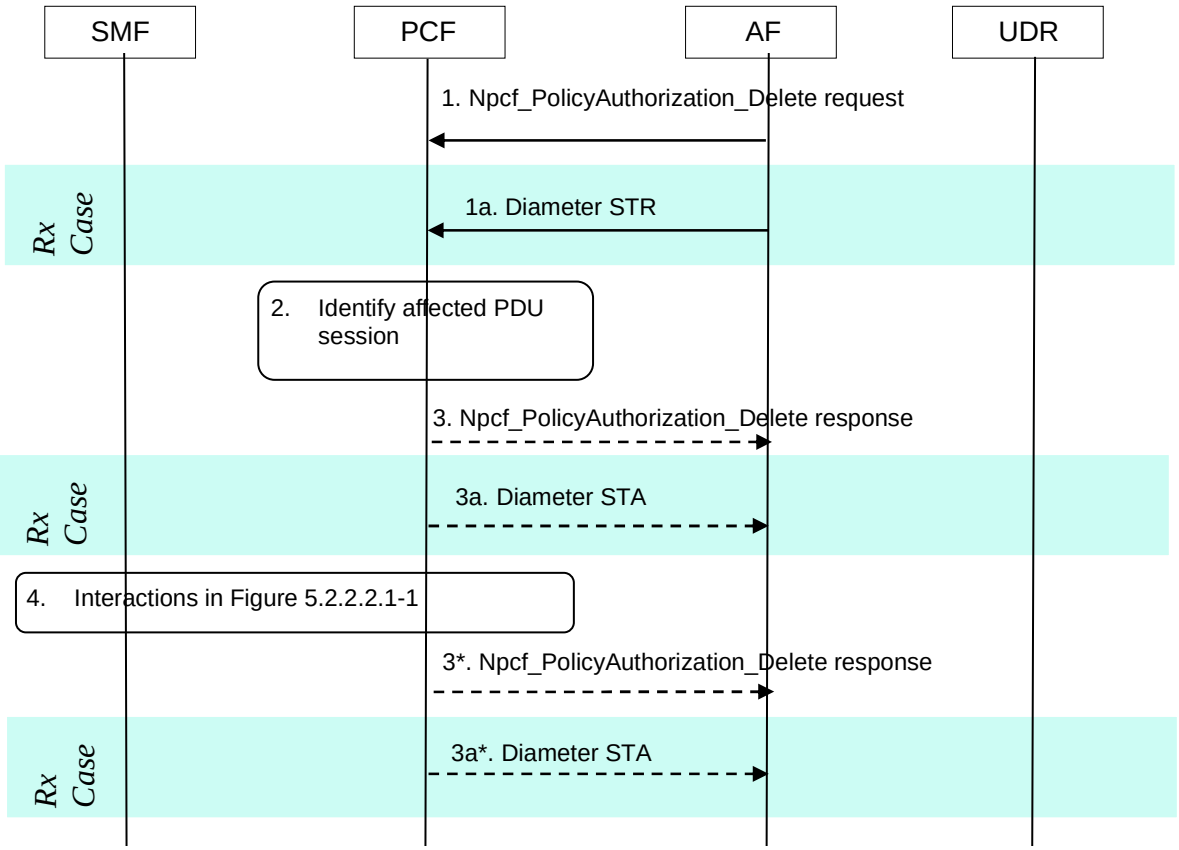


Figure 5.2.2.2.2.3-1: AF Session Termination triggers PCF-initiated SM Policy Association Modification procedure

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 as defined in clause 4.2.3.2 of 3GPP TS 29.514 [10]. 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. The request may include the events to subscribe to

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.

   If the request in step 1 or step 1a does not include the event(s) or it includes the event(s) but the corresponding information is available at the PCF, step 3 or step3a is performed respectively; otherwise, the step 3* or step3a* is performed respectively.

3. The PCF removes the AF application session context and sends an HTTP "204 No Content" or HTTP "200 OK" response to the AF.

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

3*. The PCF removes the AF application session context and sends an HTTP "200 OK" response with the information corresponding to the requested event(s) to the AF.

   3a*. The PCF sends a Diameter STA, session termination answer with the information corresponding to the requested event(s), 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 or a PCC rule error is reported.

For the integration with TSC networks the AF represented in the figures is either the TSN AF (integration with IEEE TSN networks) or the TSCTSF (integration with other TSC networks than IEEE TSN).

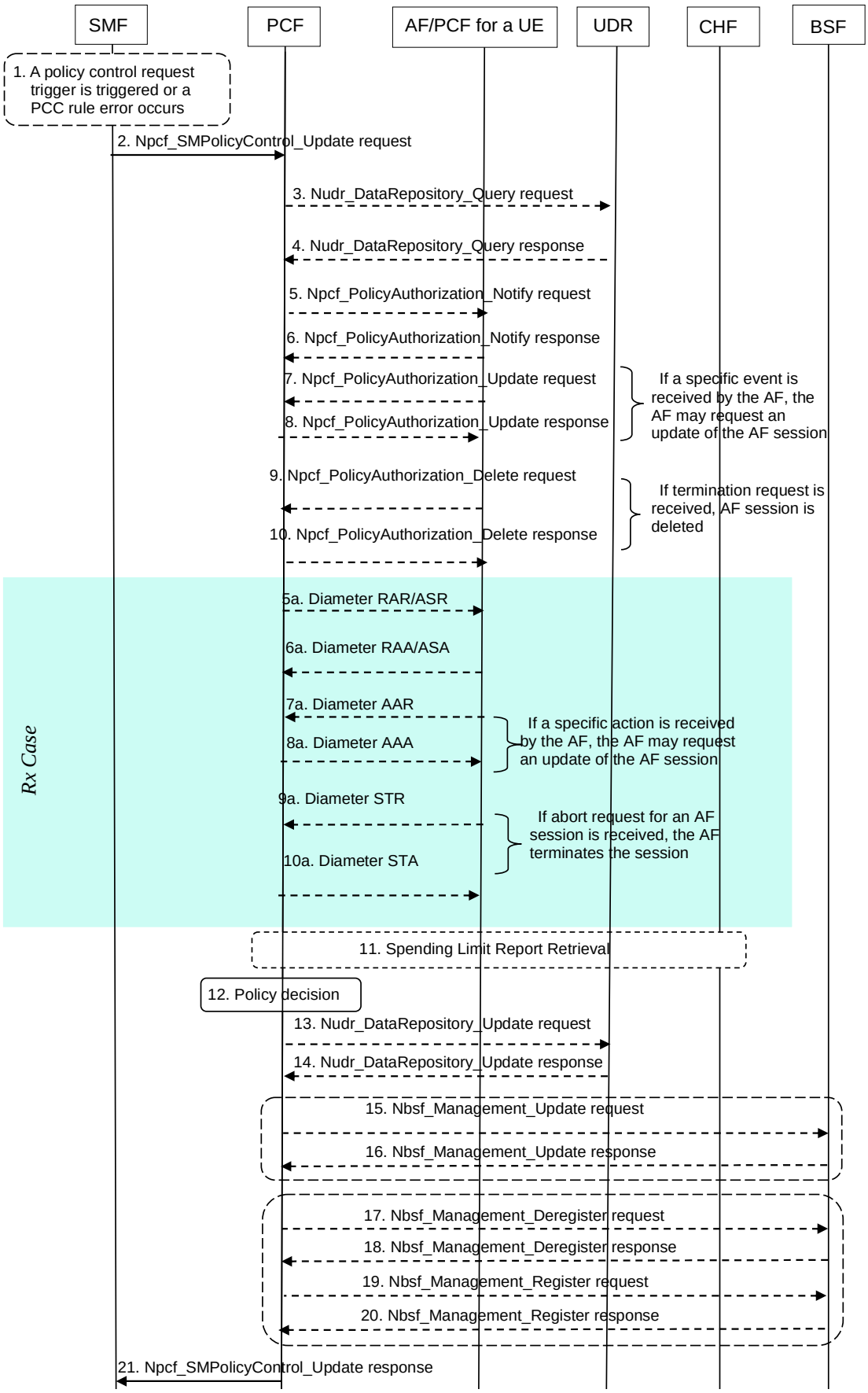


Figure 5.2.2.3-1: SMF-initiated SM Policy Association Modification procedure

1. The SMF detects a policy control request trigger condition is met or an error is reported.

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 or a PCC rule error occurs.

   If the feature "TimeSensitiveNetworking" or "TimeSensitiveCommunication" is supported and the "TSN_BRIDGE_INFO" policy control request trigger is provisioned in the SMF, the SMF may provide during PDU session establishment TSC user plan node information (DS-TT port number, DS-TT MAC address, if applicable, TSC user plane node Id and UE-DS-TT residence time, if available), and, if available, a UMIC and/or one or more PMIC(s) to the PCF, or, during PDU session modification procedures, updated UMIC and/or PMIC(s).

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.

   Additionally, when network slice data rate related policy control is supported by the PCF, the PCF may invoke the Nudr_DataRepository_Query service operation towards the UDR by sending an HTTP GET request targeting the "SlicePolicyControlData" resource.

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.

NOTE 1: If the Npcf_SMPolicyControl_Update message of step 2 includes usage report(s), the (H-)PCF can also invoke the Nudr_DataRepository_Update service operation by sending an HTTP PATCH request to the "SessionManagementPolicyData" resource in order to update the usage monitoring information according to the received usage report(s).

NOTE 2: If the Npcf_SMPolicyControl_Update message of step 2 includes the outcome of the resource allocation and network slice data rate policy control is supported, the (H-)PCF can also invoke the Nudr_DataRepository_Update service operation by sending an HTTP PATCH request targeting the "SlicePolicyControlData" resource in order to update the Remaining Maximum Slice Data Rate information.

5. The PCF invokes the Npcf_PolicyAuthorization_Notify service operation to indicate that an event for which the AF requested a notification has occurred by sending the HTTP POST request with "{notifUri}/notify" as the callback URI to the AF or to request to the AF the deletion of the active application session if all the service data flows for the AF session are deleted by sending the HTTP POST request with "{notifUri}/terminate" as the callback URI to the AF.

   If the feature "TimeSensitiveNetworking" or "TimeSensitiveCommunication" is supported:

   - When the PCF detects that there is no Individual Application Session Context resource bound to the Individual SM Policy resource the PCF shall provide the new TSC user plane node information received in step 2 to the TSN AF or TSCTSF by sending an HTTP POST request to the "{notifUri}/new-bridge" request URI, where the "{notifUri}" value is pre-configured in the PCF or, if not pre-configured, discovered by invoking the Nnrf_NFDiscovery service as defined in 3GPP TS 29.510 [51].

NOTE 3: The TSCTSF registers in the NRF the notification URI within the default notification subscription for time sensitive communication and time synchronization notifications as described in 3GPP TS 29.510 [51].

   - When the PCF detects that there is an Individual Application Session Context resource bound to the Individual SM Policy resource, the PCF shall provide the received UMIC and/or PMICs to the AF by sending an HTTP POST request to the "{notifUri}/notify" callback URI.

   When the PCF as a PCF for a PDU session becomes aware that a SM Policy Association that is being modified is receiving the callback URI of the PCF for a UE in step 2, the PCF shall send the event of PDU session established to the PCF for a UE by sending an HTTP POST request to the "{notifUri}/pdu-session" callback URI as defined in subclause 4.2.5.22 of 3GPP TS 29.514 [10].

   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. If all service data flows for an AF session are deleted, the PCF sends a Diameter ASR to request to the AF the termination of the active session.

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

If the feature "TimeSensitiveNetworking" or "TimeSensitiveCommunication" is supported and the TSN AF or TSCTSF received the notification of new TSC user plan node information over the "{notifUri}/new-bridge" request URI, the TSN AF or TSCTSF shall trigger the Npcf_PolicyAuthorization_Create service operation as described in clause 5.2.2.2.2.1, to request the creation of a new Individual Application Session Context resource specific to the PDU session identified by, for Ethernet type of PDU sessions, the received MAC address of the DS-TT port and for IP type of PDU sessions, the received UE IP address.

NOTE 4: For the time synchronization service, the AF subscription to UE availability for time-synchronization service can occur after the PDU Session establishment has been completed in 5GS. Similarly, for the AF session with required QoS, the indication of the required QoS and TSC Assistance Container information can occur after the completion of the PDU session establishment. In such cases, the PCF sends the notification to the TSCTSF about the detection of a TSC user plane node information during PDU session establishment, but the TSCTSF doesn't have the time synchronization or required QoS available for the PDU session. In this case, the TSCTSF could defer the invocation of the Npcf_PolicyAuthorization_Create service operation till the reception of the subscription to UE availability for time synchronization or the AF session with required QoS occurs.

If the PCF for a UE receives the notification of PDU session establishment over the "{notifUri}/pdu-session" request URI and if the "ApplicationDetectionEvents" feature is supported, the PCF for a UE may trigger the Npcf_PolicyAuthorization_Subscribe service operation described in clause 4.2.6.9 to subscribe to the notification of the application detection;

6a. If the AF receives an event notification, the AF replies with a Diameter RAA and may provide within it updated service information. If the AF receives an indication that all service data flows for an AF session are deleted, the AF replies with a Diameter ASA.

7. If the PCF indicates in step 5 that an event for the active application session has occurred, 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.

7a. If the PCF indicates in step 5a that an event for the active application session has occurred, the AF may send a Diameter AAR to the PCF including the modified service information.

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

8a, The AF responds by sending a Diameter AAA to the PCF.

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.

9a. The AF sends a Diameter STR message to the PCF to indicate that the AF session is terminated.

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.

10a. The PCF responds by sending a Diameter STA message to the AF and 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 clause 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 clause 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 clause 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 21.

13-14. If network slice data rate related policy control applies, the (H-)PCF may invoke the Nudr_DataRepository_Update service operation by sending an HTTP PATCH request targeting the "SlicePolicyControlData" resource in order to update the Remaining Maximum Slice Data Rate information.

If the BindingUpdate feature defined in 3GPP TS 29.521 [22] is supported, the steps 15 to 16 will be performed, otherwise the steps 17 to 20 will be performed.

15. If the UE address changes and the binding information has been previously registered in the BSF, or if the "ExtendedSamePcf" feature is supported, and the PCF registered binding information without including the UE address and UE address is received in step 2 and required for the retrieval of binding information by any NF (e.g. for PDU session binding), the PCF invokes the Nbsf_Management_Update service operation by sending an HTTP PATCH request to update the binding information in the BSF as detailed in clause 8.5.7.

16. The PCF receives an HTTP "200 OK" response from the BSF.

17. 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 clause 8.5.3.

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

19. 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, or if the "ExtendedSamePcf" feature is supported, and the PCF registered binding information without including the UE address and UE address is received in step 2 and required for the retrieval of binding information by any NF, 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 clause 8.5.2.

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

21. 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).

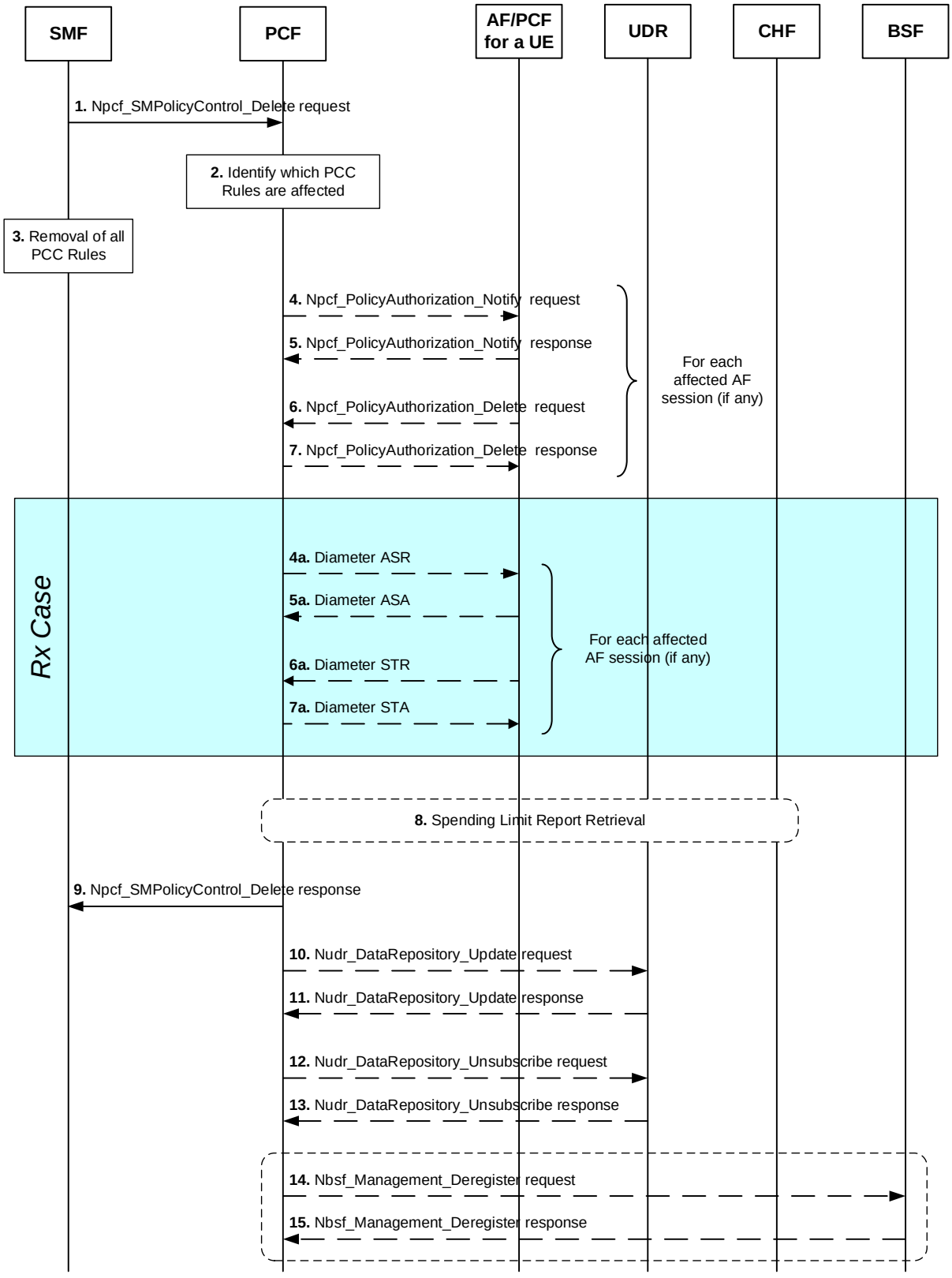


Figure 5.2.3.1-1: SMF-initiated SM Policy Association Termination procedure

This procedure concerns both roaming and non-roaming scenarios.

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

NOTE 1: For LBO roaming case, session management policy data is not stored in the VPLMN. Therefore, interactions between PCF and UDR in the SM Policy Association Termination procedures do not apply to this scenario.

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 as defined in clause 4.2.5.2 of 3GPP TS 29.512 [9]. 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 callback URI to the AF to trigger the AF to request the application session context termination.

   When the PCF as a PDU session determins that the SM Policy Association that is terminating contains the callback URI for the PCF for a UE, the PCF shall send the event of PDU session terminated to the PCF for a UE by sending an HTTP POST request to the "{notifUri}/pdu-session" callback URI as defined in clause 4.2.5.22 of 3GPP TS 29.514 [10].

   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. The request may include the events to subscribe to.

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 in step 6 and/or the RAN-NAS-Cause feature is supported, 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. 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 in step 6a and/or the RAN-NAS-Cause feature is supported, the PCF informs the AF about the access network information.

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

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

10. The PCF 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 and S-NSSAI are terminated.

    Additionally, if network slice data rate related policy control applies, the (H-)PCF may invoke the Nudr_DataRepository_Update service operation by sending an HTTP PATCH request targeting the "SlicePolicyControlData" resource in order to update the Remaining Maximum Slice Data Rate information.

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 changes 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.

- Additionally, to unsubscribe from notifications about IPTV configuration data changes at the UDR, the PCF invokes the Nudr_DataRepository_Unsubscribe service operation by sending an HTTP DELETE request to the "IndividualApplicationDataSubscription" 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 clause 8.5.3.

NOTE: The PCF invokes the Nbsf_Management_Deregister for every binding information previously registered in the BSF for the PDU session.

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

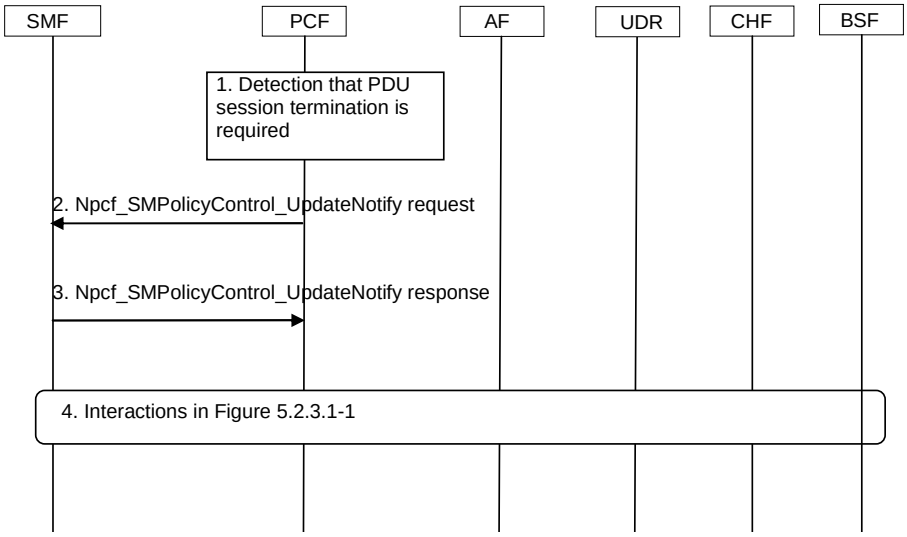


Figure 5.2.3.2-1: PCF-initiated SM Policy Association Termination procedure

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 "{notificationUri}/delete" as the callback URI to trigger the SMF to request the release of the PDU session as defined in clause 4.2.3.3 of 3GPP TS 29.512 [9]. The request includes resource URI of the individual SM policy to be deleted and the cause why the PCF requests the termination.

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.

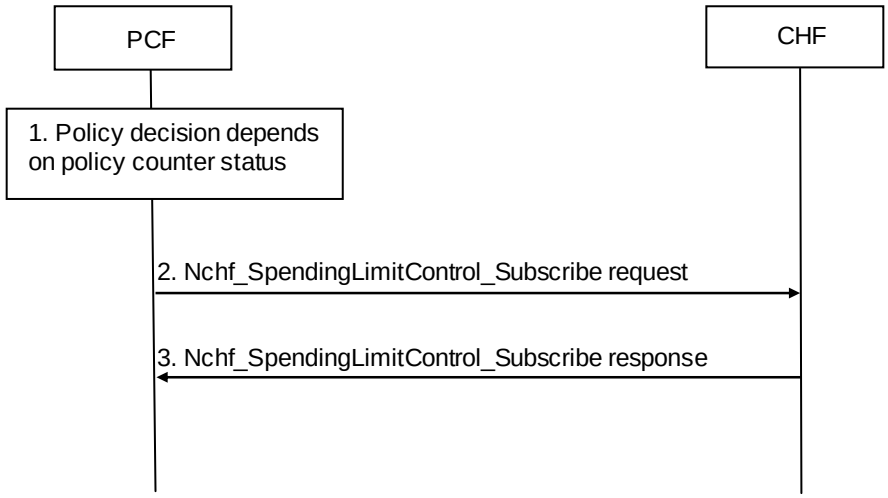


Figure 5.3.2-1: Initial Spending Limit Report Request procedure

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.

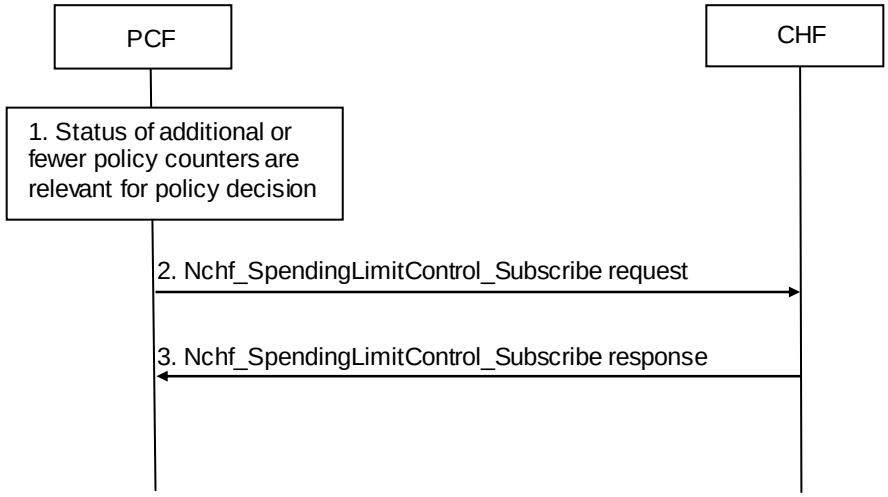


Figure 5.3.3-1: Intermediate Spending Limit Report Request procedure

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.

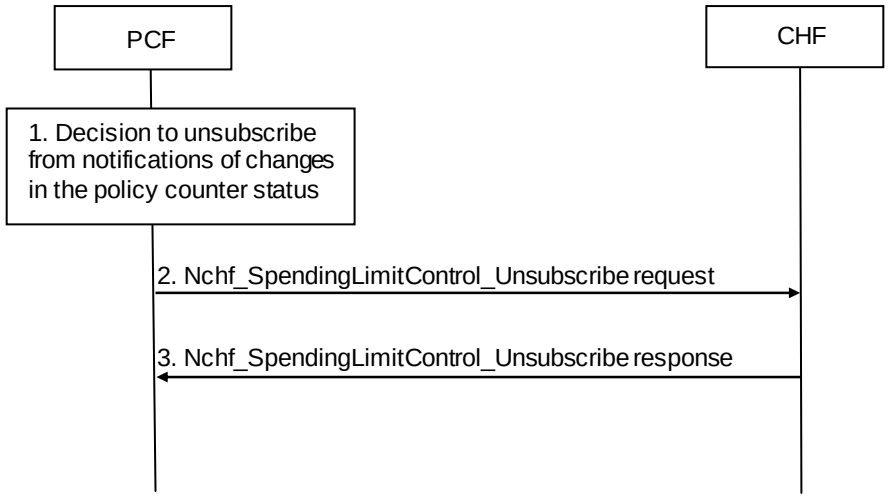


Figure 5.3.4-1: Final Spending Limit Report Request procedure

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.

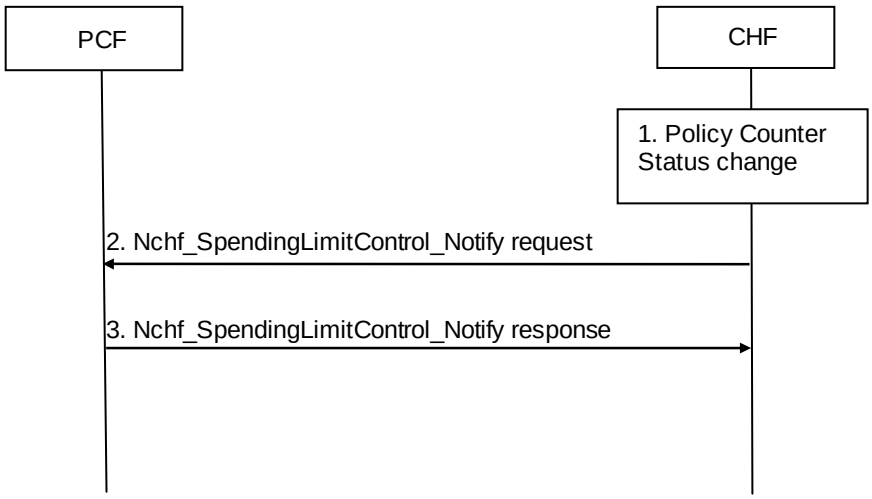


Figure 5.3.5-1: Spending Limit Report procedure

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.

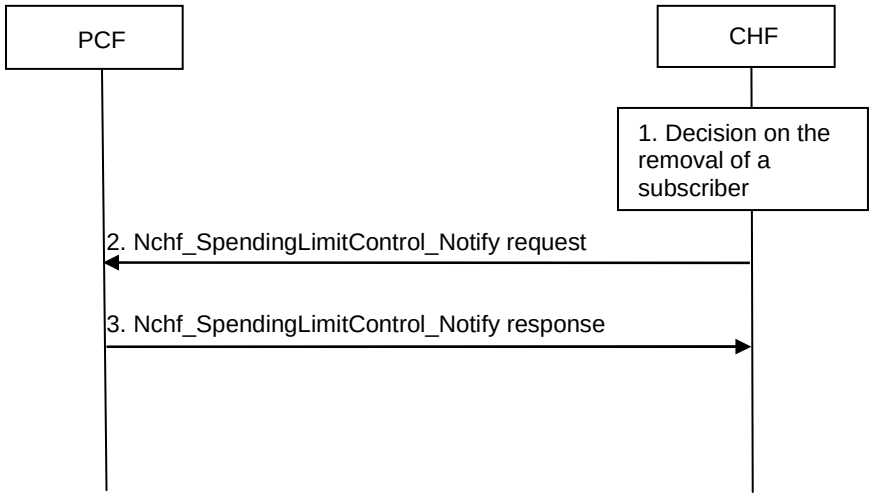


Figure 5.3.6-1: Subscription Termination Request procedure

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 analytics information as described in 3GPP TS 29.552 [48].

5.4.2 NWDAF Discovery and Selection by the PCF

The PCF performs discovery and selection of NWDAF as follows:

- When the "EneNA" feature is supported as described in 3GPP TS 29.507 [7], the PCF for the UE may select the list of NWDAF instance IDs used for the UE and their associated Analytic ID(s) based on the NWDAF information provided by the AMF as part of the AM Policy Association Establishment and/or Modification procedures as described in 3GPP TS 29.507 [7].
- When the "EneNA" feature is supported as described in 3GPP TS 29.512 [9], the PCF for the PDU Session may select the list of NWDAF instance IDs used for the PDU Session and their associated Analytic ID(s) based on the NWDAF information provided by the SMF as part of the SM Policy Association Establishment and/or Modification procedures as described in 3GPP TS 29.512 [9].
- When the NWDAF instance IDs provided by the AMF or SMF do not relate to the Analytics ID(s) required by the PCF, the PCF may perform NWDAF discovery as described in 3GPP TS 29.510 [51].

5.4.3 Policy decisions based on Network Analytics

The following Analytics IDs (observed events as described in 3GPP TS 29.520 [11]) are relevant for Policy decisions: "Slice Load level information", "Service Experience", "Network Performance", "Abnormal behaviour", "UE Mobility", "UE Communication", "User Data Congestion", "Data Dispersion" and "WLAN performance".

The PCF may subscribe to these events and/or may retrieve the observed events when the information is needed.

In order for the PCF to subscribe to these events, the PCF shall act as NF Service Consumer of the NWDAF as specified in 3GPP TS 29.520 [11] behaving as follows:

- The PCF may subscribe to notifications of network analytics related to "Slice Load Level Information" using the Nnwdaf_EventsSubscription_Subscribe service operation including the "event" attribute set to "SLICE_LOAD_LEVEL", the "snssais" attribute including the network slice and the "notificationMethod" attribute in "eventSubscriptions" attribute set to "THRESHOLD".

  NOTE 1: PCF does not subscribe to event "NSI_LOAD_LEVEL" since the network slice instance of a PDU session is not available in the PCF

- If the feature "ServiceExperience" is supported as defined in TS 29.520 [11], the PCF may subscribe to notifications of network analytics related to "Service Experience" using the Nnwdaf_EventsSubscription_Subscribe service operation including the "event" attribute set to "SERVICE_EXPERIENCE", the "tgtUe" attribute with the identification of target UE(s) to which the subscription applies included in the "supis", "intGroupIds" or "anyUe" attribute, the "appIds" attribute with the identification of application(s) to which the subscription applies, the "ratFreqs" attribute if the feature "ServiceExperienceExt" is also supported including all the RAT types and/or all the frequencies that the NWDAF received for the application or specific RAT type(s) and/or frequencies where the UE camps and the service experience threshold value(s) for the RAT Type(s) and/or Frequency value(s).

- If the feature "NetworkPerformance" is supported as defined in TS 29.520 [11], the PCF may subscribe to notifications of network analytics related to "Network Performance" using the Nnwdaf_EventsSubscription_Subscribe service operation including the "event" attribute set to "NETWORK_PERFORMANCE", the "tgtUe" attribute with the identification of target UE(s) to which the subscription applies within the "intGroupIds" attribute and the "networkArea" attribute with the identification network area to which the subscription applies.

- If the feature "AbnormalBehaviour" is supported as defined in TS 29.520 [11], the PCF may subscribe to notifications of network analytics related to "Abnormal Behavior" using the Nnwdaf_EventsSubscription_Subscribe service operation including the "event" attribute set to "ABNORMAL_BEHAVIOUR", the "tgtUe" attribute with the identification of target UE(s) to which the subscription applies included in the "supis", "intGroupIds" or "anyUe" attribute and either the "exptAnaType" attribute with the expected analytics or the"excepRequs" attribute with a list of exception Ids with the associated thresholds. Per each Exception Id, it is possible to provide additional information as described in TS 29.520 [11].

- If the feature "UeMobility" is supported as defined in TS 29.520 [11], the PCF may subscribe to notifications of network analytics related to "UE Mobility" using the Nnwdaf_EventsSubscription_Subscribe service operation including the "event" attribute set to "UE_MOBILITY", the "tgtUe" attribute with the identification of target UE(s) to which the subscription applies within the "supis" or "intGroupIds" attribute and the "networkArea" attribute with the identification network area to which the subscription applies.

- If the feature "UeCommunication" is supported as defined in TS 29.520 [11], the PCF may subscribe to notifications of network analytics related to "UE communication" using the Nnwdaf_EventsSubscription_Subscribe service operation including the "event" attribute set to "UE_COMMUNICATION", the "tgtUe" attribute with the identification of target UE(s) to which the subscription applies included in the "supis"or "intGroupIds" attribute and optionally the "appIds" attribute with the identification of application(s) to which the subscription applies.

- If the feature "UserDataCongestion" is supported as defined in TS 29.520 [11], the PCF may subscribe to notifications of network analytics related to "User Data Congestion" using the Nnwdaf_EventsSubscription_Subscribe service operation including the "event" attribute set to "USER_DATA_CONGESTION" and the "tgtUe" attribute with the identification of the target UE to which the subscription applies included in the "supis" attribute and optionally the "networkArea", "congThresholds" attributes with the area of interests and the reporting threshold respectively. If the feature "UserDataCongestionExt" is supported, the PCF may also provide the "maxTopAppUlNbr" and/or "maxTopAppDlNbr" attributes with the requested maximum number of top applications that contribute the most to the traffic.

- If the feature "Dispersion" is supported as defined in TS 29.520 [11], the PCF may subscribe to notifications of network analytics related to "Dispersion" using the Nnwdaf_EventsSubscription_Subscribe service operation including the "event" attribute set to "DISPERSION", the "tgtUe" attribute with the identification of target UE(s)

to which the subscription applies included in the "supis", "intGroupIds" or "anyUe" attribute and the "disperType" attribute within the "disperReqs" attribute set to the applicable dispersion analytic type. Optionally, the PCF may include the "networkArea" attribute with the identification network area to which the subscription applies, the identification of the network slice(s) by "snssais" attribute and/or the dispersion analytics requirements in "disperReqs" attribute, which for the requested dispersion type may include dispersion class within "disperClass" set to "TOP_HEAVY". If the PCF is interested in the average data rate in the network slice, the PCF may set the "disperType" attribute within the "disperReqs" attribute set to "DVDA" and it shall provide the network slice within the "snssais" attribute and the "tgtUe" attribute set to "anyUe".

- If the feature "WlanPerformance" is supported as defined in TS 29.520 [11], the PCF may subscribe to notifications of network analytics related to "WLAN Performance" using the Nnwdaf_EventsSubscription_Subscribe service operation including the "event" attribute set to "WLAN_PERFORMANCE" and the "tgtUe" attribute with the identification of target UE(s) to which the subscription applies included in the "supis", "intGroupIds" or "anyUe" attribute. The PCF may provide any of "networkArea", "ssIds" or "bssIds" attributes to which the subscription applies within "wlanReqs" attribute.

When the PCF requires the events related to any of these analytics Ids immediately, it shall initiate an Nnwdaf_AnalyticsInfo_Request service operation towards the NWDAF. In this case, the same level of information as for the subscription to events shall be provided as query parameters in the request, that is, the required event, filter and requirement information shall be provided in the "event-id", "event-filter" and "ana-req" URI query parameters.

Upon reception of any of the events as described above either in a subscription or retrieval request, the NWDAF shall behave as described in TS 29.520 [11].

The subscribing and/or retrieving of analytics information by the PCF from the NWDAF may be triggered by:

- Requests from AF/NEF;
- AM Policy association establishment or modification request from the AMF;
- SM Policy association establishment or modification request from the SMF;
- Notifications received from UDR or CHF on UE subscription change;
- Analytics information received.

NOTE 2: Examples of operator policies where network analytics information from NWDAF is required as inputs for policy decisions are described in clause 6.1.1.3 of 3GPP TS 23.503[4].

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.
4. The procedure of BDT warning notification.
5. The procedure of Background Data Transfer policy applying.
6. The procedure of IPTV configuration provisioning.
7. The procedure of AF-based service parameter provisioning.
8. The procedure of QoS monitoring.
9. The procedure of AF-triggered dynamically changing AM policies.

5.5.2 Management of Packet Flow Descriptions

5.5.2.1 AF-initiated PFD management procedure

This clause 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.

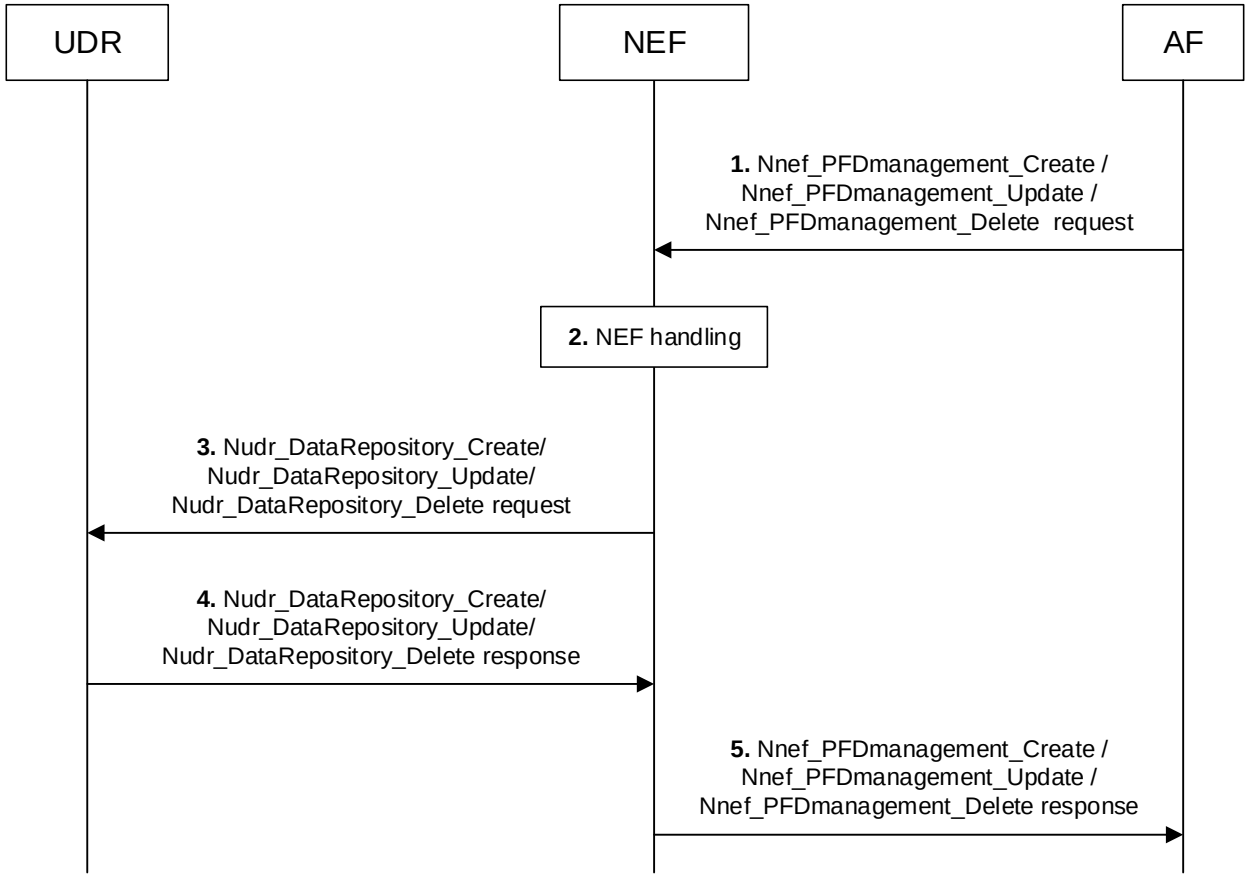


Figure 5.5.2.1-1: AF-initiated PFDF management procedure

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 "PFD Management Transactions".

   To update the PFDs for an existing individual transaction including one or more application identifier(s), 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" including one or more application identifier(s), 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 PFDs creation for a new application identifier 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" for the requested application identifier.

   - if PFDs update for an existing application identifier was requested in step 1, the NEF shall invoke the Nudr_DataRepository_Update service operation by sending an HTTP PUT request message to the resource "Individual PFD Data" for the requested application identifier.

   - if PFDs removal for an existing application identifier 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" for the requested application identifier.

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; or

- 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 PFDF to the SMF.

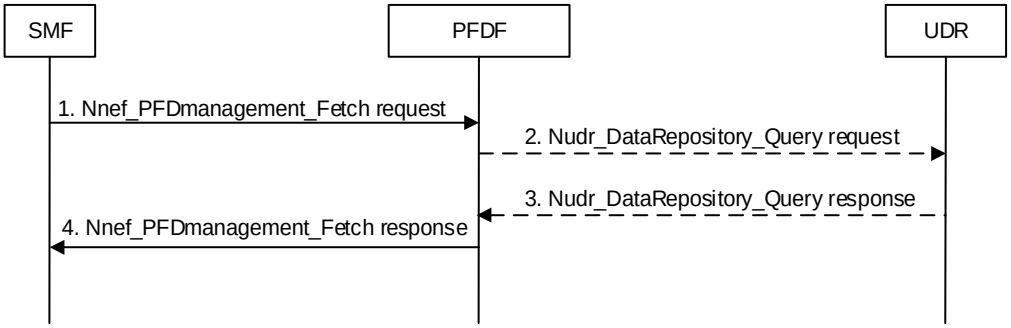


Figure 5.5.2.2.1-1: PFD retrieval by SMF

1. In order to retrieve the PFDs of individual application identifier, the SMF may invoke Nnef_PFDmanagement_Fetch service operation by sending an HTTP GET request message to the resource "{apiRoot}/nnef-pfdmanagement/v1/applications/{appId}" for the full pull procedure or invoke the Nnef_PFDmanagement_Fetch service operation by sending an HTTP POST request message to the resource "{apiRoot}/nnef-pfdmanagement/v1/applications/partialpull" for the partial pull procedure if the "PartialPull" feature is supported.

   In order to retrieve the PFDs of collection of application identifiers, the SMF may invoke the Nnef_PFDmanagement_Fetch service operation by sending an HTTP GET request message to the resource "{apiRoot}/nnef-pfdmanagement/v1/applications" with query parameters indicating the requested application

identifiers for the full pull procedure or invoke the Nnef_PFDmanagement_Fetch service operation by sending an HTTP POST request message to the resource "{apiRoot}/nnef-pfdmanagement/v1/applications/partialpull" for the partial pull procedure if the "PartialPull" feature is supported.

If the "NotificationPush" feature is supported and the PFD retrieval is performed due to a Notification Push received by the PFDF, the PFDF may indicate the PFD(s) operation in "pfdOp" attribute for SMF to determine the invoke action as defined in clause 5.5.2.2.2.

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,

   - in order to retrieve the PFDs of individual application identifier, the PFDF shall invoke Nudr_DataRepository_Query service operation by sending an HTTP GET request message to the UDR to the resource "Individual PFD Data".

   - in order to retrieve the PFDs of collection of application identifiers, the PFDF shall invoke the Nudr_DataRepository_Query service operation by sending an HTTP GET request message to the UDR to the resource "PFD Data" with query parameters indicating the requested application identifiers.

NOTE 2: For details of Nudr_DataRepository_Query service operation refer to 3GPP TS 29.519 [12].

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

4. The PFDF sends the "200 OK" response including the PFDs for the requested application identifier(s) to the SMF or sends the "204 No Content" response to indicate that the PFD(s) for all the requested application identifier(s) are not changed since last request if the partial pull procedure was invoked.

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.

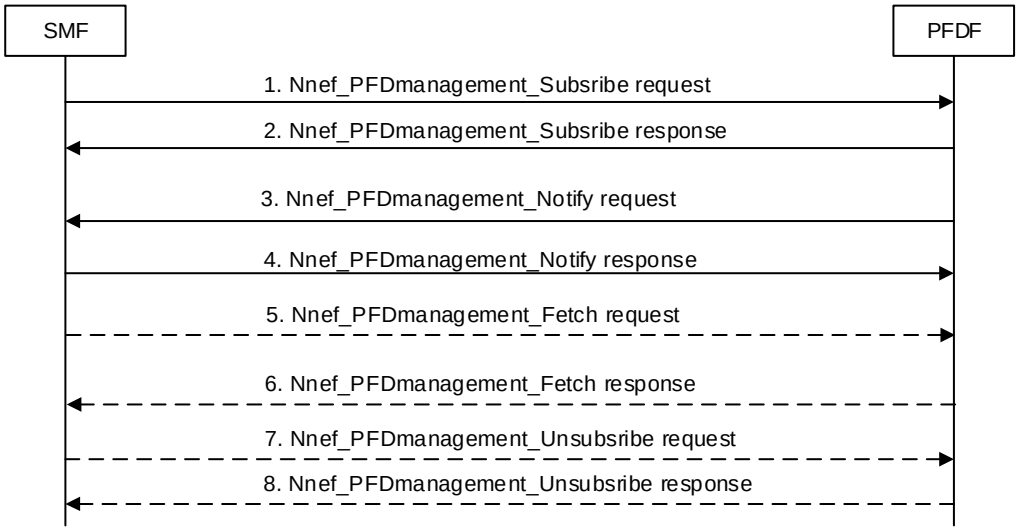


Figure 5.5.2.2.2-1: PFDF management in the SMF

1-2. In order to subscribe to the notification of events when the PFDs for application identifier change, the SMF invokes the 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, the PFDF sends the POST response message a "201 Created" to the SMF.

In order to update the existing event subscription and if the feature PfdChgSubsUpdate is supported, the SMF invokes the Nnef_PFDmanagement_Subscribe service operation by sending an HTTP PUT message to the

resource "Individual PFD subscription". If the request is accepted, the PFDF sends an HTTP "200 OK" response 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 may send an HTTP POST request message containing one or more PfdChangeNotification data structure to the notification URI "{notifyUri}" as defined in clause 4.2.4.2 of 3GPP TS 29.551 [25]. 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).

If the NotificationPush feature is supported, the PFDF may send an HTTP POST request message containing one or more NotificationPush data structure to the notification URI "{notifyUri}/notifypush" to request the SMF to retrieve the PFDs from the PFDF and/or remove the PFD(s). The SMF replies to the PFDF with a "204 No Content" status code if the SMF accepted the request.

5-6. If the SMF received the HTTP POST request message to request the SMF to retrieve the PFDs from the PFDF, depends on PFDF indication or SMF determination, the SMF may invoke the full pull procedure defined in clause 4.2.2.2 of 3GPP TS 29.551 [25] or invoke the partial pull procedure defined in clause 4.2.2.3 of 3GPP TS 29.551 [25] if the "PartialPull" feature is supported, using Nnef_PFDmanagement_Fetch service operation, to retrieve the PFD(s) for the application identifier(s).

7-8. 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/Fetch 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] clause 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 clause 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 clause 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) or to the same SNPN.

NOTE 4: The roaming scenarios for SNPNs are not supported in this Release.

NOTE 5: AF requests invoked from an AF located in the HPLMN for home routed roaming scenario are not supported.

NOTE 6: For details of Nnef_TrafficInfluence_Create/Update/Delete/AppRelocationInfo service operations refer to 3GPP TS 29.522 [24].

NOTE 7: For details of the Nudr_DataRepository_Create/Update/Delete service operations refer to 3GPP TS 29.519 [12] and 3GPP TS 29.504 [27].

NOTE 8: For details of the Nsmf_EventExposure_Notify/AppRelocationInfo service operations refer to 3GPP TS 29.508 [8].

NOTE 9: For details of the Npcf_PolicyAuthorization_Create/Update/Delete service operations refer to 3GPP TS 29.514 [10].

NOTE 10: For details of the Npcf_SMPolicyControl_UpdateNotify service operation refer to 3GPP TS 29.512 [9].

NOTE 11: For details of the Nbsf_Management_Discovery service operation refer to 3GPP TS 29.521 [22].

5.5.3.2 AF requests targeting an individual UE address

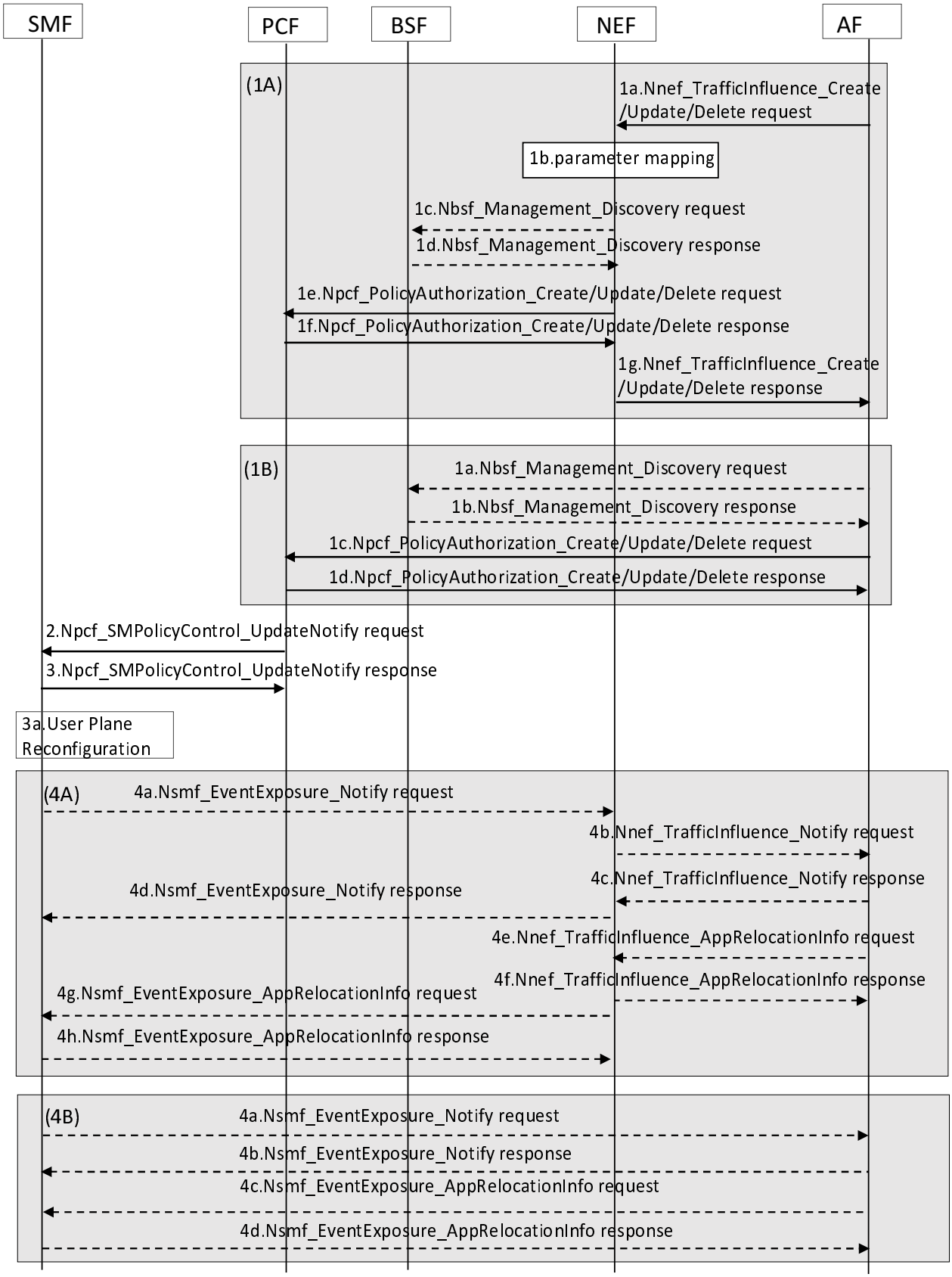


Figure 5.5.3.2-1: Processing AF requests to influence traffic routing for Sessions identified by an UE address

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 clause 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 clause 5.2.2.2.2.1. If the "URLLC" feature defined in 3GPP TS 29.514 [10] is supported, and the indication of AF acknowledgement was received from the AF request, the NEF forwards the indication to the PCF as described in 3GPP TS 29.514 [10]. If the "SimultConnectivity" feature defined in 3GPP TS 29.514 [10] is supported, and the indication of simultaneous temporary connectivity for source and target PSA, and, optionally, guidance about when the connectivity over the source PSA can be removed were received from the AF request, the NEF forwards the received indication(s) to the PCF as described in 3GPP TS 29.514 [10]. If the "EASDiscovery" feature defined in 3GPP TS 29.514 [10] is supported, and, the indication of the EAS rediscovery is received from the AF request, the NEF forwards the received indication to the PCF as described in 3GPP TS 29.514 [10]. If the "EASIPreplacement" feature defined in 3GPP TS 29.514 [10] is supported and the EAS IP replacement information is received in the AF request, the NEF forwards the received EAS IP replacement information to the PCF as described in 3GPP TS 29.514 [10].

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 clause 5.2.2.2.2.2. If the "URLLC" feature defined in 3GPP TS 29.514 [10] is supported, and the indication of AF acknowledgement was received from the AF request, the NEF forwards the indication to the PCF as described in 3GPP TS 29.514 [10]. If the "SimultConnectivity" feature defined in 3GPP TS 29.514 [10] is supported, and the indication of simultaneous temporary connectivity for source and target PSA, and, optionally, guidance about when the connectivity over the source PSA can be removed were received from the AF request, the NEF forwards the received indication(s) to the PCF as described in 3GPP TS 29.514 [10].

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 clause 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 clause 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 clause 5.2.2.2.2.1. If the "URLLC" feature defined in 3GPP TS 29.514 [10] is supported, the AF may provide an indication of AF acknowledgement to be expected as described in 3GPP TS 29.514 [10]. If the "SimultConnectivity" feature defined in 3GPP TS 29.514 [10] is supported, the AF may provide an indication of simultaneous temporary connectivity for source and target PSA, and, optionally, guidance about when the connectivity over the source PSA can be removed were received from the AF request to the PCF as described in 3GPP TS 29.514 [10]. If the "EASDiscovery" feature defined in 3GPP TS 29.514 [10] is supported, the AF may provide an indication of the EAS rediscovery to the PCF as described in 3GPP TS 29.514 [10]. If the "EASIPreplacement" feature defined in 3GPP TS 29.514 [10] is supported, the AF may provide the EAS IP replacement information to the PCF as described in 3GPP TS 29.514 [10]. If the "AF_latency" feature defined in 3GPP TS 29.514 [10] is supported, the AF may provide the maximum allowed user plane latency to the PCF as described in 3GPP TS 29.514 [10].

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 clause 5.2.2.2.2.2. If the "URLLC" feature defined in 3GPP TS 29.514 [10] is supported, the AF may

provide an indication of AF acknowledgement to be expected as described in 3GPP TS 29.514 [10]. If the "SimultConnectivity" feature defined in 3GPP TS 29.514 [10] is supported, the AF may provide an indication of simultaneous temporary connectivity for source and target PSA, and, optionally, guidance about when the connectivity over the source PSA can be removed were received from the AF request to the PCF as described in 3GPP TS 29.514 [10]. If the "EASDiscovery" feature defined in 3GPP TS 29.514 [10] is supported, the AF may provide an indication of the EAS rediscovery to the PCF as described in 3GPP TS 29.514 [10]. If the "EASIPreplacement" feature defined in 3GPP TS 29.514 [10] is supported, the AF may provide the EAS IP replacement information to the PCF as described in 3GPP TS 29.514 [10]. If the "AF_latency" feature defined in 3GPP TS 29.514 [10] is supported, the AF may provide the maximum allowed user plane latency to the PCF as described in 3GPP TS 29.514 [10].

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 clause 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 callback URI "{notificationUri}/update" as described in clause 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) , in addition, if the "URLLC" feature defined in 3GPP TS 29.512 [9] is supported, and the indication of AF acknowledgement was received from the AF request, the PCF includes within the PCC rule(s) the indication of AF acknowledgement to be expected as specified in 3GPP TS 29.512 [9]. If the "SimultConnectivity" feature defined in 3GPP TS 29.512 [9] is supported, and the indication of simultaneous temporary connectivity for source and target PSA, and, optionally, guidance about when the connectivity over the source PSA can be removed, were received from the AF request, the PCF includes within the PCC rule(s) the received indication(s) as specified in 3GPP TS 29.512 [9]. If the "EASDiscovery" feature defined in 3GPP TS 29.512 [9] is supported, and the indication of the EAS rediscovery was received in the AF request, the PCF includes within the PCC rule(s) the received indication as specified in 3GPP TS 29.512 [9]. If the "EASIPreplacement" feature defined in 3GPP TS 29.512 [9] is supported, and the EAS IP replacement information was received in the AF request, the PCF includes within the PCC rule(s) the received information as specified in 3GPP TS 29.512 [9]. If the "AF_latency" feature defined in 3GPP TS 29.512 [9] is supported, and the maximum allowed user plane latency was received, the PCF includes within the PCC rule(s) the received maximum allowed user plane latency as specified in 3GPP 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.

- 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.

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].

3a. When the SMF installs PCC rule successfully, the SMF determines whether UP path change needs to be enforced. In this case, the SMF:

- when early notification is required, shall notify as described in step 4 before reconfiguring the User Plane of the PDU session;

- takes appropriate actions to reconfigure the User plane of the PDU Session such as:

  i. adding, replacing or removing a UPF in the data path to e.g. act as an UL CL or a Branching Point;

  ii. allocate a new Prefix to the UE (when IPv6 multi-Homing applies);

  iii. updating the UPF in the target DNAI with new traffic steering rules;

  iv. using the received maximum allowed user plane latency to decide whether edge relocation is needed to ensure that the user plane latency does not exceed the value and whether to relocate the PSA UPF to satisfy the user plane latency

  v. (re)configure Local PSA for EAS IP address replacement if applicable;

  vi. establishing a temporary N9 forwarding tunnel between the source UL CL and target UL CL and, if the AF requested so, and "SimultConnectivity" is supported in the concerned interfaces, maintaining

simultaneous connectivity temporarily for the source and target PSA until the traffic ceases to exist for an AF indicated period of time or locally configured value; and

- when late notification is required, shall notify as described in step 4 after reconfiguring the User Plane of the PDU session.

If the "EASDiscovery" feature is supported, and if UP path is enforced and/or the indication of the EAS rediscovery was received, the SMF indicates to the UE to refresh the cached EAS information as defined in clause 6.3.2 of 3GPP TS 24.501 [20].

4A. In case of 1A, if the SMF observes PDU Session related event(s) that AF has subscribed to, the SMF sends notification to the AF via the NEF.

4a-4d. The SMF invokes Nsmf_EventExposure_Notify service operation 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. Notification Correlation ID to AF Transaction ID, etc.), and invokes the Nnef_TrafficInfluence_Notify service operation to forward the notification to the AF. If the indication of AF acknowledgement to be expected was included in the PCC rule(s), the SMF may notify with a notification URI for AF acknowledgement as described in 3GPP TS 29.508 [8], and then the NEF also notifies with a URI for the AF acknowledgement as described in 3GPP TS 29.522 [24].

4e-4h. When receiving the notification with the URI for AF acknowledgement, the AF acknowledges the notification to the SMF identified by the notification URI via the NEF. If the "EASIPreplacement" feature defined in 3GPP TS 29.522 [24] is supported, the AF may provide the EAS IP replacement information to the NEF. Then the NEF notifies the SMF of the EAS IP replacement information as described in 3GPP TS 29.508 [8] if the NEF determines that the SMF supports the "EASIPreplacement" featureas defined in 3GPP TS 29.508 [8]. The AF may provide an indication that buffering of uplink traffic to the target DNAI is needed to the NEF. Then the NEF notifies the SMF of indication as described in 3GPP TS 29.508 [8] if the NEF determines that the SMF supports the "ULBuffering" feature as defined in 3GPP TS 29.508 [8].

The step is the same as steps 7-14 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 sends notification to the AF directly.

4a-4b. The SMF invokes Nsmf_EventExposure_Notify service operation to the AF directly by sending an HTTP POST request to the callback URI "{notifUri}", and the AF sends a "204 No Content" response to the SMF. If the indication of AF acknowledgement to be expected was included in the PCC rule(s), the SMF may provide an URI for the AF acknowledgement as described in 3GPP TS 29.508 [8].

4c-4d. When receiving the notification with the URI for AF acknowledgement from the SMF, the AF invokes Nsmf_EventExposure_AppRelocationInfo service operation by sending an HTTP POST request to the callback URI "{ackUri}" to acknowledge the notification, and the SMF sends a "204 No Content" response to the AF. The AF may provide the EAS IP replacement information to the SMF as described in 3GPP TS 29.508 [8] if the AF determines that the SMF supports the "EASIPreplacement" feature as defined in 3GPP TS 29.508 [8].The AF may provide an indication that buffering of uplink traffic to the target DNAI is needed to the SMF as described in 3GPP TS 29.508 [8] if the AF determines that the SMF supports the "ULBuffering" feature as defined in 3GPP TS 29.508 [8].

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.

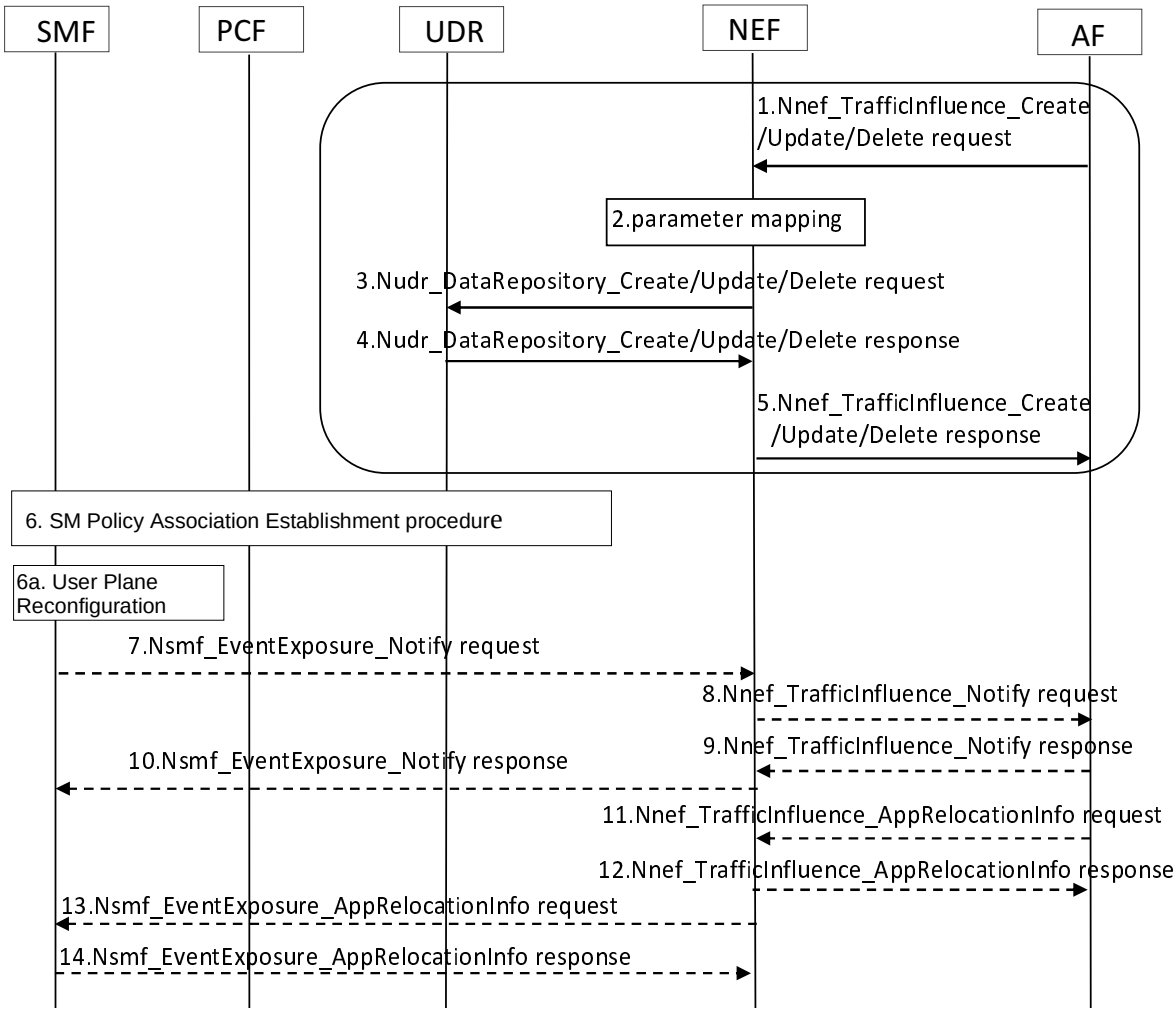


Figure 5.5.3.3-1: Processing AF requests to influence traffic routing for Sessions not identified by an UE address, affecting future PDU session

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. If the "URLLC" feature defined in 3GPP TS 29.522 [24] is supported, the AF may provide an indication of AF acknowledgement to be expected. If the "AF_latency" feature defined in 3GPP TS 29.522 [24] is supported, the AF may provide a maximum allowed user plane latency to ensure that the user plane latency in the 5GC does not exceed that value and to allow the SMF decide whether to relocate the PSA UPF to satisfy the user plane latency. If the "SimultConnectivity" feature defined in 3GPP TS 29.522 [24] is supported, the AF may provide the indication of simultaneous temporary connectivity for source and target PSA, and, optionally, guidance about when the connectivity over the source PSA can be removed.

   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. If the "URLLC" feature defined in 3GPP TS 29.522 [24] is supported, the AF may provide an indication of AF acknowledgement to be expected. If the "AF_latency" feature defined in 3GPP TS 29.522 [24] is supported, the AF may provide a maximum allowed user plane latency to ensure that the user plane latency in the 5GC does not exceed that value and to alow the SMF decide whether to relocate the PSA UPF to satisfy the user plane latency. If the "SimultConnectivity" feature defined in 3GPP TS 29.522 [24] is supported, the AF may provide the indication of simultaneous temporary connectivity for source and target PSA, and, optionally, guidance about when the connectivity over the source PSA can be removed.

   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.

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. If the "SimultConnectivity" feature defined in 3GPP TS 29.519 [12] is supported, and the indication of simultaneous temporary connectivity for source and target PSA, and, optionally, guidance about when the connectivity over the source PSA can be removed, were received from the AF request, the NEF includes within the creation request the received indication(s) as specified in 3GPP TS 29.519 [12]. If the "AF_latency" feature defined in 3GPP TS 29.519 [12] is supported, and the maximum allowed user plane latency was received from the AF request, the NEF includes within the creation request the received maximum allowed user plane latency as specified in 3GPP TS 29.519 [12].

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. If the "SimultConnectivity" feature defined in 3GPP TS 29.519 [12] is supported, and the indication of simultaneous temporary connectivity for source and target PSA, and, optionally, guidance about when the connectivity over the source PSA can be removed, were received from the AF request, the NEF includes within the update request the received indication(s) as specified in 3GPP TS 29.519 [12]. If the "AF_latency" feature defined in 3GPP TS 29.519 [12] is supported, and the maximum allowed user plane latency was received from the AF request, the NEF includes within the update request the received maximum allowed user plane latency as specified in 3GPP TS 29.519 [12].

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.

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 clause 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 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].

If the "SimultConnectivity" feature defined in 3GPP TS 29.512 [9] is supported, and the indication of simultaneous temporary connectivity for source and target PSA, and, optionally, guidance about when the connectivity over the source PSA can be removed, were stored in UDR, the PCF includes within the PCC rule(s) the received indication(s) as specified in 3GPP TS 29.512 [9].

If the "AF_latency" feature defined in 3GPP TS 29.512 [9] is supported, and the maximum allowed user plane latency was stored in UDR, the PCF includes within the PCC rule(s) the received maximum allowed user plane latency as specified in 3GPP TS 29.512 [9].

6a. This step is the same as the step 3a in Figure 5.5.3.2-1.

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 callback URI "{notifUri}". If the indication of AF acknowledgement to be expected was included in the PCC rule(s), the SMF may notify with an URI for the AF acknowledgement as described in 3GPP TS 29.508 [8].

8. When receiving the Nsmf_EventExposure_Notify service operation, the NEF performs information mapping (e.g. Notification Correlation 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 callback URI "notificationDestination" as specified in 3GPP TS 29.522 [24]. If the notification from the SMF includes an URI for the AF acknowledgement, the NEF also notifies with a URI for the AF acknowledgement as described in 3GPP 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 SMF.

11-12. When receiving the notification with the URI for AF acknowledgement from the NEF, the AF invokes Nnef_TrafficInfluence_AppRelocationInfo service operation by sending an HTTP POST request to the callback URI "{afAckUri}" to acknowledge the notification, and the NEF sends a "204 No Content" response to the AF. If the "ULBuffering" feature is supported, the AF may provide an indication that buffering of uplink traffic to the target DNAI is needed to the NEF.

13-14. When receiving the AF acknowledgement from the AF, to forward it to the SMF, the NEF invokes Nsmf_EventExposure_AppRelocationInfo service operation by sending an HTTP POST request to the callback URI "{ackUri}", and the SMF sends a "204 No Content" response to the NEF. If the NEF receives the indication that buffering of uplink traffic to the target DNAI is needed and the NEF determines that the SMF supports the "ULBuffering" feature as defined in 3GPP TS 29.508 [8], the NEF provides the indication that buffering of uplink traffic to the target DNAI is needed to the SMF.

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.

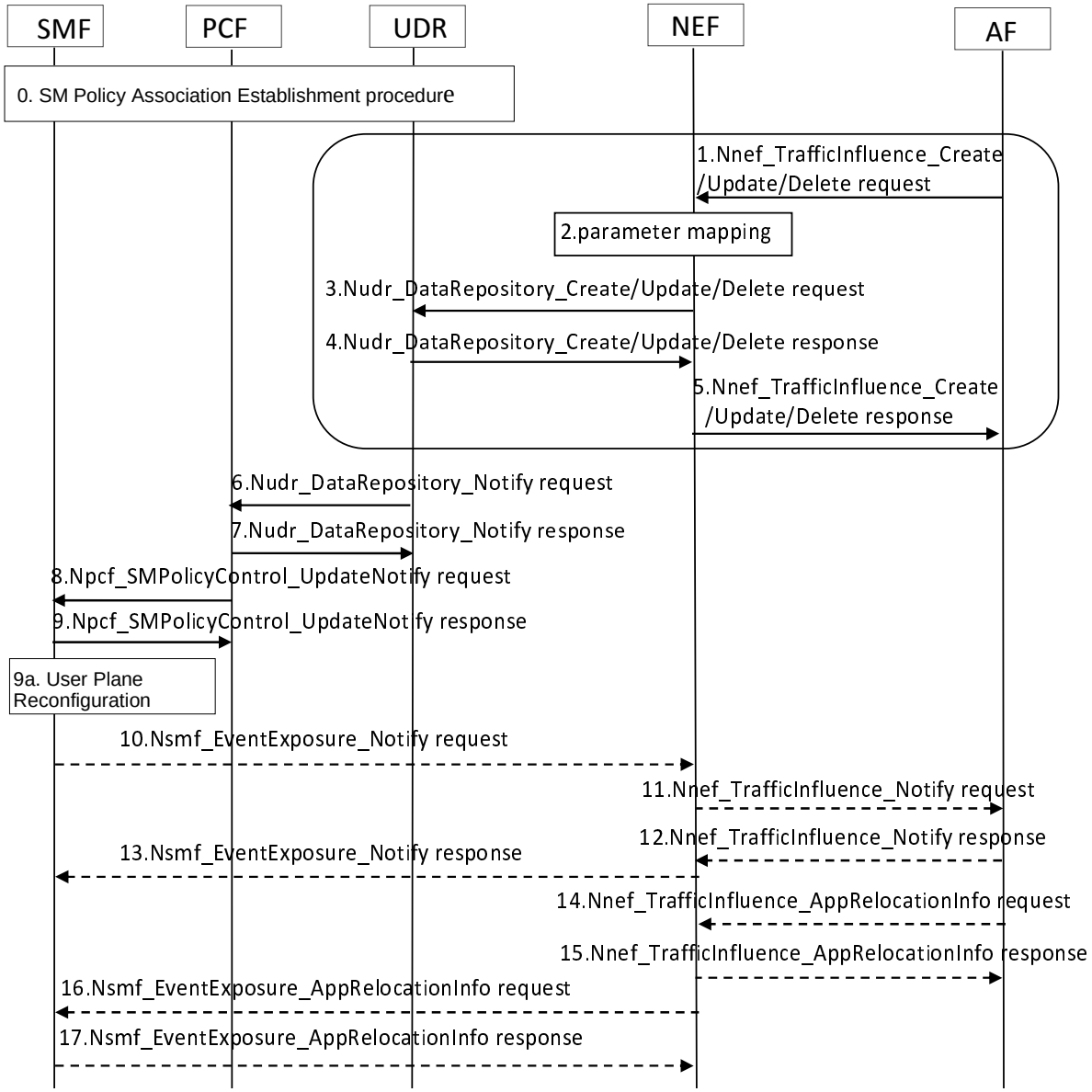


Figure 5.5.3.3-2: Processing AF requests to influence traffic routing for Sessions not identified by an UE address, affecting ongoing PDU session

0. The PCF subscribes to the changes of traffic influence data in the UDR during SM Policy Association establishment procedure (see clause 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 callback 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 callback URI "{notificationUri}/update" as described in clause 5.2.2.2.1.

If the AF subscribes to UP Path change event, the PCF includes the information on AF subscription to UP path change event 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].

If the "SimultConnectivity" feature defined in 3GPP TS 29.512 [9] is supported, and the indication of simultaneous temporary connectivity for source and target PSA, and, optionally, guidance about when the connectivity over the source PSA can be removed, were stored in UDR, the PCF includes within the PCC rule(s) the received indication(s) as specified in 3GPP TS 29.512 [9].

If the "AF_latency" feature defined in 3GPP TS 29.512 [9] is supported, and the maximum allowed user plane latency was stored in UDR, the PCF includes within the PCC rule(s) the received maximum allowed user plane latency as specified in 3GPP TS 29.512 [9].

9a. This step is the same as step 6a in Figure 5.5.3.3-1.

10-17. These steps are the same as steps 7-14 in Figure 5.5.3.3-1.

5.5.4 Negotiation for future background data transfer procedure

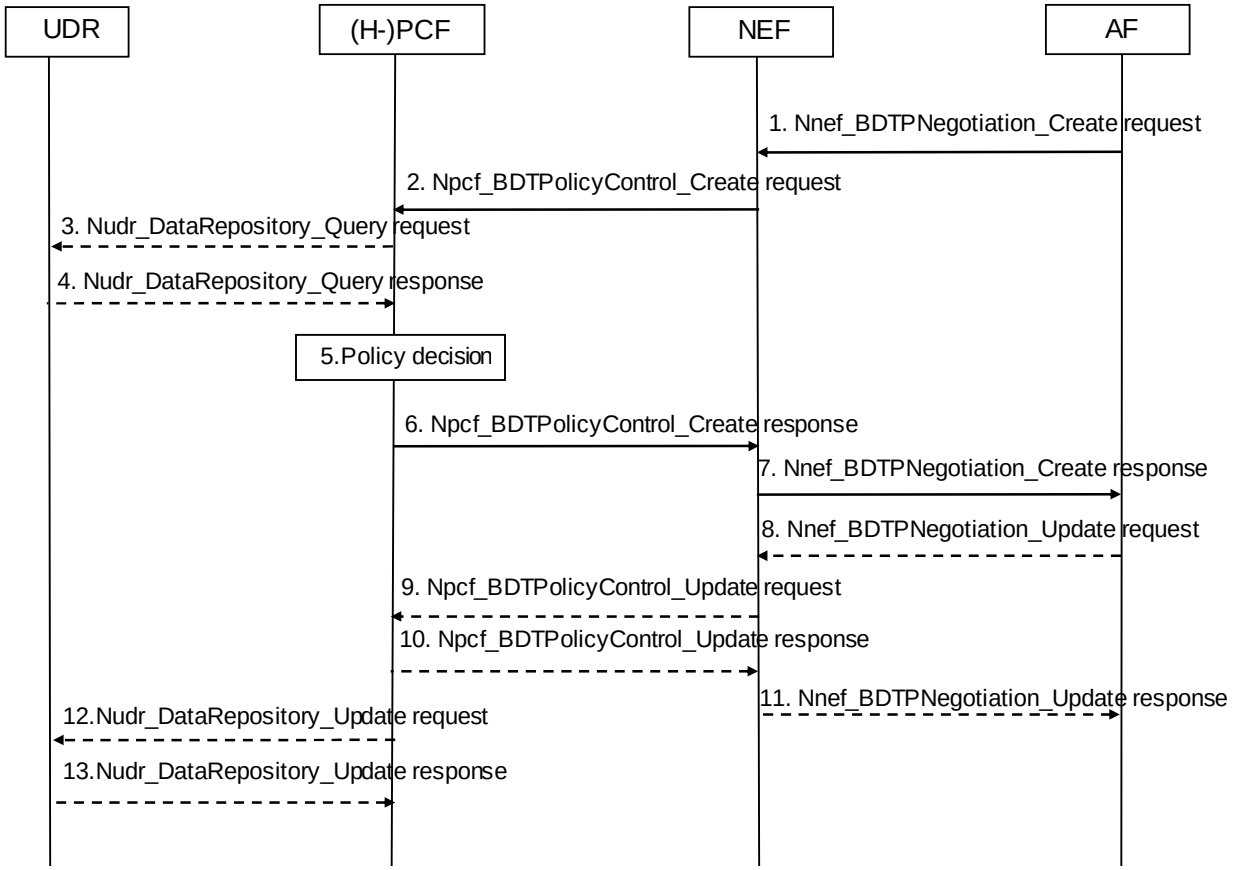


Figure 5.5.4-1: Negotiation for future background data transfer procedure

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.

   If the "BdtNotification_5G" feature defined in 3GPP TS 29.122 [34] is supported, the AF request may contain a notification URI to request the BDT warning notification.

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).

   If the AF requests the BDT warning notification in step 1, and if the "BdtNotification_5G" feature defined in 3GPP TS 29.544 [26] is supported, the NEF provides a notification URI to request the BDT warning notification correspondingly.

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, network performance information from the NWDAF 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].

5.5.5 BDT warning notification procedure

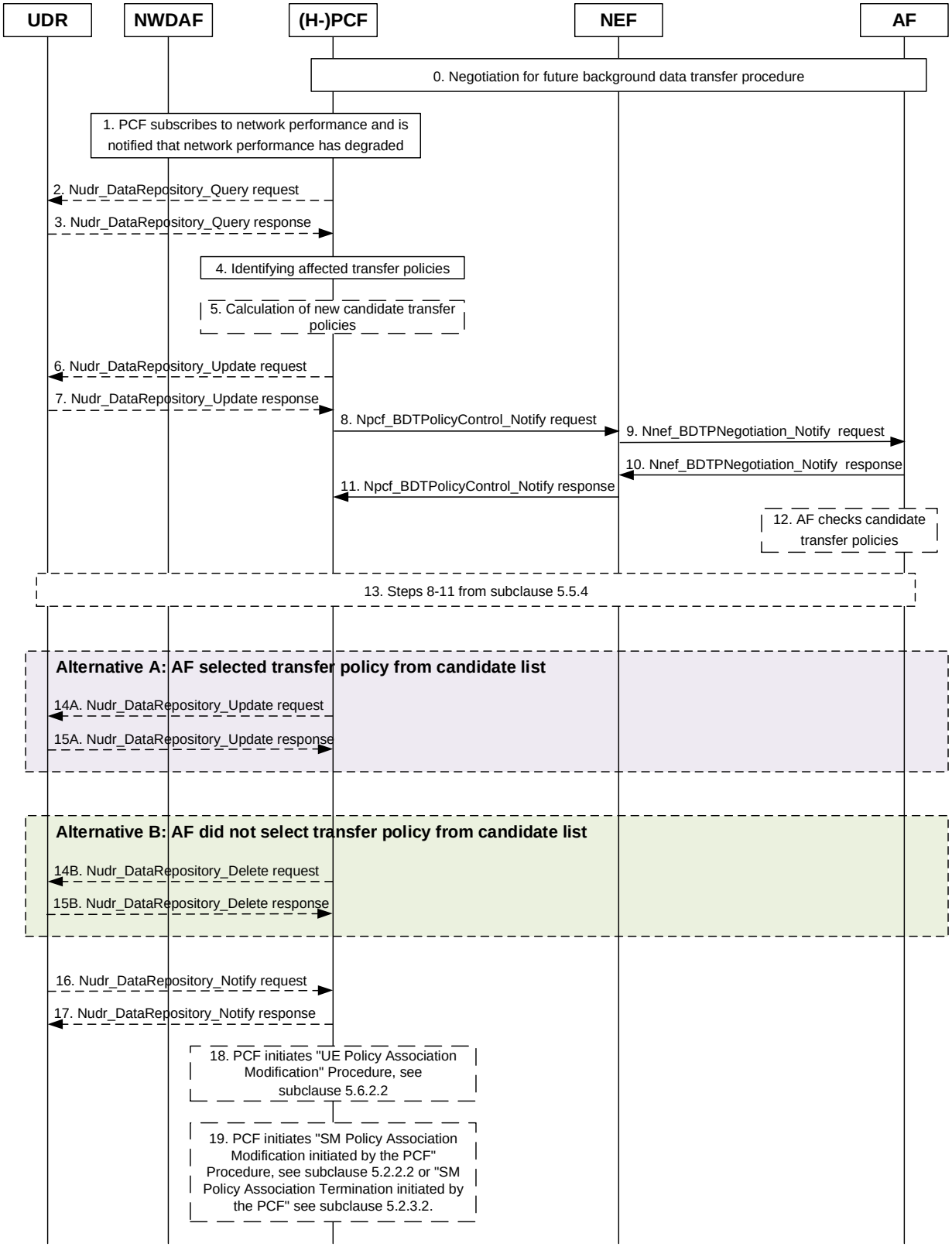


Figure 5.5.5-1: BDT warning notification procedure

0. The AF subscribes to BDT warning notification from the (H-)PCF via NEF during Negotiation for future background data transfer procedure (see clause 5.5.4).

1. The (H-)PCF subscribes to network performance from the NWDAF, and is notified when the network performance in the area of interest goes below the criteria from the NWDAF as described in clause 5.7.5 of 3GPP TS 29.552 [29552].

2-3. The (H-)PCF may invoke the Nudr_DataRepository_Query service operation by sending an HTTP GET request to the "BdtData" collection resource, to request from the UDR all stored transfer policies. The UDR sends an HTTP "200 OK" response to the (H-)PCF.

NOTE 1: If only one PCF is deployed in the network, transfer policies might be locally stored in the PCF and the interaction with the UDR is not required.

4. The (H-)PCF identifies the transfer policies that are affected by degradation of the network performance and for each affected transfer policy the (H-)PCF determines the ASP of which the background traffic will be influenced by the degradation of network performance and which requested the H-PCF to send the notification.

5. The (H-)PCF decides, based on operator policies, for each of the affected transfer policies whether a list of candidate transfer policies has to be calculated.

NOTE 2: If the (H-)PCF does not find any new candidate BDT policies, the previously negotiated BDT policy is kept and no interaction with the AF occurs i.e. steps 6 to 19 are not performed.

6-7. If the (H-)PCF stored the affected transfer policy in the UDR and one or more new candidate BDT policies are calculated, the (H-)PCF invokes the Nudr_DataRepository_Update service operation by sending an HTTP PATCH request to the resource "IndividualBdtData", to invalidate the affected background transfer policy in the UDR. The UDR sends an HTTP "200 OK" or "204 No Content" response to the (H-)PCF.

8. The (H-)PCF invokes the Npcf_BDTPolicyControl_Notify service operation by sending the HTTP POST request with the BDT warning notification to the Notification URI "{notifUri}".

   The BDT warning notification includes the BDT Reference ID of the impacted transfer policy and optionally the time window when the network performance will go below the criteria set by the operator, the network area where the network performance will go below the criteria set by the operator and the list of candidate transfer policies.

9. Upon the reception of the BDT warning notification from the (H-)PCF, the NEF invokes the Nnef_BDTPNegotiation_Notify service operation by sending the HTTP POST request with the BDT warning notification to the Notification URI "{notificationDestination}".

10. The AF sends an HTTP POST response to the NEF.

11. The NEF sends an HTTP POST response to the (H-)PCF.

12. When the AF receives the BDT warning notification, the AF checks new candidate background transfer policies.

13. If the AF selected one of the background transfer policies from the received candidate list or decided to indicate that none of the candidate background transfer policies is acceptable, steps 8 - 11 from clause 5.5.4 are executed with the exception that an indication that no background transfer policy is selected is included in the HTTP PATCH request if the AF did not select any of the background transfer policy.

14A-15A. If the AF selected one of the background transfer policies from the candidate list and if the (H-)PCF stored the affected transfer policy in the UDR, the (H-)PCF shall invoke the Nudr_DataRepository_Update service operation by sending an HTTP PATCH request to the resource "IndividualBdtData", to update the UDR with the selected candidate transfer policy. The UDR sends an HTTP "200 OK" or "204 No Content" response to the (H-)PCF.

14B-15B. If the AF did not select one of the background transfer policies from the candidate list and if the (H-)PCF stored the affected transfer policy in the UDR, the (H-)PCF shall invoke the Nudr_DataRepository_Delete service operation to remove the affected transfer policy from the UDR by sending the HTTP DELETE request to the "IndividualBdtData" resource. The UDR sends an HTTP "204 No Content" response to the (H-)PCF.

NOTE 3: If the AF did not invoke within an operator configurable time the Nnef_BDTPNegotiation_Update service operation to indicate if the one of the background transfer policies from the candidate list is selected or not, the (H-)PCF might remove the no longer valid BDT policy from UDR.

16-17. If the PCF subscribed to notification of "IndividualBDTdata" resource data changes in the UDR, i.e. the transfer policies are updated or deleted, the UDR invokes the Nudr_DataRepository_Notify service operation to the PCF by sending the HTTP POST request to the callback URI "{notificationUri}" as specified in 3GPP TS 29.519 [12].

NOTE 4: The PCF might be a different one than the PCF handling the BDT negotiation procedures, although in the figure it is represented as the same one for the simplification.

18. If the (H-)PCF identifies the URSP rules to UE need to be updated the (H-)PCF initiates the procedure "UE Policy Association Modification" defined in clause 5.6.2.2.2.

19. If the (H-)PCF identifies that:

- the PCC rules and/or session rules delivered to the SMF need to be updated the (H-)PCF initiates the procedure "SM Policy Association Modification initiated by the PCF" defined in clause 5.2.2.2; or

- the SM policy association needs to be terminated the (H-)PCF initiates the procedure "SM Policy Association Termination initiated by the PCF" defined in clause 5.2.3.2..

NOTE 5: For details of Nnef_BDTPNegotiation_Notify service operation refer to 3GPP TS 29.522 [24].

NOTE 6: For details of Npcf_BDTPolicyControl_Notify service operation refer to 3GPP TS 29.554 [26].

NOTE 7: For details of Nudr_DataRepository_Query/Update/Notify/Delete service operations refer to 3GPP TS 29.519 [12] and 3GPP TS 29.504 [27].

The AF can modify a BDT warning notification request indication as shown in figure 5.5.5-2.

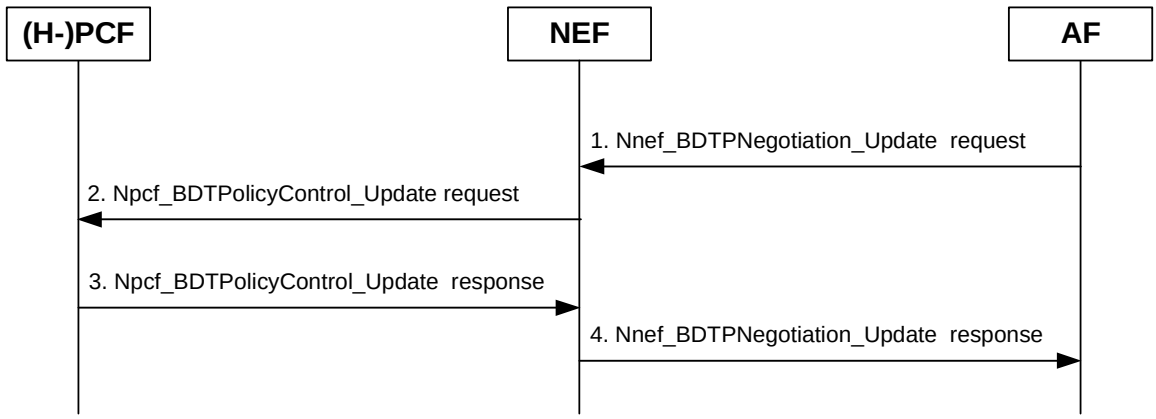


Figure 5.5.5-2: Modification of BDT warning notification request indication

1. If the AF decides to modify the BDT warning notification request, the AF invokes the Nnef_BDTPNegotiation_Update service operation by sending an HTTP PATCH request to the resource "Individual BDT Subscription".

2. The NEF invokes the Npcf_BDTPolicyControl_Update service operation by sending an HTTP PATCH request to the resource "Individual BDT policy". Based on the request from the AF, the NEF indicates to the (H-)PCF whether a BDT warning notification is enabled or disabled.

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

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

5.5.6 Background data transfer policy applying procedure

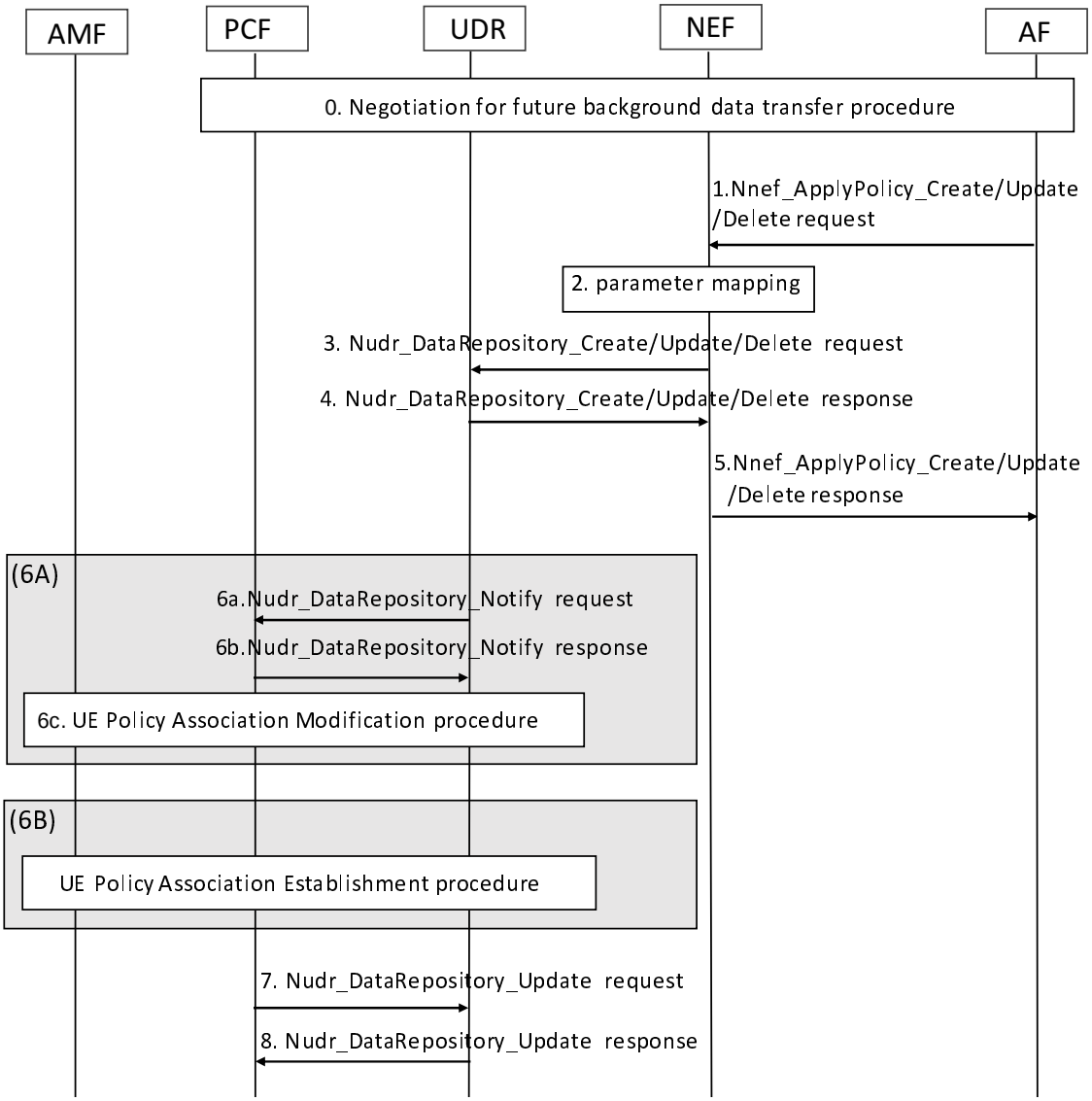


Figure 5.5.6-1: Background data transfer policy applying procedure

0. The AF negotiates policy for background data transfer during Negotiation for future background data transfer procedure (see clause 5.5.4).

1. To apply the negotiated Background Data Transfer Policy to UE or a group of UE, the AF invokes the Nnef_ApplyPolicy_Create service operation to the NEF by sending the HTTP POST request to the "Applied BDT Policy Subscriptions" resource.

   To update the applied policy, the AF invokes the Nnef_ApplyPolicy_Update service operation by sending the HTTP PATCH request to the "Individual Applied BDT Policy Subscription" resource.

   To remove the applied policy, the AF invokes the Nnef_ApplyPolicy_Delete service operation by sending the HTTP DELETE request to the "Individual Applied BDT Policy Subscription" resource.

NOTE 1: For details of Nnef_ApplyPolicy_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 23.502 [3].

3-4. When receiving the Nnef_ApplyPolicy_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 Applied BDT Policy Data" resource, and the UDR sends a "201 Created" response.

When receiving the Nnef_ApplyPolicy_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 request to the resource "Individual Applied BDT Policy Data", and the UDR sends a "200 OK" or "204 No Content" response.

When receiving the Nnef_ApplyPolicy_Delete request, t he 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 Applied BDT Policy Data" resource, and the UDR sends a "204 No Content" response.

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

6A. The PCF previously subscribed to the changes of Applied BDT Policy Data during UE Policy Association Establishment procedure (see clause 5.6.1.2).

6a. The UDR invokes the Nudr_DataRepository_Notify service operation to PCF(s) that have subscribed to the changes of Applied BDT Policy Data by sending the HTTP POST request to the callback URI "{notificationUri}".

6b. The PCF sends a "204 No Content" response to the UDR.

6c. The PCF initiates UE Policy Association Modification procedure (see clause 5.6.2.2.2) to send the background data transfer policy to the UE.

6B. The PCF retrieves the Applied BDT Policy Data in the UDR by invoking the Nudr_DataRepository_Query service operation and sends the background data transfer policy to the UE during UE Policy Association Establishment procedure (see clause 5.6.1.2).

7. The PCF invokes the Nudr_DataRepository_Update service operation to the UDR by sending the HTTP PATCH request to the "SessionManagementPolicyData" resource, to store the BDT reference ID(s) into the PDU session related policy data.

8. The UDR sends a "204 No Content" or "200 OK" response to the PCF.

NOTE 2: For details of the Nudr_DataRepository_Create/Update/Delete/Notify service operations refer to 3GPP TS 29.504 [27] and 3GPP TS 29.519 [12].

5.5.7 IPTV configuration provisioning

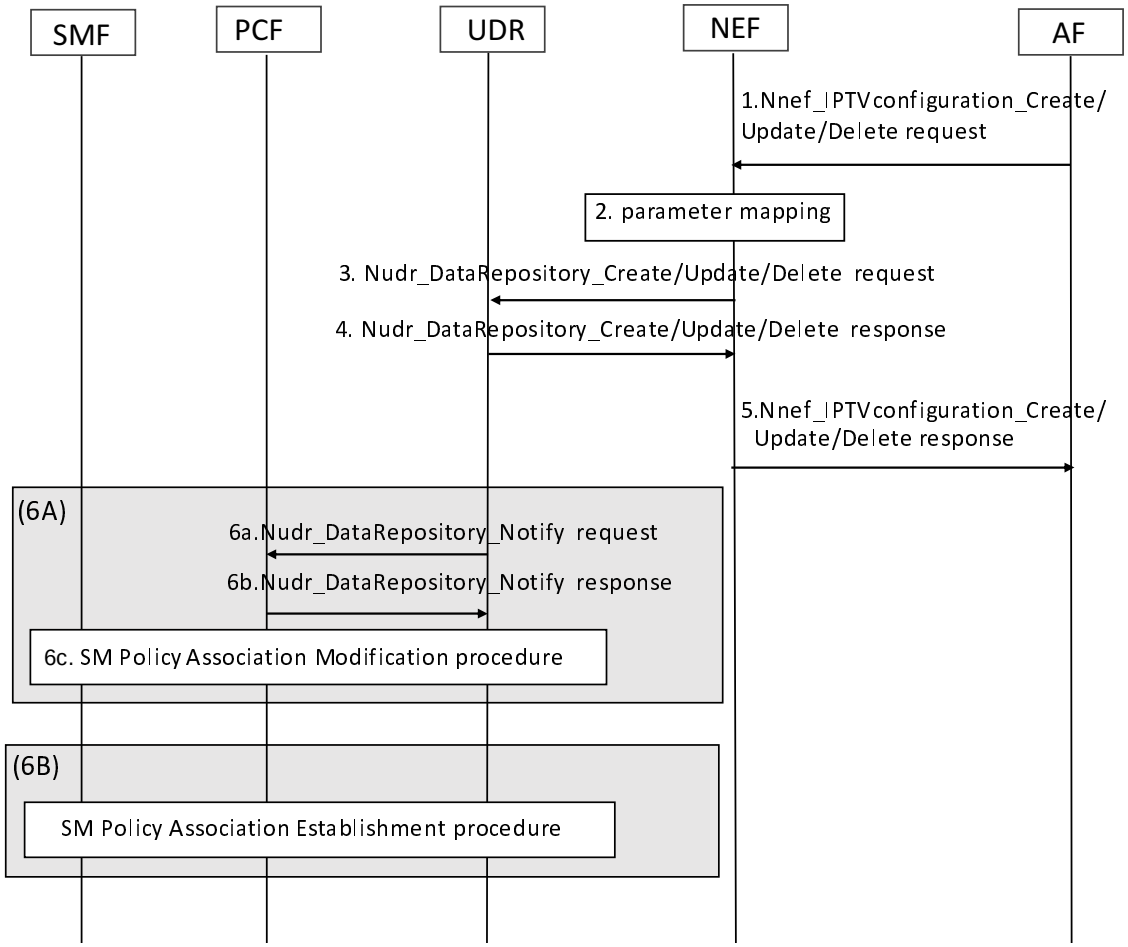


Figure 5.5.7-1: IPTV configuration provisioning procedure

1. To configure IPTV information to UE or a group of UE, the AF invokes the Nnef_IPTVconfiguration_Create service operation to the NEF by sending an HTTP POST request to the "IPTV Configurations" resource .

   To update an existing IPTV configuration, the AF invokes the Nnef_IPTVconfiguration_Update service operation by sending an HTTP PUT or PATCH request to the "Individual IPTV Configuration" resource.

   To remove an existing IPTV configuration, the AF invokes the Nnef_IPTVconfiguration_Delete service operation by sending an HTTP DELETE request to the "Individual IPTV Configuration" resource.

NOTE 1: For details of Nnef_IPTVconfiguration_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 23.502 [3].

3-4. When receiving the Nnef_IPTVconfiguration_Create request, the NEF invokes the Nudr_DataRepository_Create service operation to store the IPTV configuration in the UDR by sending the HTTP PUT request to the "Individual IPTV Configuration" resource, and the UDR sends a "201 Created" response.

   When receiving the Nnef_IPTVconfiguration_Update request, the NEF invokes the Nudr_DataRepository_Update service operation to modify the IPTV configuration in the UDR by sending the HTTP PUT/PATCH request to the resource "Individual IPTV Configuration", and the UDR sends a "200 OK" or "204 No Content" response.

When receiving the Nnef_IPTVconfiguration_Delete request, the NEF invokes the Nudr_DataRepository_Delete service operation to delete the IPTV configuration from the UDR by sending the HTTP DELETE request to the "Individual IPTV Configuration" resource, and the UDR sends a "204 No Content" response.

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

6A. The PCF previously subscribed to the changes of IPTV configuration during SM Policy Association Establishment procedure (see clause 5.2.1).

6a. The UDR invokes the Nudr_DataRepository_Notify service operation to PCF(s) that have subscribed to the changes of IPTV configuration by sending the HTTP POST request to the callback URI "{notificationUri}".

6b. The PCF sends a "204 No Content" response to the UDR.

6c. The PCF determines PCC rules based on the received IPTV configuration and initiates SM Policy Association Modification procedure (see clause 5.2.2.2.1).

6B. The PCF retrieves the IPTV configuration in the UDR by invoking the Nudr_DataRepository_Query service operation, determines PCC rules based on the retrieved IPTV configuration and send the PCC rules to the SMF during SM Policy Association Establishment procedure (see clause 5.2.1).

NOTE 2: For details of the Nudr_DataRepository_Create/Update/Delete/Notify service operations refer to 3GPP TS 29.504 [27] and 3GPP TS 29.519 [12].

5.5.8 AF-based service parameter provisioning

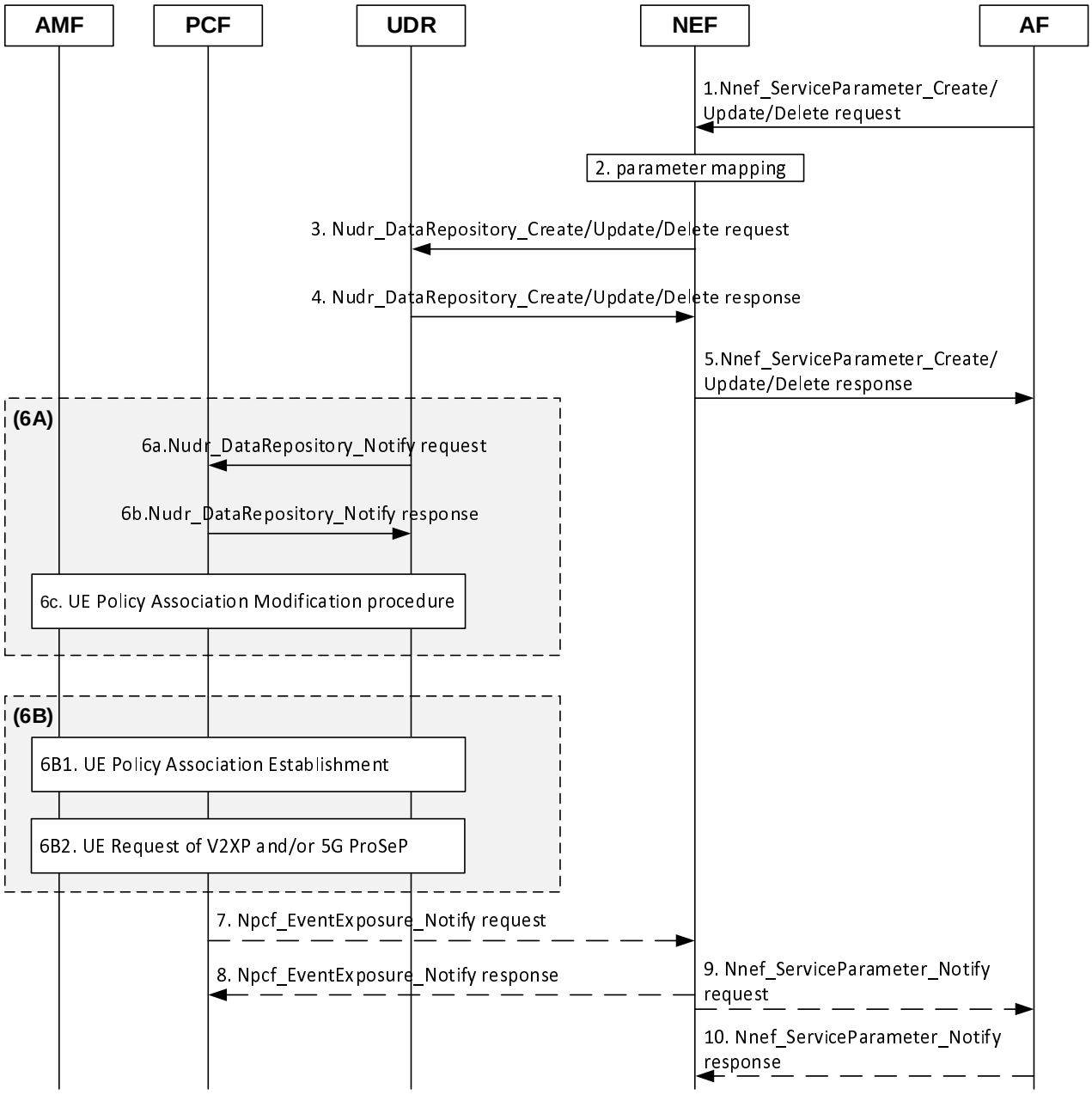


Figure 5.5.8-1: AF-based service parameter provisioning procedure

1. To provide service specific parameters (e.g. for URSP influence, V2X, or 5G ProSe) to a UE or a group of UEs, the AF invokes the Nnef_ServiceParameter_Create service operation to the NEF by sending an HTTP POST request to the "Service Parameter Subscriptions" resource.

   To update existing service specific parameters, the AF invokes the Nnef_ServiceParameter_Update service operation by sending an HTTP PUT or PATCH request to the concerned "Individual Service Parameter Subscription" resource.

   To remove existing service specific parameters, the AF invokes the Nnef_ServiceParameter_Delete service operation by sending an HTTP DELETE request to the concerned "Individual Service Parameter Subscription" resource.

   The request may include AF subscription information to the report of the outcome of UE Policy procedure.

NOTE 1: For further details on the Nnef_ServiceParameter_Create/Update/Delete service operations, refer to 3GPP TS 29.522 [24].

2. Upon reception of the AF request, the NEF authorizes it and then performs the mapping of the information provided by the AF into associated information needed by the 5GC (e.g. GPSI to SUPI), as described in 3GPP TS 23.502 [3]. The NEF may also support service specific authorization as described in clause 4.4.20 of 3GPP TS 29.522 [24].

3-4. When receiving the Nnef_ServiceParameter_Create request, the NEF invokes the Nudr_DataRepository_Create service operation to store the received service parameters in the UDR by sending an HTTP PUT request to the "Individual Service Parameter Data" resource, and the UDR replies with a "201 Created" response (if the processing of the request is successful).

When receiving the Nnef_ServiceParameter_Update request, the NEF invokes the Nudr_DataRepository_Update service operation to request the modification of the service parameters in the UDR by sending an HTTP PUT/PATCH request to the concerned "Individual Service Parameter Data" resource, and the UDR replies with a "200 OK" or "204 No Content" response (if the processing of the request is successful).

When receiving the Nnef_ServiceParameter_Delete request, the NEF invokes the Nudr_DataRepository_Delete service operation to request the deletion of the service parameters from the UDR by sending an HTTP DELETE request to the concerned "Individual Service Parameter Data" resource, and the UDR replies with a "204 No Content" response (if the processing of the request is successful).

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

6A. If the PCF(s) have previously subscribed to the changes of service parameters during the UE Policy Association Establishment procedure (see clause 5.6.1), then:

6a. The UDR invokes the Nudr_DataRepository_Notify service operation to the PCF(s) that have subscribed to the changes of service parameters by sending an HTTP POST request to the associated callback URI(s) "{notificationUri}";

6b. The PCF(s) send back "204 No Content" response(s) to the UDR; and

6c. The PCF(s) may derive UE policies (e.g. URSP, V2X, and/or 5G ProSe policies) based on the received service parameters from the UDR, UE subscription data, local operator policies, the previously received requested V2X/5G ProSe policies and UE capabilities (e.g., V2X capabilities) from the AMF, and initiate a UE Policy Association Modification procedure if applicable (see clause 5.6.2.2) to deliver the UE policies to the UE.

6B.

6B1 During UE Policy Association Establishment procedure (see clause 5.6.1), the PCF(s) retrieve the service parameters in the UDR by invoking the Nudr_DataRepository_Query service operation, determine UE policies (e.g. URSP, V2X, and/or 5G ProSe policies) based on the retrieved service parameters from the UDR, UE subscription data, local operator policies and UE capabilities (e.g. V2X capabilities and/or 5G ProSe capabilities) from the AMF , and if applicable, deliver the UE policies (including the determined V2XP and/or 5G ProSeP) to the UE and corresponding V2X N2 PC5 and/or ProSe N2 PC5 policy to the NG-RAN.

6B2. After registration, when the UE requests V2XP and/or 5G ProSeP, the AMF sends to the PCF an Namf_Communication_N1MessageNotify service operation with the requested V2XP and/or 5G ProSeP. The PCF retrieves the service parameter in the UDR by invoking the Nudr_DataRepository_Query service operation, determines V2XP and/or 5G ProSeP based on the retrieved service parameter from the UDR, the received requested V2XP and/or 5G ProSeP, UE subscription data, local operator policies and the UE capabilities (e.g., V2X capabilities and/or ProSe capabilities) previously received from the AMF, and delivers the V2XP and/or 5G ProSeP to the UE and the corresponding V2X N2 PC5 and/or ProSe N2 PC5 policy to the NG-RAN.

NOTE 2: For further details on the Nudr_DataRepository_Create/Update/Delete/Notify service operations, refer to 3GPP TS 29.504 [27] and 3GPP TS 29.519 [12].

7. If the AF subscribed to notifications about the outcome of UE Policies delivery (provision/update/removal) due to Service specific parameter provisioning and the PCF derived the corresponding UE policies, the PCF invokes

the Npcf_EventExposure_Notify service operation to inform the NEF about the outcome of the procedure by sending the HTTP POST request to the callback URI "{notifUri}".

NOTE 3: The Callback URI "{notifUri}" is used for both implicit and explicit subscriptions as described in 3GPP TS 29.523 [49]. Notification URI for implicit subscriptions is retrieved from UDR as described in 3GPP TS 29.519 [12].

8. The NEF sends back "204 No Content" response to the PCF.

9. When the NEF receives Npcf_EventExposure_Notify, the NEF performs information mapping as described in 3GPP TS 29.522 [24] and triggers the appropriate Nnef_ServiceParameter_Notify message.

10. The AF sends back an HTTP response message to the NEF to acknowledge the notification.

5.5.9 QoS monitoring procedure

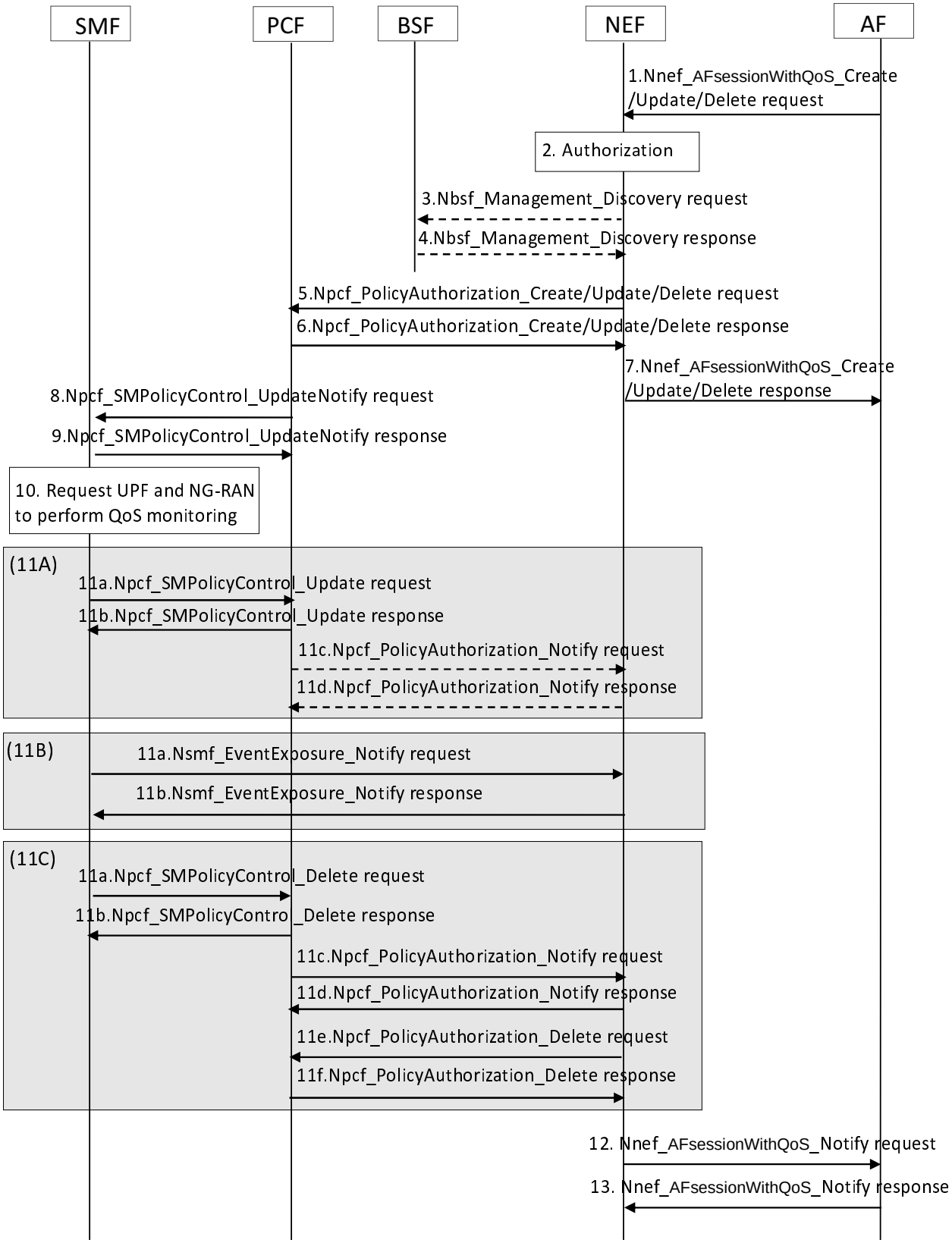


Figure 5.5.9-1: QoS monitoring procedure

1. The AF subscribes to or unsubscribes from the QoS monitoring notification from the PCF via the NEF.

   To create a subscription to the QoS monitoring information, the AF invokes the Nnef_AFsessionWithQoS_Create service operation to the NEF by sending the HTTP POST request to the "AS Session with Required QoS Subscriptions" resource. If the feature "ExposureToEAS" is supported, the AF may request the direct event notification from the UPF.

   To modify an existing subscription to the QoS monitoring information, the AF invokes the Nnef_AFsessionWithQoS_Update service operation by sending the HTTP PUT or PATCH request to the "Individual AS Session with Required QoS Subscription" resource.

   To remove a subscription to QoS monitoring information, the AF invokes the Nnef_AFsessionWithQoS_Delete service operation by sending the HTTP DELETE request to the "Individual AS Session with Required QoS Subscription" resource.

2. Upon receipt of the AF request, the NEF authorizes it.

3-4. 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 clause 8.5.4, to obtain the selected PCF ID for the ongoing PDU session identified by the individual UE address in the AF request.

5-6. The NEF forwards the AF request to the PCF.

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

   When receiving the Nnef_AFsessionWithQoS_Update request in step 1, 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 clause 5.2.2.2.2.2.

   When receiving the Nnef_AFsessionWithQoS_Delete request in step 1, 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 clause 5.2.2.2.2.3.

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

8. 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 callback URI "{notificationUri}/update" as described in clause 5.2.2.2.1.

   If the AF subscribes to QoS monitoring event, the PCF includes the related QoS monitoring information within the corresponding PCC rule(s).

   If the PCF determines that the QoS monitoring event notification shall be sent to the NEF via the PCF, the PCF provides the "QOS_MONITORING" policy control request trigger if not previously provided, as specified in 3GPP TS 29.512 [9].

   If the PCF determines that the QoS monitoring event notification shall be sent to the NEF directly from the SMF, the PCF includes the notification URI pointing to the NEF within the "notifyUri" attribute, the notification and the correlation id assigned by the NEF within the "notifyCorreId" attribute, as specified in 3GPP TS 29.512 [9].

   When the feature "ExposureToEAS" is supported and if the PCF received from the NEF the indication of direct QoS monitoring event notification, the PCF includes the notification URI pointing to the NEF within the "notifyUri" attribute, the notification correlation id assigned by the NEF within the "notifyCorreId" attribute and the indication of direct QoS monitoring event notification within the "directNotifInd" attribute, if available, as specified in 3GPP TS 29.512 [9]. The PCF may also determine that duplicated notification is required, i.e. both direct notification to the NEF (i.e. sent from UPF) and notification to the PCF is required, as specified in 3GPP TS 23.548 [57]. In this case, the PCF also provides the "QOS_MONITORING" policy control request trigger if not previously provided, as specified in 3GPP TS 29.512 [9].

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

9. The SMF sends an HTTP 200 OK response message to the PCF.

10. When the SMF receives the PCC rule, the SMF shall send a QoS Monitoring request to the UPF and NG-RAN as defined in 3GPP TS 29.512 [9].

    When the SMF receives the indication of direct QoS monitoring event notification within the PCC rule, the SMF shall send to the UPF the request to report directly to the NEF the QoS monitoring events. When the NEF receives the QoS monitoring report from the UPF as specified in 3GPP TS 29.564 [56], the NEF invokes the Nnef_AFsessionWithQoS_Notify service operation as described in steps 12-13.

11A. In case in step 8 the PCF determines that the notification shall be sent to the PCF:

    11a-11b. Upon receipt of the QoS monitoring report from the UPF, the SMF invokes the Npcf_SMPolicyControl_Update service operation to the PCF by sending an HTTP POST request to the "Individual SM Policy" resource. The PCF sends an HTTP POST response to the SMF.

    11c-11d. Upon receipt of the QoS monitoring event notification from the SMF, the PCF checks whether the notification needs to be sent to the NEF as described in 3GPP TS 29.512 [9], clause 4.2.3.25, and in that case, the PCF invokes the Npcf_PolicyAuthorization_Notify service operation to forward the notification to the NEF by sending the HTTP POST request to the callback URI "{notifUri}/notify". The NEF sends an HTTP POST response to the PCF. Otherwise, these steps do not apply.

11B. In case in step 8 the PCF determines that the notification shall be sent to the NEF directly from the SMF:

11a-11b. Upon receipt of the QoS monitoring report from the UPF, the SMF invokes Nsmf_EventExposure_Notify service operation to forward the notification to the NEF by sending an HTTP POST request to the callback URI "{notifUri}" received in step 8. The NEF sends an HTTP POST response to the SMF.11C.If the AF indicated to be notified of QoS Monitoring at PDU Session termination:

    11a-11b. When the PDU Session is terminated, 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, and report the QoS monitoring information if received from the UPF. The PCF sends an HTTP POST response to the SMF.

    11c-11d. The PCF invokes the Npcf_PolicyAuthorization_Notify service operation by sending the HTTP POST request to the callback URI "{notifUri}/terminate" to trigger the AF to request the application session context termination via the NEF. The NEF sends an HTTP POST response to the PCF.

    11e. The NEF invokes the Npcf_PolicyAuthorization_Delete service operation by sending the HTTP POST request to the "Individual Application Session Context" resource.to delete the application session.

    11f. The PCF removes the AF application session context and sends an HTTP POST response to the NEF with the QoS monitoring information received in step 11a.

12-13. Upon receipt of the QoS monitoring information in step 11, the NEF invokes the Nnef_AFsessionWithQoS_Notify service operation to forward the QoS monitoring information to the AF.

NOTE 1: For details of Nnef_AFsessionWithQoS_Create/Update/Delete/Notify service operations refer to 3GPP TS 29.122 [34].

NOTE 2: For details of the Npcf_PolicyAuthorization_Create/Update/Delete/Notify service operations refer to 3GPP TS 29.514 [10].

NOTE 3: For details of the Npcf_SMPolicyControl_UpdateNotify/Update/Delete service operations refer to 3GPP TS 29.512 [9].

NOTE 4: For details of the Nbsf_Management_Discovery service operation refer to 3GPP TS 29.521 [22].

NOTE 5: For details of the Nsmf_EventExposure_Notify service operation refer to 3GPP TS 29.508 [8].

5.5.10 AF-triggered dynamically changing AM policies

5.5.10.1 General

As described in clause 6.1.2.6 of 3GPP TS 23.503 [4], an AF may send requests to influence Access and Mobility related policies of a UE. The AF may also provide in its request subscriptions to events (e.g. related to service area coverage changes).

The following cases are included in this clause:

- AF requests targeting an individual UE without conditions related to the application traffic: these requests are routed (by the AF or by the NEF) to the PCF for the UE as described in clause 5.5.10.2.
- AF requests targeting an individual UE, a group of UEs, any UE accessing a combination of DNN and S-NSSAI, or all UEs using a specific application. For such requests the AF shall contact the NEF and the NEF stores the AF request information in the UDR. The PCF(s) for the UE receive a corresponding notification if they had subscribed to the creation / modification / deletion of the AF request information corresponding to the respective UDR Data Keys / Data Sub-Keys. This case is described in clause 5.5.10.3.

This clause applies to non-roaming, i.e. to cases where the PCF, AF, AMF and SMF belong to the Serving PLMN or AF belongs to a third party with which the Serving PLMN has an agreement.

5.5.10.2 Access and Mobility policy authorization requests targeting an individual UE

This procedure concerns only non-roaming scenarios, i.e. to cases where the involved entities serving the UE (i.e. NEF, PCF, BSF, AMF) belong to the home PLMN. The AF may belong to the home PLMN (trusted AF) or to a third party (untrusted AF).

This procedure is used for individual UEs when the request shall be applied independently of conditions related to the application traffic. The AF may interact with NFs of the Core Network either directly or via the NEF. The procedure for the NEF-mediated case is described in Figure 5.5.10.2-1, while the procedure for the direct case is described in Figure 5.5.10.2-2.

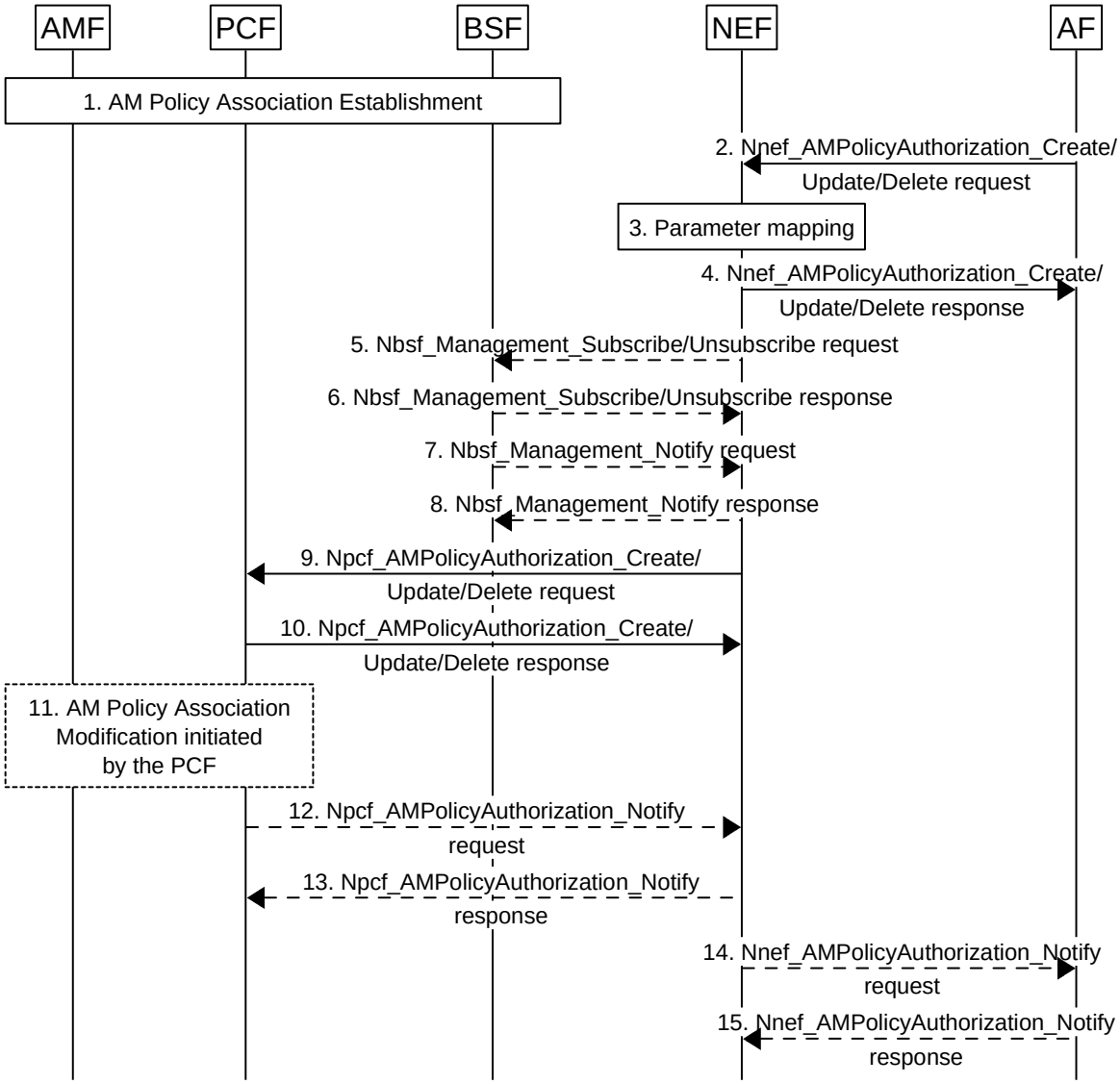


Figure 5.5.10.2-1: Processing NEF-mediated AF requests for Access and Mobility related policy authorization for a UE

1. An AM Policy Association is established as described in clause 5.1.1. This step can occur at any time before step 7.

2. To create a new AF request, the AF invokes the Nnef_AMPolicyAuthorization_Create service operation to the NEF by sending an HTTP POST request to the "Application AM Contexts" resource as described in clause 4.4.26.2 of 3GPP TS 29.522 [24].

   To update an existing AF request, the AF invokes the Nnef_AMPolicyAuthorization_Update service operation by sending an HTTP PATCH request to the "Individual Application AM Context" resource as described in clause 4.4.26.3 of 3GPP TS 29.522 [24].

   To remove an existing AF request, the AF invokes the Nnef_AMPolicyAuthorization_Delete service operation by sending an HTTP DELETE request to the "Individual Application AM Context" resource as described in clause 4.4.26.4 of 3GPP TS 29.522 [24].

3. Upon receipt of the AF request, the NEF authorizes it, stores it, and performs the mapping from the information provided by the AF into information needed by the 5GC (e.g. translate a GPSI into a SUPI) as described in 3GPP TS 23.501 [2] and 3GPP TS 23.502 [3].

4. The NEF responds to the AF request creation, update, or deletion as described respectively in clauses 4.4.26.2, 4.4.26.3, or 4.4.26.4 of 3GPP TS 29.522 [24].

If the creation or update request included the subscription to event(s) together with the indication of immediate reporting of the currently available values of the subscribed events, the NEF includes in the response the applicable event(s) information, if available, as specified in clauses 4.4.26.2, or 4.4.26.4 of 3GPP TS 29.522 [24]. In this case, the response is deferred after step 10.

5. The NEF may subscribe to (or unsubscribe from) the BSF using Nbsf_Management_Subscribe (or Nbsf_Management_Unsubscribe) to be informed about the PCF for a UE of the UE targeted in the AF request received in step 2, as described in clause 4.2.6 (for subscribing) or clause 4.2.7 (for unsubscribing) of 3GPP TS 29.521 [22].

6. The BSF responds by confirming the received request and, in the case of subscription, including the existing PCF for a UE registration in the response, if found, as described in clause 4.2.6.2 of 3GPP TS 29.521 [22].

7. The BSF notifies the NEF once there is a PCF for a UE registration for the UE indicated in the subscription as described in clause 4.2.8 of 3GPP TS 29.521 [22].

8. The NEF confirms the received notification by sending a "204 No Content" response as described in clause 4.2.8 of 3GPP TS 29.521 [22].

9. The NEF forwards the AF request to the PCF.

   If the NEF received the Nnef_AMPolicyAuthorization_Create request in step 2, the NEF invokes the Npcf_AMPolicyAuthorization_Create service operation by sending an HTTP POST request to the "Application AM Contexts" resource as described in clause 4.2.2 of 3GPP TS 29.534 [50].

   If the NEF received the Nnef_AMPolicyAuthorization_Update request in step 2, the NEF invokes the Npcf_AMPolicyAuthorization_Update service operation by sending an HTTP PATCH request to the "Individual Application AM Context" resource as described in clause 4.2.3 of 3GPP TS 29.534 [50].

   If the NEF received the Nnef_AMPolicyAuthorization_Delete request in step 2, the NEF invokes the Npcf_AMPolicyAuthorization_Delete service operation by sending an HTTP DELETE request to the "Individual Application AM Context" resource as described in clause 4.2.4 of 3GPP TS 29.534 [50].

10. The PCF responds to the creation, update, or deletion request as described respectively in clauses 4.2.2, 4.2.3, or 4.2.4 of 3GPP TS 29.534 [50].

    If the creation or update request included the subscription to event(s) together with the indication of immediate reporting of the currently available values of the subscribed events, the PCF includes in the response the applicable event(s) information, if available, as specified respectively in clauses 4.2.2 or 4.2.3 of 3GPP TS 29.534 [50].

11. AM Policy Association modification initiated by the PCF may be performed as described in clause 5.1.2.2.

12-13. If an event (e.g. service coverage area change) occurs to which the NEF has previously subscribed, the PCF notifies the NEF using the Npcf_AMPolicyAuthorization_Notify service operation by sending an HTTP POST request to the callback URI included in the subscription, and the NEF responds by sending a confirmation, as described in clause 4.2.7 of 3GPP TS 29.534 [50].

14-15. When the NEF receives from the PCF an event (e.g. service coverage area change) to which the AF has previously subscribed, the NEF notifies the AF using the Nnef_AMPolicyAuthorization_Notify service operation by sending an HTTP POST request to the callback URI included in the subscription, and the AF responds by sending a confirmation, as described in clause 4.4.26.7 of 3GPP TS 29.522 [24].

NOTE: The subscriptions required for steps 12-15 can have happened either in the Create/Update steps or with a separate Subscribe message which is not shown in the call flow.

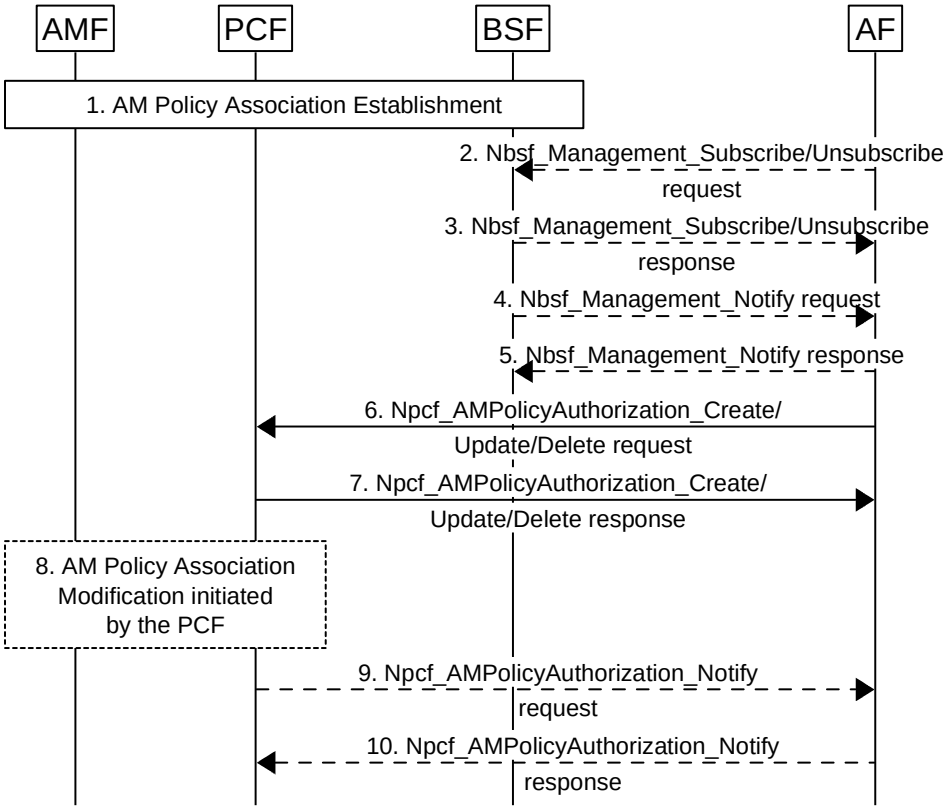


Figure 5.5.10.2-2: Processing direct AF requests for Access and Mobility related policy authorization for a UE

1. An AM Policy Association is established as described in clause 5.1.1. This step can occur at any time before step 4.

2. The AF may subscribe to (or unsubscribe from) the BSF using Nbsf_Management_Subscribe (or Nbsf_Management_Unsubscribe) to be informed about PCF for a UE registrations for the target UE, as described in clause 4.2.6 (for subscribing) or clause 4.2.7 (for unsubscribing) of 3GPP TS 29.521 [22].

3. The BSF responds by confirming the received request and, in the case of subscription, including the existing PCF for a UE registration in the response, if found, as described in clause 4.2.6.2 of 3GPP TS 29.521 [22].

4. The BSF notifies the AF once there is a PCF for a UE registration for the UE indicated in the subscription as described in clause 4.2.8 of 3GPP TS 29.521 [22].

5. The AF confirms the received notification by sending a "204 No Content" response as described in clause 4.2.8 of 3GPP TS 29.521 [22].

6. To create a new AF request, the AF invokes the Npcf_AMPolicyAuthorization_Create service operation by sending an HTTP POST request to the "Application AM Contexts" resource as described in clause 4.2.2 of 3GPP TS 29.534 [50].

   To update an existing AF request, the AF invokes the Npcf_AMPolicyAuthorization_Update service operation by sending an HTTP PATCH request to the "Individual Application AM Context" resource as described in clause 4.2.3 of 3GPP TS 29.534 [50].

   To remove an existing AF request, the AF invokes the Npcf_AMPolicyAuthorization_Delete service operation by sending an HTTP DELETE request to the "Individual Application AM Context" resource as described in clause 4.2.4 of 3GPP TS 29.534 [50].

7. The PCF responds to the creation, update, or deletion request as described respectively in clauses 4.2.2, 4.2.3, or 4.2.4 of 3GPP TS 29.534 [50].

   If the creation or update request included the subscription to event(s) together with the indication of immediate reporting of the currently available values of the subscribed events, the PCF includes in the response the

applicable event(s) information, if available, as specified respectively in clauses 4.2.2 or 4.2.3 of 3GPP TS 29.534 [50].

8. AM Policy Association modification initiated by the PCF may be performed as described in clause 5.1.2.2.

9-10. When an event (e.g. service coverage area change) occurs to which the AF has previously subscribed, the PCF notifies the AF using the Npcf_AMPolicyAuthorization_Notify service operation by sending an HTTP POST request to the callback URI included in the subscription, and the AF responds by sending a confirmation, as described in clause 4.2.7 of 3GPP TS 29.534 [50].

NOTE: The subscriptions required for steps 9-10 can have happened either in the Create/Update steps or with a separate Subscribe message which is not shown in the call flow.

5.5.10.3 AF requests to influence AM policies

This procedure concerns only non-roaming scenarios, i.e. to cases where the involved entities serving the UE (i.e. NEF, UDR, PCF, BSF, AMF) belong to the home PLMN. The AF may belong to the home PLMN (trusted AF) or to a third party (untrusted AF).

This procedure is used by the AF to provide its AM policy related request for one or multiple UEs at any time.

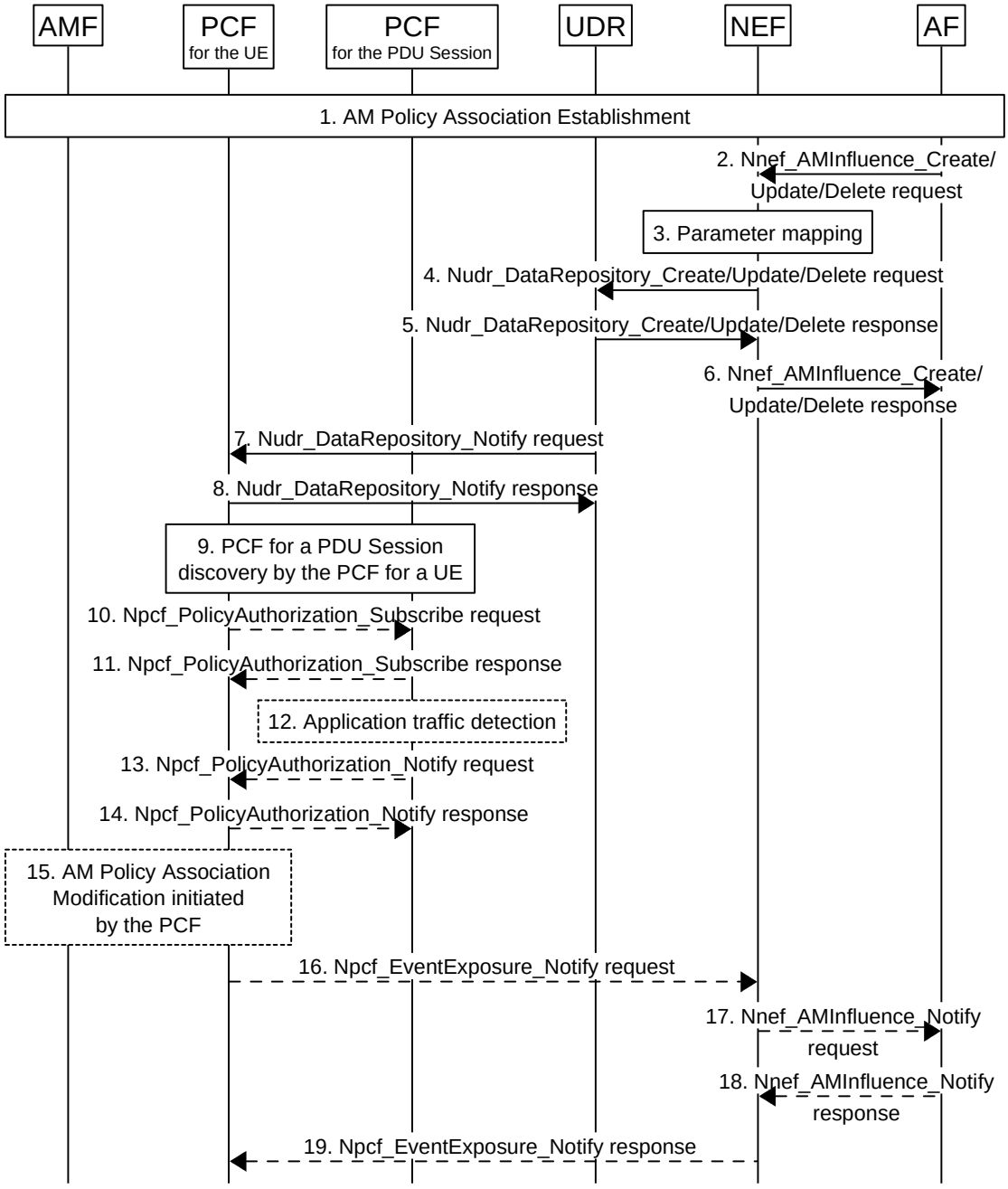


Figure 5.5.10.3-1: Processing AF requests to influence Access and Mobility related policy

1. An AM Policy Association is established as described in clause 5.1.1 (including the retrieval of and subscription to AM Influence data in steps 2 and 4). This step may occur at any time before step 7.

2. To create a new AF request, the AF invokes the Nnef_AMInfluence_Create service operation to the NEF by sending an HTTP POST request to the "AM Influence Subscription" resource. The AF may subscribe to Access and Mobility management related events (e.g. about service area coverage change outcome) as part of this operation.

   To update an existing AF request, the AF invokes the Nnef_AMInfluence_Update service operation by sending an HTTP PUT or PATCH request to the "Individual AM Influence Subscription" resource. The AF may subscribe to or unsubscribe from Access and Mobility management related events (e.g. about service area coverage change outcome) as part of this operation.

   To remove an existing AF request, the AF invokes the Nnef_AMInfluence_Delete service operation by sending an HTTP DELETE request to the "Individual AM Influence Subscription" resource. The AF may unsubscribe from Access and Mobility management related events (e.g. about service area coverage change outcome) as part of this operation.

3. 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 (e.g. translate a GPSI into a SUPI) as described in clause 4.4.27 of 3GPP TS 29.522 [24].

4-5. When receiving the Nnef_AMInfluence_Create request, the NEF invokes the Nudr_DataRepository_Create service operation to store the AF request information in the UDR by sending an HTTP PUT request to the "Individual AM Influence Data" resource, and the UDR sends a "201 Created" response.

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

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

6. The NEF sends an HTTP response message to the AF correspondingly.

7-8. The UDR notifies the PCF(s) that have subscriptions (from step 1) which match the received AF request using the Nudr_DataRepository_Notify service operation by sending an HTTP POST request to the callback URI of the PCF that was included in the subscription, and the PCF(s) send a "204 No Content" response.

9. If the received AM Influence data indicated that the AM policy depends on PDU session traffic events (e.g. the application start and application stop for an application Id or PDU session establishment and termination for a DNN and S-NSSAI combination), the PCF for the UE may discover the PCF(s) for a PDU Session that handle(s) the respective UE traffic as described in clause 8.4a.

10-11. If the received AM Influence data indicated that the request is dependent (or does not depend anymore) on the existence of UE traffic that matches one or more application identifiers and the feature "ApplicationDetectionEvents" defined in 3GPP TS 29.514 [10] is supported, the PCF for the UE may subscribe (or unsubscribe) to the PCF(s) for the PDU Session for notifications about application traffic detection (e.g. start, stop) of the application(s) indicated in the AM Influence data using the Npcf_PolicyAuthorization_Subscribe service operation as described in 3GPP TS 29.514 [10] clause 4.2.6.9.

12. The PCF for the PDU Session creates PCC rule(s) including the application ID(s) in the service data flow description, if they do not already exist, and installs the PCC rule(s) and the Policy Control request trigger(s), also if they do not already exist, to detect the start/stop of application traffic in the SMF as described in 3GPP TS 29.512 [9]. When the SMF detects that the Policy Control Request Trigger is met, the SMF reports to the PCF for the PDU session the start or stop of concerned the application traffic.

13-14. The PCF for the PDU Session may notify the PCF for the UE about the detected event using the Npcf_PolicyAuthorization_Notify service operation by sending an HTTP POST request to the notification URI received in the subscription, and the PCF for the UE responds with "204 No Content", as described in 3GPP TS 29.514 [10] clause 4.2.5.19.

15. AM Policy Association modification initiated by the PCF may be performed as described in clause 5.1.2.2.

16-19. If the AF had subscribed to an Access and Mobility management related event (e.g. about service area coverage change outcome), the PCF may send respective notification(s) to the NEF using the Npcf_EventExposure_Notify service operation by sending an HTTP POST message as described in clause 4.2.4.2 of 3GPP TS 29.523 [49] to the notification URI that was included in the AM Influence data retrieved from the UDR. The NEF forwards such received notifications to the AF using the Nnef_AMInfluence_Notify service operation by sending an HTTP POST message to the notification URI previously received from the AF. The AF sends a "204 No Content" response to the NEF and the NEF sends a "204 No Content" response to the PCF.

5.6 UE Policy Association Management

5.6.1 UE Policy Association Establishment

5.6.1.1 General

The procedures in this clause 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

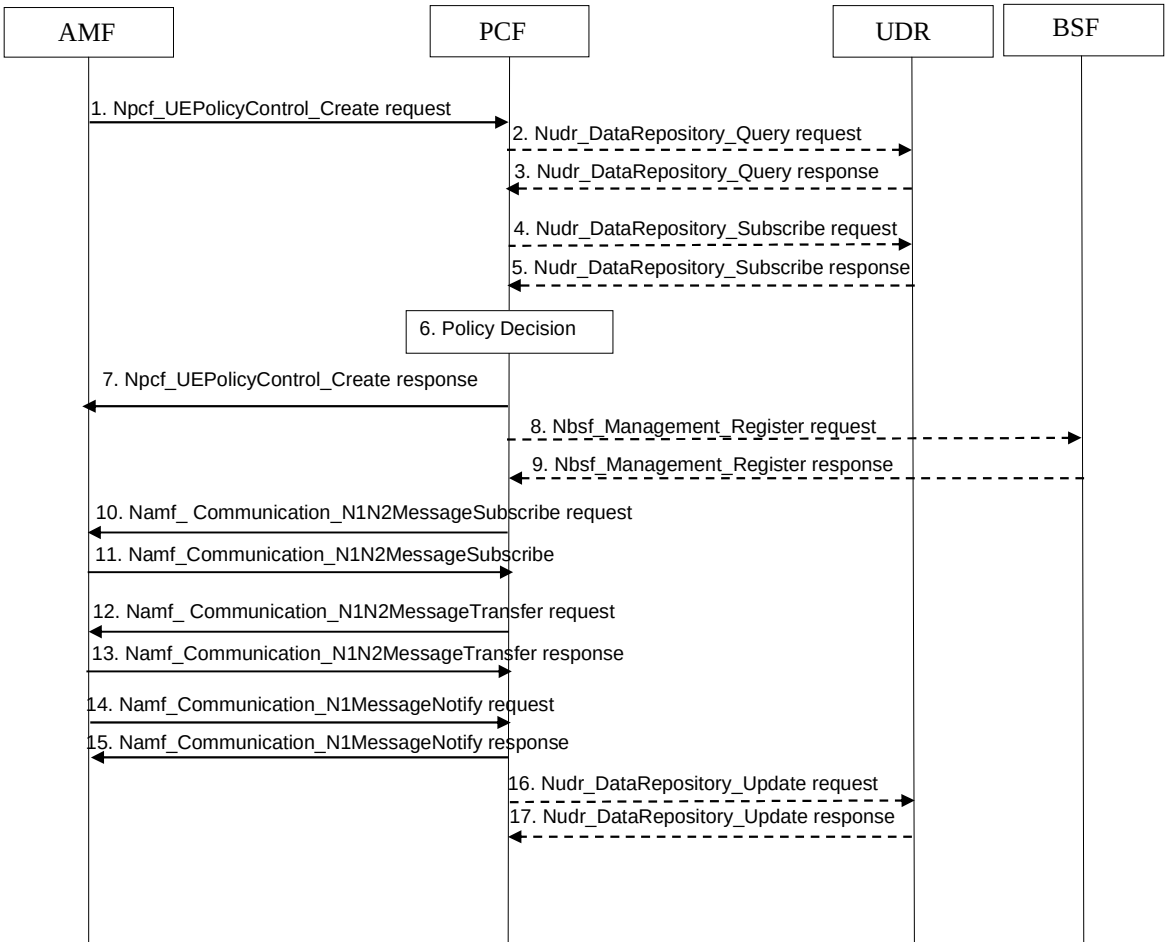


Figure 5.6.1.2-1: UE Policy Association Establishment procedure - Non-roaming

1. The AMF receives the registration request from the AN.

   Based on local policy, and the authorized capabilities received from the UE (e.g. V2X capabilities and/or 5G ProSe capabilities), as defined in clause 4.2.2.1 of 3GPP TS 29.525 [31], the AMF decides to select and contact the PCF to create the UE policy association . The AMF invokes the Npcf_UEPolicyControl_Create service

operation by sending an HTTP POST request to the "UE Policy Associations" resource as defined in clause 4.2.2.1 of 3GPP TS 29.525 [31].

2-3. 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. The UDR sends an HTTP "200 OK" response to the PCF with the latest UPSIs and its content, and/or the subscription data.

Additionally, if the "EnhancedBackgroundDataTransfer" feature defined in 3GPP TS 29.504 [27] is supported, the PCF invokes the Nudr_DataRepository_Query service operation to the UDR by sending the HTTP GET request to the "Applied BDT Policy Data" resource to retrieve the applied BDT Policy Data. The UDR sends an HTTP "200 OK" response with the stored applied BDT Policy Data. And then, if the corresponding transfer policy is not locally stored in the PCF, the PCF invokes the Nudr_DataRepository_Query service operation by sending the HTTP GET request to the "IndividualBdtData" resource or the "BdtData" collection resource with the URI query parameter "bdt-ref-ids" as specified in 3GPP TS 29.519 [12], to retrieve the related Background Data Transfer policy information (i.e. Time window and Location criteria) stored in the UDR. The UDR sends an HTTP "200 OK" response to the PCF.

Additionally, if the "AfGuideURSP" feature is supported and URSPs are influenced by the AF, and/or V2XP and/or the "ProSe" feature is supported and ProSeP policies may be delivered to the UE, the PCF invokes the Nudr_DataRepository_Query service operation to the UDR by sending the HTTP GET request to the "Service Parameter Data" resource to retrieve the service parameter data. The UDR sends an HTTP "200 OK" response with the stored service parameter data.

Additionally, the PCF invokes the Nudr_DataRepository_Query service operation to the UDR by sending the HTTP GET request to the "5GVnGroupsInternal" resource to retrieve the group configuration of the received 5G VN Group Id as specified in 3GPP TS 29.505 [47], if not internally available.

NOTE 1: The PCF can internally store the retrieved 5G VN group configuration data for later use for other SUPIs that belong to the same Internal-Group-Id.

4-5. The PCF may request notifications from the UDR on changes in the policy data subscription information (e.g, UE Policy Set resource), and in this case, the PCF shall invoke 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 "EnhancedBackgroundDataTransfer" feature defined in 3GPP TS 29.504 [27] is supported, to request notifications from the UDR on changes in the applied BDT Policy Data, the PCF invokes the Nudr_DataRepository_Subscribe service operation by sending an HTTP POST request to the "ApplicationDataSubscriptions" resource. The UDR sends an HTTP "201 Created" response to acknowledge the subscription.

Additionally, if the PCF requests notifications from the UDR on changes in the service parameter data, the PCF invokes the Nudr_DataRepository_Subscribe service operation by sending an HTTP POST request to the "ApplicationDataSubscriptions" resource. The UDR sends an HTTP "201 Created" response to acknowledge the subscription.

Additionally, to request notifications from the UDR on changes in the 5G VN group configuration data associated to each of the Internal-Group-Id provided to the PCF, the PCF invokes the Nudr_DataRepository_Subscribe service operation by sending an HTTP POST request to the "SubscriptionDataSubscriptions" resource as specified in 3GPP TS 29.505 [47], if not internally available. The UDR sends an HTTP "201 Created" response to acknowledge the subscription.

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

The PCF determines whether and which ANDSP and/or URSP has to be provisioned or updated based on the received list of UPSIs from the UE, if available, the UE Policy Sections stored in the UDR, if available, other received UE parameters, if available, the policy subscription and application data retrieved from UDR, if available, and local policies as defined in clauses 4.2.2.2.1.1, 4.2.2.2.2 (for ANDSP) and/or 4.2.2.2.3 (for URSP) of 3GPP TS 29.525 [31].

If the "V2X" feature is supported, the PCF determines whether the V2XP and the V2X N2 PC5 policy have to be provisioned as defined in clauses 4.2.2.2.1.2 and 4.2.2.3 of 3GPP TS 29.525 [31].

If the "ProSe" feature is supported, the PCF determines whether the ProSeP and the 5G ProSe N2 PC5 policy have to be provisioned as defined in clauses 4.2.2.2.1.3 and 4.2.2.4 of 3GPP TS 29.525 [31].

In addition, the PCF checks if the size of determined UE policy 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 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.

8-9. If the "ProSe" feature is supported for the Npcf_UEPolicyControl service, the PCF may register with the BSF as the PCF serving this UE, if not already registered at the AM Policy Association establishment. This is performed by using the Nbsf_Management_Register operation, providing as inputs the SUPI, the GPSI, if available, and the PCF end points related to the Npcf_AMPolicyAuthorization service.

10. To subscribe to notifications of N1 message for UE Policy Delivery Result, or subsequent UE policy requests (e.g. for V2XP and/or ProSeP), 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.

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

12. 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.

    If the "V2X" feature is supported and the PCF determines to provision V2XP and V2X N2 PC5 policy in step 6, the PCF sends the V2XP to the UE and the V2X N2 PC5 policy to the NG-RAN via the AMF by invoking the Namf_Communication_N1N2MessageTransfer service operation.

    If the "ProSe" feature is supported and the PCF determines to provision ProSeP and 5G ProSe N2 PC5 policy in step 6, the PCF sends the ProSeP to the UE and the5G ProSe N2 PC5 policy to the NG-RAN via the AMF by invoking the Namf_Communication_N1N2MessageTransfer service operation.

    The PCF can provision the UE policy (including V2XP and/or ProSeP) and V2X N2 PC5 policy and/or 5G ProSe N2 PC5 Policy in the same message.

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

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

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

16-17. 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

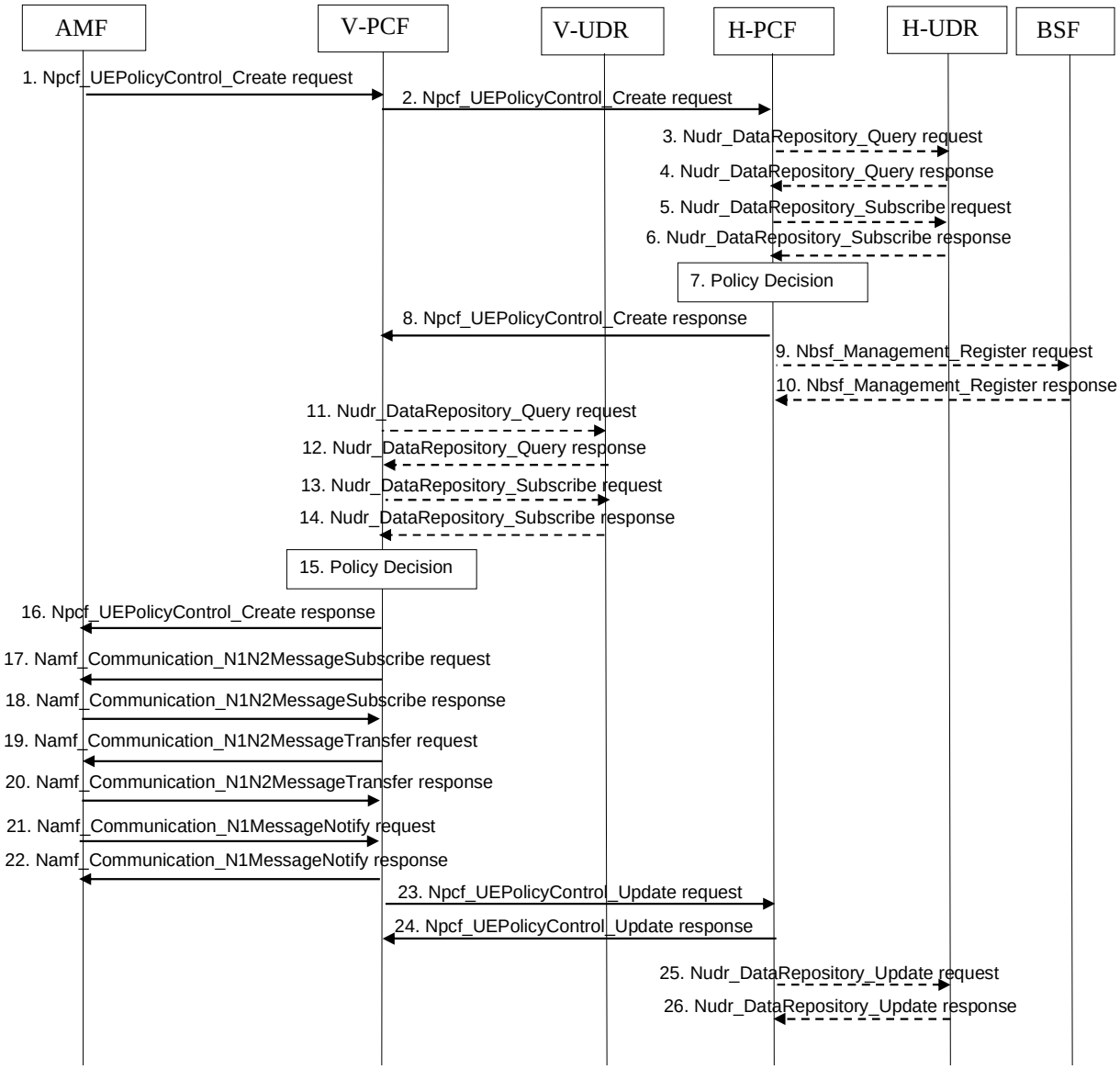


Figure 5.6.1.3-1: UE Policy Association Establishment procedure - Roaming

1. The AMF receives the registration request from the AN.

   Based on local policy, and the capabilities received from the UE (e.g. V2X capabilities) , as defined in clause 4.2.2.1 of 3GPP TS 29.525 [31], 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 as defined in clause 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 clause 5.6.1.2, except the description of "EnhancedBackgroundDataTransfer" feature is not applicable.

7. The H-PCF determines whether and which ANDSP and/or URSP has to be provisioned or updated based on the received list of UPSIs from the UE, if available, the UE Policy Sections stored in the UDR, if available, other received UE parameters, if available, the policy subscription and application data retrieved from UDR, if

available, and local policies as defined in clauses 4.2.2.2.1.1, 4.2.2.2.2 (for ANDSP) and/or 4.2.2.2.3 (for URSP) of 3GPP TS 29.525 [31].

If the "V2X" feature is supported, the H-PCF determines whether the V2XP and the V2X N2 PC5 policy have to be provisioned as defined in clause s 4.2.2.2.1.2 and 4.2.2.3 of 3GPP TS 29.525 [31].

If the "ProSe" feature is supported, the H-PCF determines whether the ProSeP and the 5G ProSe N2 PC5 policy have to be provisioned as defined in clauses 4.2.2.2.1.3 and 4.2.2.4 of 3GPP TS 29.525 [31].

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 clause 5.6.2.2.3.

8. The H-PCF sends an HTTP "201 Created" response to the V-PCF with the decided UE policy, Policy Control Request Trigger(s) and N2 PC5 policy if available.

9-10. If the "ProSe" feature is supported for the Npcf_UEPolicyControl service, the H-PCF may register with the BSF as the PCF serving this UE. This is performed by using the Nbsf_Management_Register operation, providing as inputs the SUPI, the GPSI, if available, and the PCF end points related to the Npcf_AMPolicyAuthorization service.

11. 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.

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

13. 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.

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

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

The V-PCF determines whether and which visited ANDSP has to be provisioned based on the received list of UPSIs from the UE, if available, the UE Policy Sections locally configured or stored in the UDR for the UE PLMN, other received UE parameters, if available, and local polices as defined in clauses 4.2.2.2.1.1, and 4.2.2.2.2 of 3GPP TS 29.525 [31].

If the "V2X" feature is supported and the V-PCF received the V2XP and the V2X N2 PC5 policy, the V-PCF sends the V2XP to the UE and the V2X N2 PC5 policy to the NG-RAN via the AMF by invoking the Namf_Communication_N1N2MessageTransfer service operation.

If the "ProSe" feature is supported and the V-PCF received the ProSeP and the 5G ProSe N2 PC5 policy, the V-PCF sends the ProSeP to the UE and the 5G ProSe N2 PC5 policy to the NG-RAN via the AMF by invoking the Namf_Communication_N1N2MessageTransfer service operation.

The PCF can provision the UE policy (including V2XP and/or ProSeP) and V2X N2 PC5 policy and/or 5G ProSe N2 PC5 Policy in the same message.

In addition, the V-PCF checks if the size of determined UE policy 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 messages 19 to 24 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 19 to 24 are thus executed several times, one time for each UE policy information fragment.

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

17. To subscribe to notifications of N1 message for UE Policy Delivery Result, or subsequent UE policy requests (e.g. for V2XP and/or ProSeP), 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.

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

19. 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.

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

21. 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.

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

23. 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.

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

25-26. 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 clause are performed when a Policy Control Request Trigger condition is met or when the new AMF reuses the UE Policy Association established by the old AMF with the 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

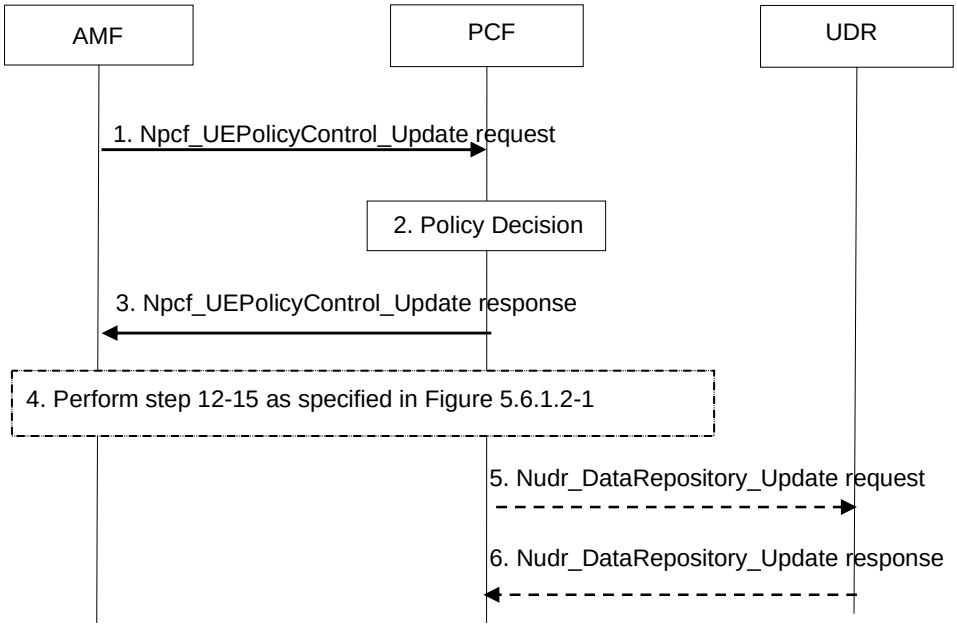


Figure 5.6.2.1.2-1: AMF-initiated UE Policy Association Modification procedure – Non-roaming

1. When the AMF detects a Policy Control Request Trigger condition is met or, when during AMF relocation, the new AMF decides to reuse the UE Policy Association established by the old AMF with thePCF, 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 and/or updated V2X N2 PC5 policy, if the "V2X" feature is supported, and/or, if the "ProSe" feature is supported, updated ProSeP within the updated UE Policy and/or 5G ProSe N2 PC5 policy. The PCF checks if the size of determined UE policy exceeds a predefined limit the same as step 6 in clause 5.6.1.2.

   The PCF determines whether and which ANDSP and/or URSP has to be provisioned or updated based on policy subscription and application data, if available, the UE Policy Sections previously delivered to the UE, if available, other UE parameters previously received from the UE, if available, the reported information by the AMF and local policies, as defined in clauses 4.2.2.2.1.1, 4.2.2.2.2 (for ANDSP) and/or 4.2.2.2.3 (for URSP) of 3GPP TS 29.525 [31].

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, and/or N2 PC5 policy and/or 5G ProSe N2 PC5 policy in step 2, steps 12-15 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

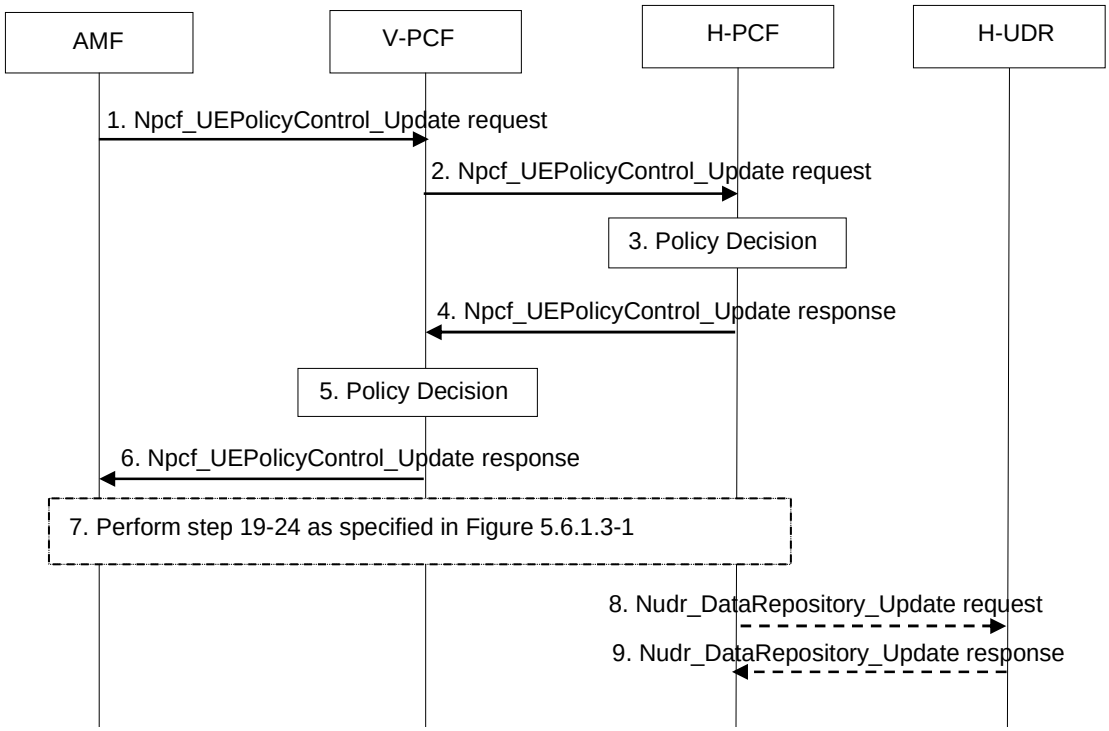


Figure 5.6.2.1.3-1: AMF-initiated UE Policy Association Modification procedure - Roaming

1. When the AMF detects a Policy Control Request Trigger condition is met or, when during AMF relocation, the new AMF decides to reuse the UE Policy Association established by the old AMF with the PCF, 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.

   If the V-PCF received a Namf_Communication_N1MessageNotify service request with a UE Policy container, the V-PCF forwards the received container to the H-PCF by sending an HTTP POST request to the "Individual UE Policy Association" resource.

3. The H-PCF makes the policy decision including the applicable updated Policy Control Request Trigger(s) and/or updated UE Policy and/or, if the "V2X" feature is supported, updated V2XP within the updated UE Policy and/or V2X N2 PC5 policy, and/or, if the "ProSe" feature is supported, updated ProSeP within the updated UE Policy and/or 5G ProSe N2 PC5 policy.

   The H-PCF determines whether and which ANDSP and/or URSP has to be provisioned or updated based on policy subscription and application data, if available, the UE Policy Sections previously delivered to the UE, if available, other UE parameters previously received from the UE, if available, the reported information by the V-PCF and local policies, as defined in clauses 4.2.2.2.1.1, 4.2.2.2.2 (for ANDSP) and/or 4.2.2.2.3 (for URSP) of 3GPP TS 29.525 [31].

   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 clause 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, if applicable. The V-PCF checks if the size of determined UE policy exceeds a predefined limit the same as step 13 in clause 5.6.1.3.

   The V-PCF determines whether VPLMN ANDSP has to be provisioned or updated based on policy subscription for the UE PLMN, other UE parameters previously received from the UE, if available, and local policies, as defined in clauses 4.2.2.2.1.1, 4.2.2.2.2 (for ANDSP) of 3GPP TS 29.525 [31].

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, V2X N2 PC5 policy and/or 5G ProSe N2 PC5 policy in step 4, steps 19-24 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 clause are performed when the UE policy (roaming case) and/or Policy Control Request Trigger(s) are 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

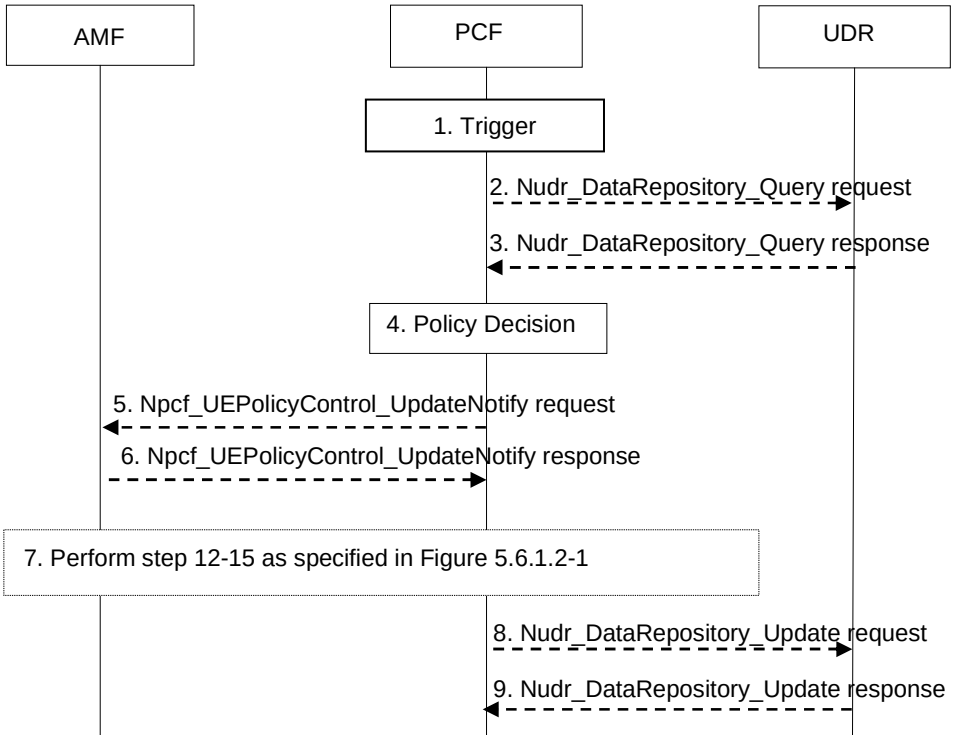


Figure 5.6.2.2.2-1: PCF-initiated UE Policy Association Modification procedure – Non-roaming

1. The PCF receives an external trigger, e.g. the subscriber policy data of a UE is changed, the applied BDT Policy Data is changed, or subscription data for the 5G VN group data 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.

NOTE 1: When the external trigger affects more than one UE (e.g. when Network Performance is degraded in a network area info) the PCF will apply the next steps to all the affected active UE Policy Associations.

2-3. If the applied BDT policy Data is changed in step1, and if the corresponding transfer policy is not locally stored in the PCF, the PCF sends the HTTP GET request to the "IndividualBdtData" resource to retrieve the related Background Data Transfer policy information (i.e. Time window and Location criteria) stored in the UDR. The UDR sends an HTTP "200 OK" response to the PCF.

4. The PCF makes the policy decision including the applicable updated Policy Control Request Trigger(s) and/or updated UE Policy and/or updated V2X N2 PC5 policy, if the "V2X" feature is supported, and/or updated 5G ProSe N2 PC5 policy, if the "ProSe" feature is supported. The PCF checks if the size of determined UE policy exceeds a predefined limit the same as step 6 in clause 5.6.1.2.

5. If the PCF decided to update the Policy Control Request Trigger(s) in step4, the V-PCF shall invoke the Npcf_UEPolicyControl_UpdateNotify service operation by sending an HTTP POST request to the callback URI "{notificationUri}/update".

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

7. If the PCF decided to update the UE policy, V2X N2 PC5 policy and/or 5G ProSe N2 PC5 policy in step 4, steps 12-15 as specified in Figure 5.6.1.2-1 are executed.

8-9. If the PCF decided to update the UE policy in step 4, steps 5-6 in clause 5.6.2.1.2 are executed.

NOTE 2: When the trigger to update the UE policy is AF-based service parameter provisioning as described in clause 5.5.8, the AF requested to be notified of the outcome of the UE Policy delivery and the PCF initiated step 7 based on the AF request, then steps 7 - 10 specified in clause 5.5.8 are executed.

5.6.2.2.3 Roaming

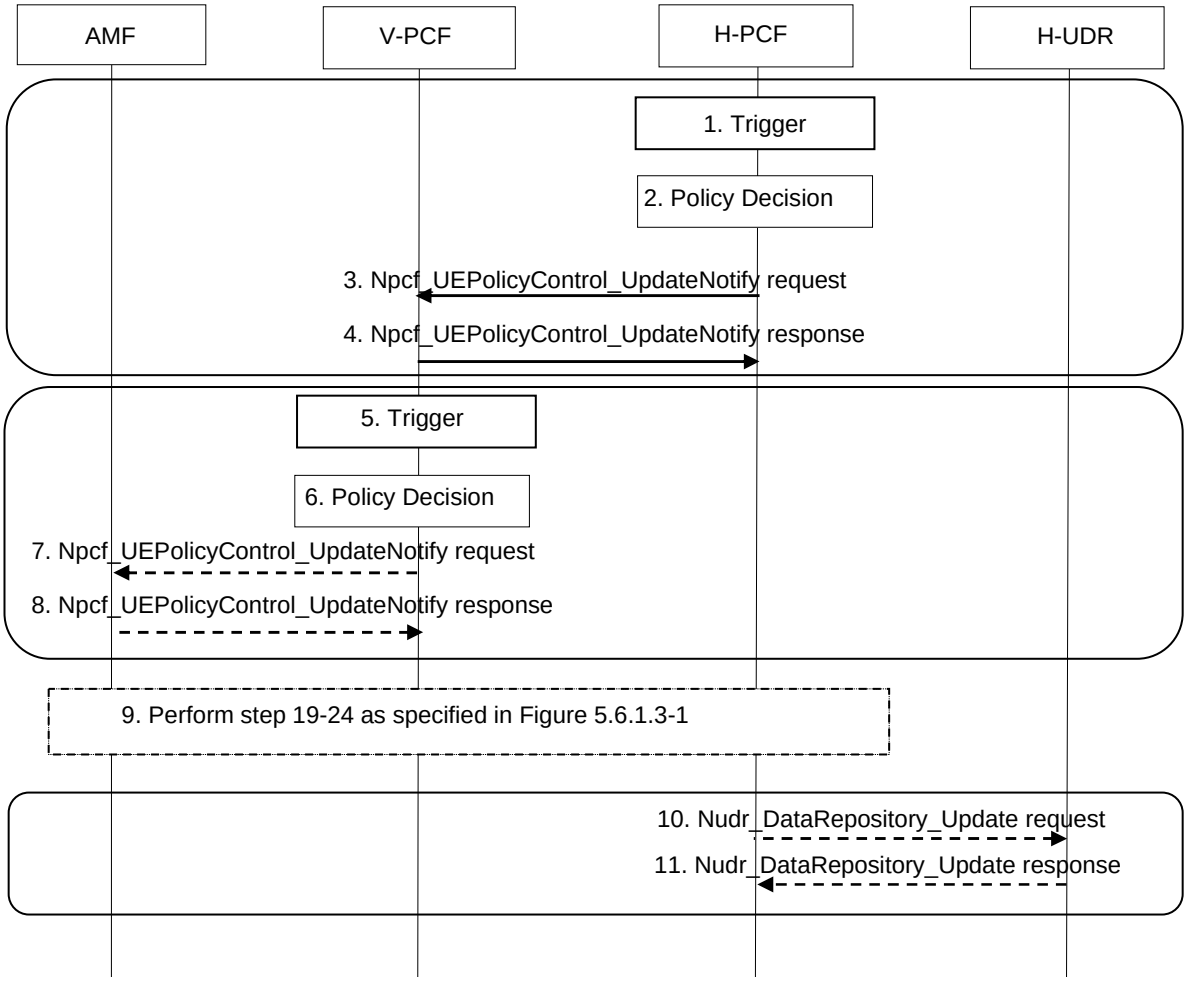


Figure 5.6.2.2.3-1: PCF-initiated UE Policy Association Modification procedure – Roaming

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 and/or updated V2X N2 PC5 policy, if the "V2X" feature is supported, and/or updated 5G ProSe N2 PC5 policy, if the "ProSe" feature is supported.

   The H-PCF determines whether and which ANDSP and/or URSP has to be provisioned or updated based on policy subscription and application data, if available, the UE Policy Sections previously delivered to the UE, if available, other UE parameters previously received from the UE, if available, and local policies, as defined in clauses 4.2.2.2.1.1, 4.2.2.2.2 (for ANDSP) and/or 4.2.2.2.3 (for URSP) of 3GPP TS 29.525 [31].

   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 callback URI "{notificationUri}/update" with the updated UE policy and/or the updated V2X N2 PC5 policy and/or the updated 5G ProSe N2 PC5 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.

NOTE 2: When the V-PCF receives an internal or external trigger to re-evaluate the UE policy decision for the roaming UEs of a PLMN ID, the PCF applies control mechanisms to avoid signalling storms and potential network overload, as e.g. limiting the number of simultaneous updates distributing the base of visiting UEs in a time dispersion interval.

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 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 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 callback URI "{notificationUri}/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 and/or V2X N2 PC5 policy, if the "V2X" feature is supported, and/or 5G ProSe N2 PC5 policy, if the "ProSe" feature is supported, in step 3, steps 19-24 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 clause 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

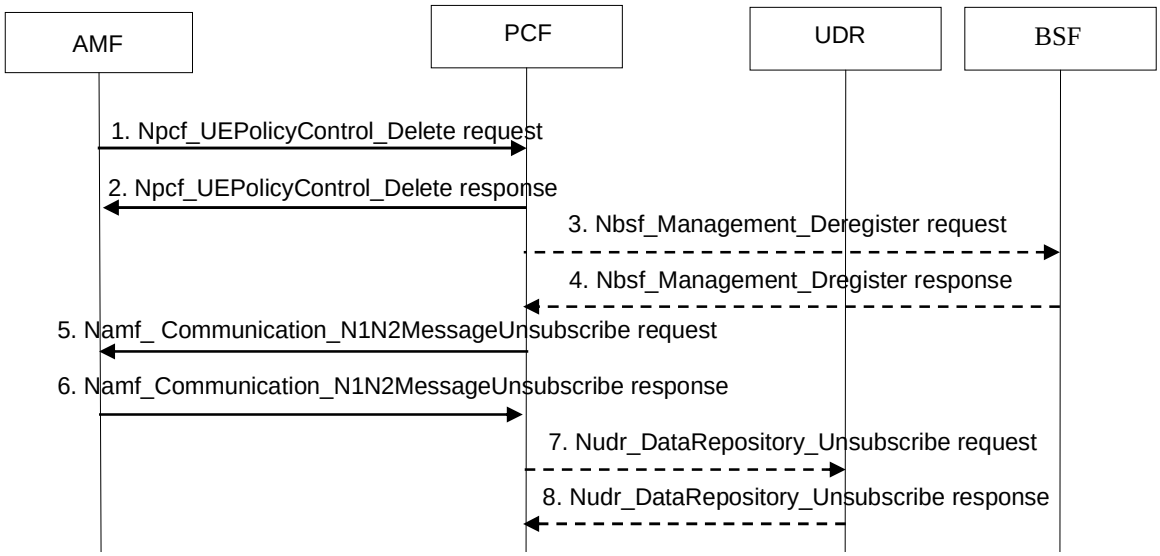


Figure 5.6.3.1.2-1: AMF-initiated UE Policy Association Termination procedure – Non-roaming

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.

3-4. If the PCF has previously registered to the BSF as the PCF that is serving this UE, the PCF deregisters from the BSF if no AM Policy Association nor UE Policy Association for this UE exists anymore. This is performed by using the Nbsf_Management_Deregister service operation.

5. 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.

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

7. 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.

- The PCF invokes also the Nudr_DataRepository_Unsubscribe service operation to unsubscribe from notifications about applied BDT Policy Data changes and service parameter data changes at the UDR by sending an HTTP DELETE request to the "IndividualApplicationDataSubscription" resource if it has subscribed such notifications.

- The PCF invokes also the Nudr_DataRepository_Unsubscribe service operation to unsubscribe from notifications about 5G VN group configuration data changes at the UDR by sending an HTTP DELETE request to the "IndividualSubscriptionDataSubscription" resource as specified in 3GPP TS 29.505 [47] if it has subscribed such notification.

NOTE: The PCF will not invoke the Nudr_DataRepository_Unsubscribe service operation when the PCF has internally stored the retrieved 5G VN group configuration data for later use for other SUPIs that belong to the same Internal-Group-Id.

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

5.6.3.1.3 Roaming

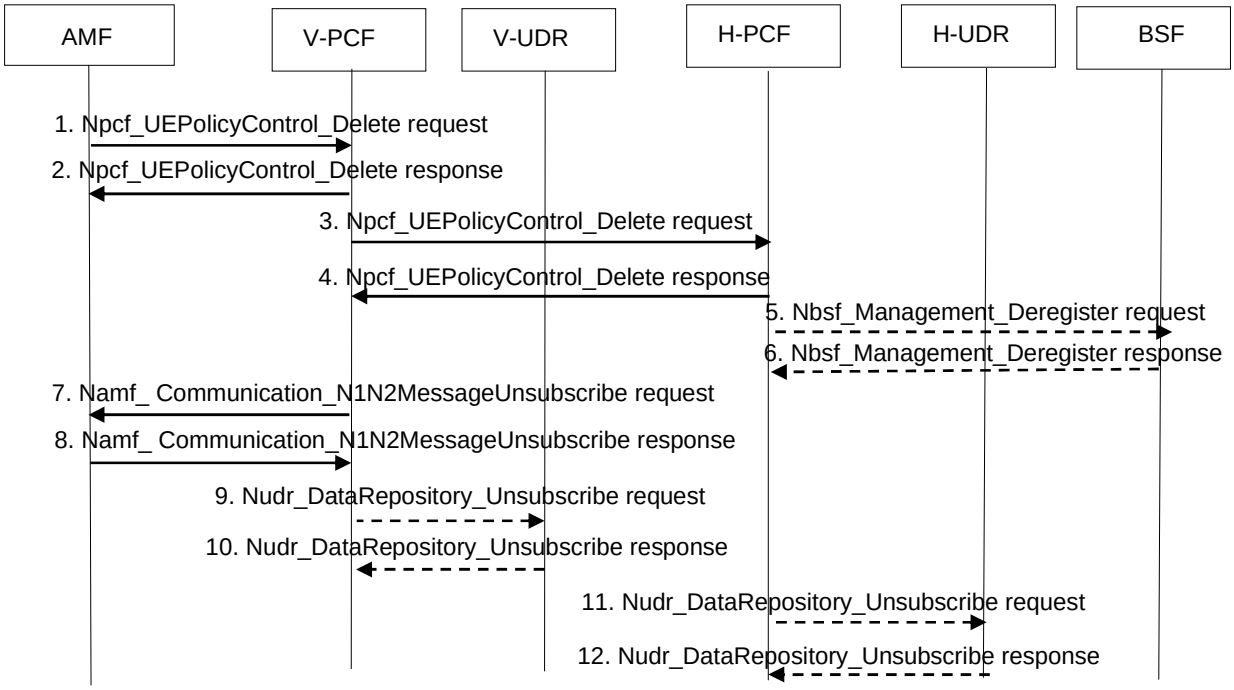


Figure 5.6.3.1.3-1: AMF-initiated UE Policy Association Termination procedure – Roaming

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.

5-6. If the H-PCF has previously registered to the BSF as the PCF that is serving this UE, the H-PCF shall deregister from the BSF if no AM Policy Association nor UE Policy Association for this UE exists anymore. This is performed by using the Nbsf_Management_Deregister service operation.

7. 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.

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

9. 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.

10. The V-UDR sends an HTTP "204 No Content" response to the V-PCF.

11. 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.

- The PCF invokes also the Nudr_DataRepository_Unsubscribe service operation to unsubscribe from notifications about service parameter data changes at the UDR by sending an HTTP DELETE request to the "IndividualApplicationDataSubscription" resource if it has subscribed such notification.

- The PCF invokes also the Nudr_DataRepository_Unsubscribe service operation to unsubscribe from notifications about 5G VN group configuration data changes at the UDR by sending an HTTP DELETE request to the "IndividualSubscriptionDataSubscription" resource as specified in 3GPP TS 29.505 [47] if it has subscribed such notification.

NOTE: The PCF will not invoke the Nudr_DataRepository_Unsubscribe service operation when the PCF has internally stored the retrieved 5G VN group configuration data for later use for other SUPIs that belong to the same Internal-Group-Id.

12. 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

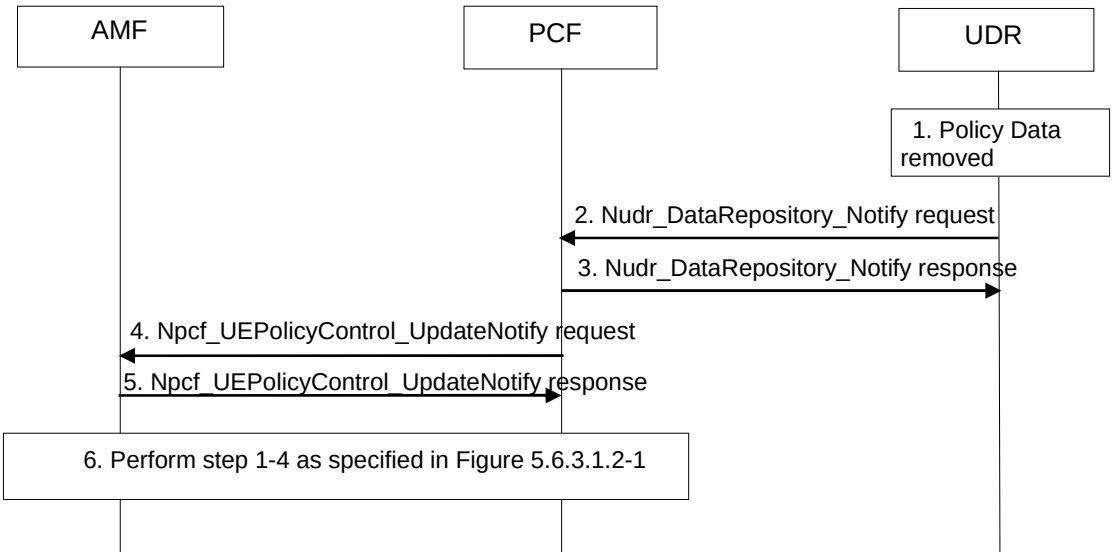


Figure 5.6.3.2.2-1: PCF-initiated UE Policy Association Termination procedure – Non-roaming

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 callback 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 callback URI "{notificationUri}/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

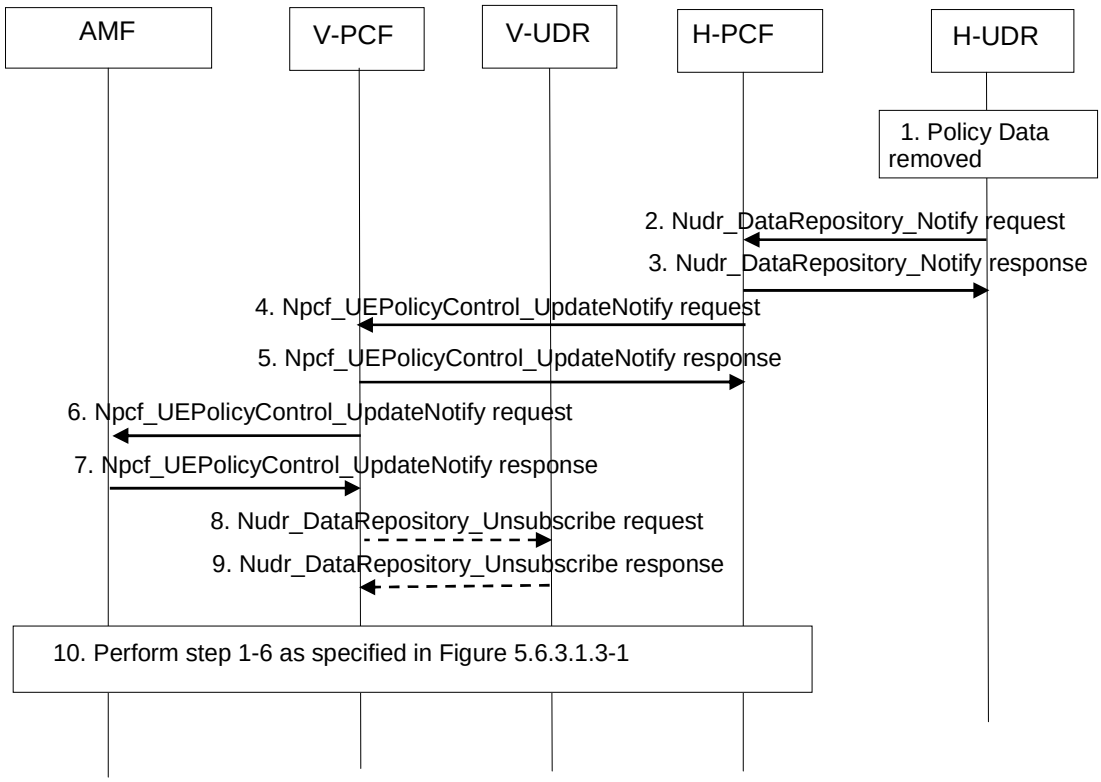


Figure 5.6.3.2.3-1: PCF-initiated UE Policy Association Termination procedure – Roaming

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 callback 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 callback URI "{notificationUri}/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 callback URI "{notificationUri}/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.

5.7 MBS Policy Association Management

5.7.1 General

Clause 5.7 specifies the detailed call flows for MBS Policy and Charging Control (PCC) for 5G multicast-broadcast services over the Npcf and Nmbsmf service-based interfaces and their relationship with the flow level signalling in the 5G system.

The stage 2 definition, architecture and procedures for MBS PCC are specified in 3GPP TS 23.247 [54].

5.7.2 MBS Policy Association Establishment

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

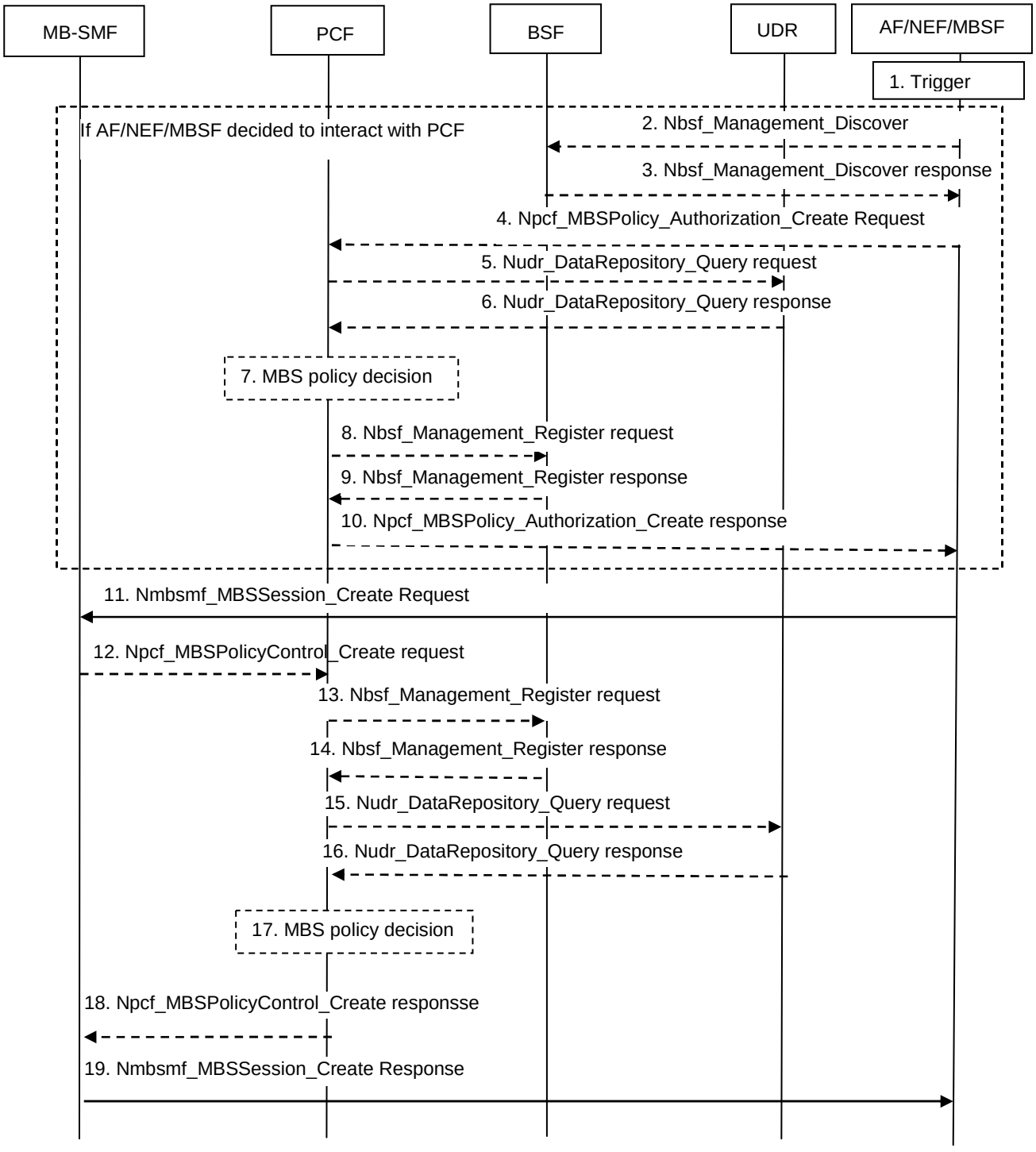


Figure 5.7.2-1: MBS Policy Association Establishment procedure

1. When the AF decides to create an MBS Session, the AF/NEF/MBSF may decide to interact with the PCF based on the local configuration. If it does, the procedure continues with step2; otherwise, the procedure continues with step 11.

2. If the AF/NEF/MBSF receives the Request for location-dependent session from the AF and if there is a need to select the same PCF for the location dependent MBS Sessions, the NEF/MBSF checks whether there is already a PCF serving the MBS session by invoking Nbsf_Management_Discover service by sending an HTTP GET request to the resource "PCF for an MBS Session Bindings" in order to discover whether there is a PCF serving the MBS session with the MBS session ID as described in 3GPP TS 29.521 [22]. In the case that the NEF/MBSF

receives a request without an MBS Session ID from the AF, the NEF/MBSF contacts with the MB-SMF to request allocation of a TMGI before the NEF/MBSF contacts with the PCF.

3. If there is a PCF serving the MBS session, the BSF sends an HTTP "200 OK" with the address of another PCF to AF/NEF/MBSF; otherwise, the BSF returns an HTTP "200 OK" with empty array (i.e. "[ ]" in JSON).

4. If the received Request is not for location-dependent session in step 1 or the BSF returned an HTTP "200 OK" with empty array (i.e. "[ ]" in JSON), the AF/NEF/MBSF discovers and selects the PCF as defined in clause 8.6.2, and then the AF/NEF/MBSF invokes the Npcf_MBSPolicyAuthorization_Create service operation by sending an HTTP POST request to the "MBS Application Session Contexts" resource as defined in clause 5.3.2.2 of 3GPP TS 29.537 [55] with the request body containing the concerned MBS Session Id, MBS service information, DNN if available and S-NSSAI if available; otherwise if the BSF returned the HTTP "200 OK" with the address of another PCF, the AF/NEF/MBSF contacts with the returned PCF by invoking the Npcf_MBSPolicyAuthorization_Create service operation.

5. 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 "MBSSessionPolicyControlData" resource as specified in 3GPP TS 29.519 [12].

6. The UDR sends an HTTP "200 OK" response to the PCF with the requested subscription data in the response message body.

7. The PCF determines whether the request is authorized and if the request is authorized, the PCF derives the MBS policies based on the received information and packages them into an MBS policy decision as described in clause 5.2.2 of 3GPP TS 29.537 [55].

8. If the request is authorized and the PCF is not already handling the MBS Session Id, the PCF may register to the BSF by sending an HTTP POST request to the "PCF for an MBS Session Bindings" resource of the Nbsf_Management_Register service as described in clause 4.2.2.4 of 3GPP TS 29.521 [22].

9. The BSF responds with "201 Created" if the registration of the PCF was successful.

10. The PCF sends an Npcf_MBSPolicy_Authorization_Create Response to the NEF/MBSF.

11. AF/NEF/MBSF selects the MB-SMF and sends Nmbsmf_MBSSession_Create Request to the MB-SMF as defined in clause 5.3.2.2 of 3GPP TS 29.532 [58].

12. Upon reception of an Nmbsmf_MBSession_Create request from the NEF/MBSF, the MB-SMF discovers and selects the PCF as defined in clause 8.6.1, and then invokes the Npcf_MBSPolicyControl_Create service operation by sending an HTTP POST request to the "MBS Policies" resource as defined in clause 5.2.2.2 of 3GPP TS 29.537 [55] with the request body containing the concerned MBS Session Id, DNN if received, S-NSSAI if received and MBS service information if received..

13. If the PCF is not handling the MBS session ID (i.e. the request from the AF/NEF/MBSF in step 11 is for location-dependent session but the PCF is not handling the MBS session ID), the PCF checks whether there is already a PCF serving the MBS session by invoking Nbsf_Management_ Register service as described in 3GPP TS 29.521 [22].

14. If there is and existing MBS Session Binding information for the MBS session ID, the the BSF rejects the request with an HTTP "403 Forbidden" status code and includes the address of the existing PCF in the response; otherwise, the BSF stores the MBS Session binding information and responds to the MB-SMF with an HTTP "201 Created".

15. If the PCF receives MBS service information from the MB-SMF and the PCF does not have the subscription data (e.g. the steps 2-10 were not executed), it invokes the Nudr_DataRepository_Query service operation to the UDR by sending an HTTP GET request to the "MBSSessionPolicyControlData" resource as specified in 3GPP TS 29.519 [12].

16. The UDR sends an HTTP "200 OK" response to the PCF with the requested subscription data in the response message body.

17. The PCF determines whether the request is authorized and if the request is authorized the PCF derives the MBS policies based on the received information and packages them into an MBS policy decision as described in clause 5.2.2 of 3GPP TS 29.537 [55]. If steps 2-10 were performed and MBS policies were derived in step 7, this step is not needed.

18. The PCF then responds to the MB-SMF. Following responses are returned to the MB-SMF:

    - If the PCF receives the HTTP "403 Forbidden" with the address of another PCF in step 14, the PCF rejects the request and responds to the MB-SMF with an HTTP "308 Permanent Redirection" status code including an HTTP Location header field containing the "apiRoot" (e.g. FQDN or IP address) of the PCF currently serving the MBS Session as described in clause 5.2.2 of 3GPP TS 29.537 [55]. In this case, the MB-SMF contacts with the returned address of the another PCF as described in step 12; otherwise,

- If the PCF receives the HTTP "201 Created " in step 14 and the request is authorized, the PCF responds to the MB-SMF with an HTTP "201 Created" status code with the response body including the derived MBS policy as described in clause 5.2.2 of 3GPP TS 29.537 [55];19. The MB-SMF sends Nmbsmf_MBSSession_Create Response to the NEF/MBSF as defined in clause 5.3.2.2 of 3GPP TS 29.532 [58].

NOTE: This steps 2, 8 and 13 are not necessary in a deployment with a single PCF.

5.7.3 MBS Policy Association Modification

5.7.3.1 General

The MBS Policy Association Modification procedure may be initiated by the AF.

5.7.3.2 MBS Policy Association Modification initiated by the AF

This procedure is performed when the AF/NEF/MBSF or the MB-SMF needs to modify MBS policy decisions related to an existing MBS Policy Association when the AF decides to update the MBS Service Information.

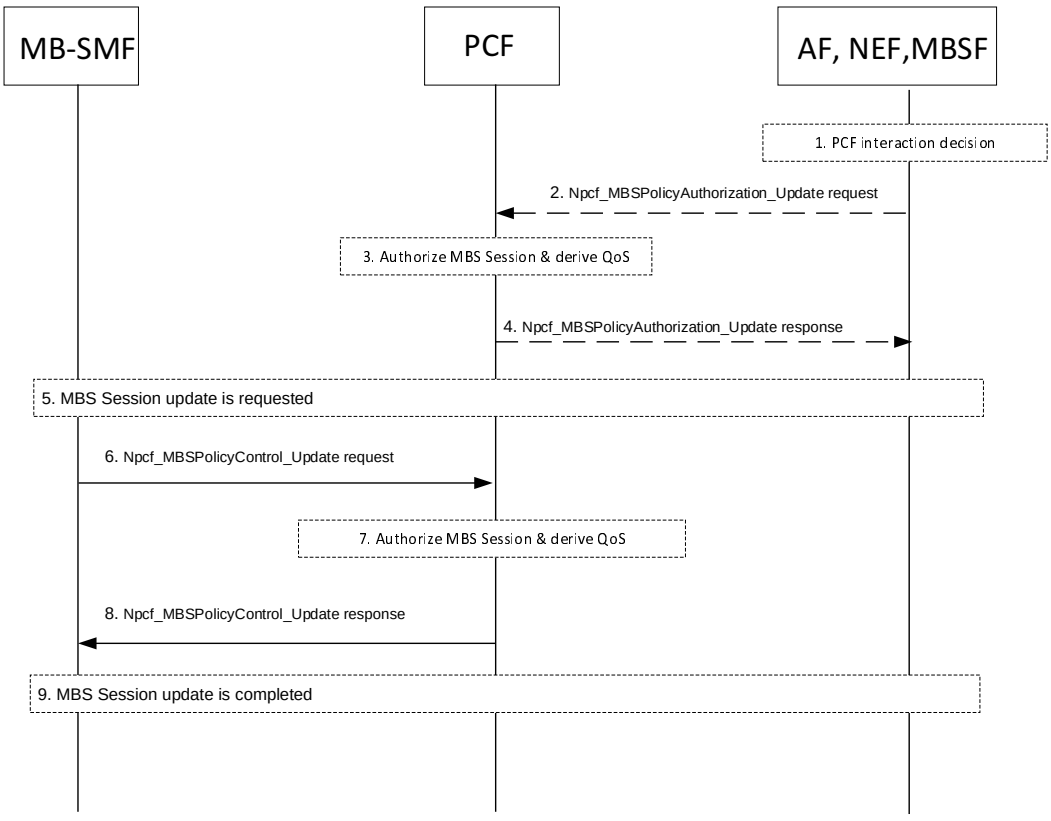


Figure 5.7.3.2-1: MBS Policy Association Modification procedure

1. When the AF decides to modify an existing MBS Session that requires policy control, the AF/NEF/MBSF may decide to interact with the PCF for early authorization based on the same decision that was made during MBS Session creation procedure (see clause 5.7.2). If no interaction is required, steps 2-4 are skipped.

2. The AF/NEF/MBSF invokes the Npcf_MBSPolicyAuthorization_Update service operation by sending an HTTP PATCH request to the "Individual MBS Application Session Context" resource as defined in clause 5.3.2.3.2 of

3GPP TS 29.537 [55] with the request body containing the MbsAppSessionCtxtPatch data structure with the modified service information within the "mbsServiceInfo" attribute.

3. The PCF determines whether the request is authorized and if the request is authorized, the PCF derives the updated QoS parameters based on the received MBS Service Information and determines whether this updated QoS is allowed. If the updated QoS is allowed, the PCF generates the updated policy information for the MBS session and packages it together with the MBS Session ID into an MBS policy decision as described in clause 5.3.2.3 of 3GPP TS 29.537 [55].

4. The PCF responds to the AF/NEF/MBSF with an HTTP "200 OK" status code with the Application Session context information within the "MbsAppSessionCtxt" data type, including the "contactPcfInd" attribute if the policy information was changed to indicate that the MB-SMF needs to contact the PCF. Alternatively, the PCF may respond with an HTTP "204 No Content" when no information is provided in the response.

5. The AF/NEF/MBSF sends Nmbsmf_MBSSession_Update Request to the MB-SMF as defined in clause 5.3.2.3 of 3GPP TS 29.532 [58].

6. If the MB-SMF received the indication to contact the PCF or did not receive it but decided to contact the PCF, the MB-SMF invokes the Npcf_MBSPolicyControl_Update service operation by sending an HTTP POST request to the PCF to update the Individual MBS Policy Association. The request body shall include the MbsPolicyCtxtDataUpdate data structure in the payload body of the HTTP POST, that may include the request trigger(s) within the "mbsPcrts " attribute and, if received from the AF/NEF/MBSF, the updated service information within the "mbsServInfo", as described in clause 5.2.2.3.2 of 3GPP TS 29.537 [55].

7. The PCF determines whether the request is authorized and if the request is authorized, the PCF checks if there is available service information. In that case, the PCF derives the updated QoS parameters based on the received MBS Service Information and determines whether this updated QoS is allowed. If the updated QoS is allowed, the PCF generates the updated policy information for the MBS session and packages it into the updated MBS policy decision as described in clause 5.2.2.3 of 3GPP TS 29.537 [55]. If the PCF did not receive MBS Service Information from the MB-SMF, the PCF identifies any updated policy information for the MBS session corresponding to the MBS session ID received from the MB-SMF.

8. Upon success, the PCF responds to the MB-SMF with an HTTP "200 OK" status code including the MbsPolicyData data structure with the input parameters within the "mbsPolicyCtxtData" attribute and the updated policy information within "mbsPolicies" attribute.

9. The AF/NEF/MBSF sends Nmbsmf_MBSSession_Update Response to the MB-SMF as defined in clause 5.3.2.3 of 3GPP TS 29.532 [58].

5.7.4 MBS Policy Association Termination

5.7.4.1 General

The MBS Policy Association Termination procedure isinitiated by the AF..

5.7.4.2 MBS Policy Association Termination initiated by the PCF

Void

5.7.4.3 MBS Policy Association Termination initiated by the AF

This procedure is performed when the AF/NEF/MBSF needs to terminate the MBS Policy Association when the AF decides to release the MBS session.

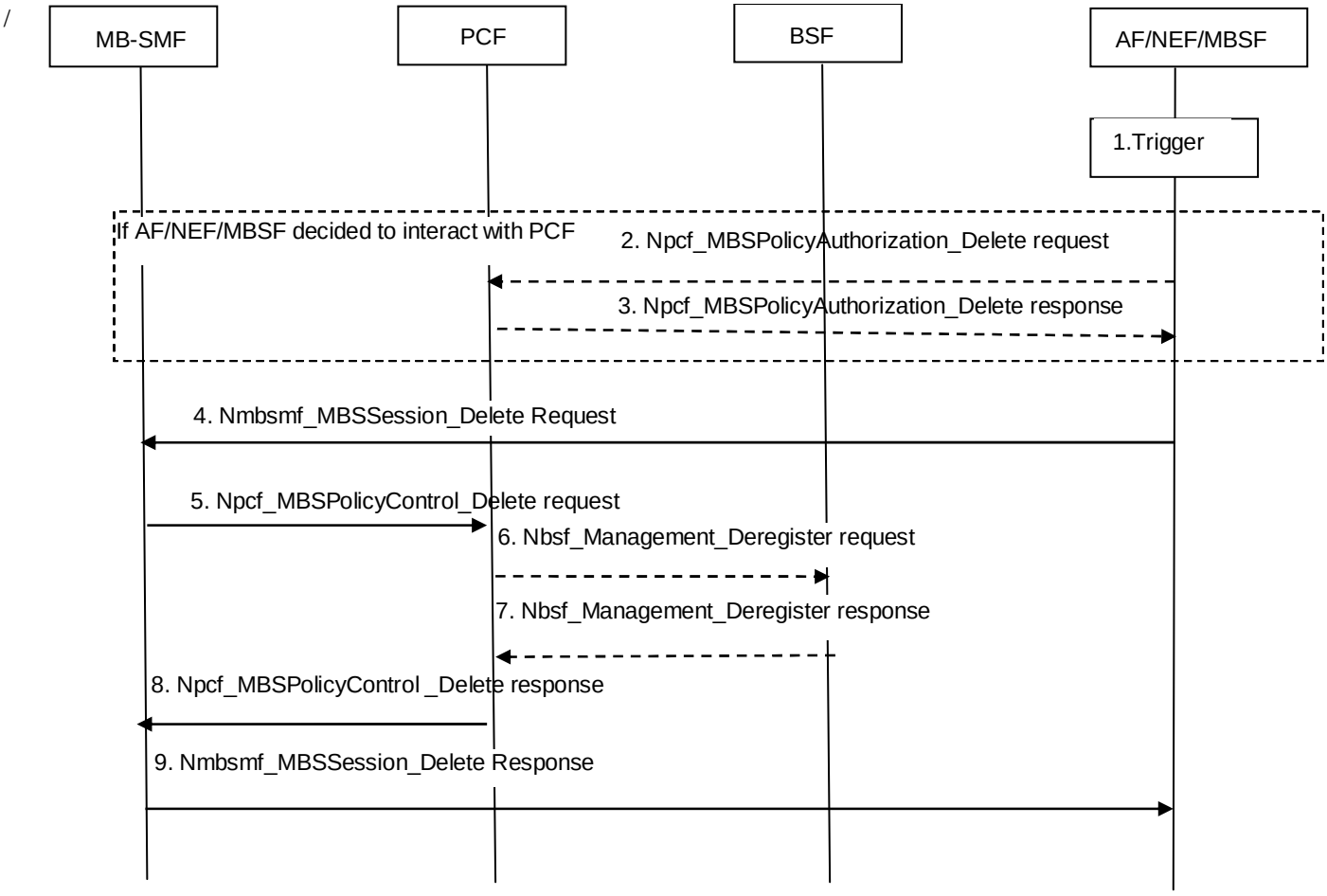


Figure 5.7.4.3-1: MBS Policy Association termination procedure initiated by the AF.

1. When the AF decides to terminate an existing MBS Session under policy control, the AF/NEF/MBSF interacts with the PCF if it was decided to contact the PCF as part of the MBS Policy Association creation procedure. In that case steps 2 and 3 applies. Otherwise, these steps are skipped.
2. The AF/NEF/MBSF invokes Npcf_MBSPolicyAuthorization_Delete Request to the PCF that handles the MBS Session by sending an HTTP DELETE request to the "Individual MBS Application Session Context" resource as defined in clause 5.3.2.4 of 3GPP TS 29.537 [55].
3. Upon success, the PCF responds with an HTTP "204 No Content" status code.
4. The AF/NEF/MBSF sends Nmbsmf_MBSSession_Delete Request to the MB-SMF as defined in clause 5.3.2.4 of 3GPP TS 29.532 [58].
5. The MB-SMF invokes the Npcf_MBSPolicyControl_Delete service operation by sending an HTTP DELETE request to the "Individual MBS Policy" resource to request the PCF to delete the context of the MBS related policy as defined in clause 5.2.2.4.2 of 3GPP TS 29.537 [55].
6. If the same PCF is used for the location dependent MBS sessions and this is the last MBS Policy Association related to that MBS Session 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 clause 8.5.3.
7. The PCF receives an HTTP "204 No Content" response from the BSF as detailed in clause 8.5.3.
8. The PCF deletes the concerned MBS Policy Association context for the terminated MBS Session and responds to the MB-SMF with an HTTP "204 No Content" status code.

NOTE: Step 6 and 8 can be executed in parallel.

9. The MB-SMF sends Nmbsmf_MBSSession_Delete Response to the NEF/MBSF as defined in clause 5.3.2.4 of 3GPP TS 29.532 [58].

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 parts:

1. Session binding.
2 PCC rule authorization.
3. QoS flow binding.

For PCC deployments not supporting MBS, the binding mechanism is described in this clause and the rest of clauses under clause 6.

When PCC is deployed in an MBS architecture as defined in 3GPP TS 23.247 [54], the binding mechanism is defined as described in clause 6.5.

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.

NOTE 1: The UE IPv4 address or IPv6 address received by the PCF from the AF can contain an IP address that belongs to the framed routes that apply to a PDU session. In this case, the association with the PDU session needs to be based on comparing the received UE address is within the one or more framed routes of the PDU session.

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

If the "TimeSensitiveNetworking" or the "TimeSensitiveCommunication" feature feature is supported, association is done by comparing the value of MAC address in the AF request with the MAC address of the DS-TT port as reported by the SMF within the TSC User Plane Node information.

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

NOTE 2: 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.

For 5G ProSe Layer-3 UE-to-Network Relay connectivity, the UE identity that the SMF has provided (i.e. 5G ProSe Layer-3 UE-to-Network Relay Identity) and the UE identity provided by the AF (i.e. 5G ProSe Layer-3 Remote UE Identity) may be different. In these scenarios, the PCF shall ignore the UE identity provided the AF, and applies the rest of received parameters, if available, to perform session binding.

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

NOTE 3: For 5G ProSe Layer-3 UE-to-Network Relay connectivity, to enable the PCF to distinguish the Relay scenario from other scenarios and hence ignore the received UE identify provided by the AF, a dedicated DNN for 5G ProSe Layer-3 UE-to-Network Relay connectivity needs to be configured in the PCF.

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

NOTE 4: 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 5: 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 6: For the Ethernet PDU session, the PCF needs to provision "UE_MAC_CH" trigger to the SMF.

NOTE 7: 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, described in 3GPP TS 23.501 [2] clause 5.7.2, 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, e.g. 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 (e.g. 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.

If "PvsSupport" feature defined in 3GPP TS 29.512 [9] is supported, and the Onboarding Network is an ON-SNPN, the authorization of PCC rule(s) associated with a PDU Session used for User Plane Remote Provisioning shall be supported without subscription information (e.g. information stored in the UDR). The PCF shall apply policies based on the locally stored Onboarding Configuration Data for this DNN and S-NSSAI combination.

NOTE 1: When the Onboarding Network is a PLMN or SNPN, the authorization of PCC rule(s) associated with a PDU Session used for User Plane Remote Provisioning is based on any 5GC specific restrictions and other information available to the PCF, e.g. user’s subscription information and operator policies (e.g., the list of allowed services within the user’s subscription and the PVS and DNS address(es) to be used in the SDF template of the PCC Rule(s) within the local configuration).

NOTE 2: 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.

The SMF shall bind a PCC rule to the default QoS flow as follows:

- For a non-GBR default QoS flow, the PCC rule(s) bound to the default QoS flow contains values of the non-GBR type 5QI, ARP, and if received, 5QI priority Level, that are identical to the corresponding values within the "authDefQos" attribute of the enforced session rule.
- For a GBR or delay critical GBR default QoS flow, the PCC rule bound to the default QoS flow contains a reference to a QoS data decision with the "defQosFlowIndication" attribute set to true and the authorized default QoS within the "authDefQos" attribute of the enforced session rule contains values of the GBR type or delay critical GBR type 5QI, ARP, GBR, MBR, and if available, 5QI priority Level, averaging window and maximum data burst volume.

When the QoS data decision which the PCC rule refers to include the "defQosFlowIndication" attribute set to true as defined in clause 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 clause 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 binds the PCC rule to the existing QoS flow, or based on local policies, or the below mentioned conditions (which QoS Flow binding shall ensure), require the establishment of a new QoS flow. If no QoS flow exists, the SMF creates 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 clause 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 clause 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.

Whenever the binding parameters of a PCC rule changes, the existing binding of this PCC rule shall be re-evaluated, i.e. the QoS flow binding procedure, is performed. The re-evaluation may, for a PCC rule, result in a new binding with another QoS flow. If the PCF requests the same change of the binding parameter value(s) for all PCC rules that are bound to the same QoS Flow, the SMF should not re-evaluate the binding of these PCC rules and instead, modify the QoS parameter value(s) of the QoS Flow accordingly.

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.

If the PCC rule is removed, the SMF shall remove the association of the PCC rule to the QoS flow. If the last PCC rule that is bound to a QoS Flow is removed, the SMF shall delete the QoS Flow.

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.

The QoS Flow binding shall also ensure that:

- If a dynamic value for the Core Network Packet Delay Budget (defined in 3GPP TS 23.501 [2] clause 5.7.3.4) is used, PCC rules with the same above binding parameters but different PDU Session anchors (i.e. the corresponding service data flows which have different CN PDBs) shall not be bound to the same QoS Flow.

NOTE 5: Different PDU Session anchors can exist if multiple RouteToLocation instances are included within the traffic control decision referred by the PCC rules.

- A PCC rule including TSCAI information is bound to a new QoS flow and no other PCC rule shall be bound to this same QoS flow. Whenever the TSC Assistance container of an existing PCC rule is changed, the binding of this PCC rule shall not be re-evaluated.

- For MA PDU Session, the QoS flow binding shall also ensure that the PCC rules for GBR or delay critical GBR service data flows allowed on different access are not bound to the same QoS flow even if the PCC rules contain the same binding parameters.

NOTE 6: For MA PDU Session, the GBR or delay critical GBR resource for a service data flow is allocated only in one access.

- When the PCF provisions a PCC rule with Alternative QoS parameter Set(s), the PCC rule is bound to a new QoS Flow and no other PCC rule is bound to this QoS Flow.

- When the PCF provisions a PCC rule with QoS Monitoring Policy, the PCC rule is bound to a new QoS flow and no other PCC rule is bound to this QoS flow.

NOTE 7: The binding of PCC rule with QoS Monitoring policy to a new QoS flow is only applicable to the Per QoS Flow per UE QoS Monitoring (as described in TS 23.501 [2] clause 5.33.3.2).

6.5 Binding mechanism in MBS deployments

6.5.1 Session Binding

MBS Session binding is the association of an AF Session information to one and only one MBS Session. When the PCF receives MBS Policy Association Create request or MBS Policy Association Update request from the MB-SMF and if the PCF does not receive MBS Service Information from the MB-SMF, the PCF shall perform the session binding and associate the MBS session with the existing IP data flows within the AF session information (and therefore the applicable MBS PCC rules). The PCF shall perform the session binding based on the MBS Session ID.

6.5.2 MBS PCC rule Authorization for an MBS session

The MBS PCC rule authorization is the selection of the 5G QoS parameters, described in 3GPP TS 23.247 [2] clause 6.10.1, for the MBS PCC rules.The PCF may perform the MBS PCC rule authorization in the following situations:

- When the MBS service information is received from the AF/NEF/MBSF. In this case, the MBS PCC rule authorization occurs at the reception of the information from the AF/NEF/MBSF.

- When the MBS service information is received from the MB-SMF. In this case, no session binding is performed.

By the authorization process the PCF determines whether the broadcast and multicast service is authorized. If so, the MBS PCC rules are created, modified or removed. If the session information is not authorized, a negative answer shall be issued to the NF that provided the information.

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

6.5.3 QoS flow binding within an MBS session

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

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

- 5QI;

- ARP;

- Priority Level (if available in the MBS PCC rule);

- Averaging Window (if available in the MBS PCC rule); and

- Maximum Data Burst Volume (if available in the MBS PCC rule).

The selected QoS flow shall have the same above binding parameters as the one indicated by the MBS PCC rule. The set of 5G QoS parameters assigned by the PCF to the service data flow is the main input for QFI allocation.

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

Whenever the binding parameters of an MBS PCC rule changes, the existing binding of this MBS PCC rule shall be re-evaluated, i.e. the QoS flow binding procedure, is performed. The re-evaluation may, for an MBS PCC rule, result in a new binding with another QoS flow. If the PCF requests the same change of the binding parameter value(s) for all MBS PCC rules that are bound to the same QoS Flow, the MB-SMF should not re-evaluate the binding of these MBS PCC rules and instead, modify the QoS parameter value(s) of the QoS Flow accordingly.

If the MBS PCC rule is removed, the MB-SMF shall remove the association of the MBS PCC rule to the QoS flow. If the last MBS PCC rule that is bound to a QoS Flow is removed, the MB-SMF shall delete the QoS Flow.

When a QoS flow is removed the MB-SMF shall report to the PCF that the MBS 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.

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.

For PCC deployments not supporting MBS, QoS parameters mapping functions are located at the AF, PCF, SMF and UE and are described in this clause and the rest of clauses under clause 7.

When PCC is deployed in an MBS architecture as defined in 3GPP TS 23.247 [54], QoS parameter mapping functions are defined as described in clause 7.5.

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].

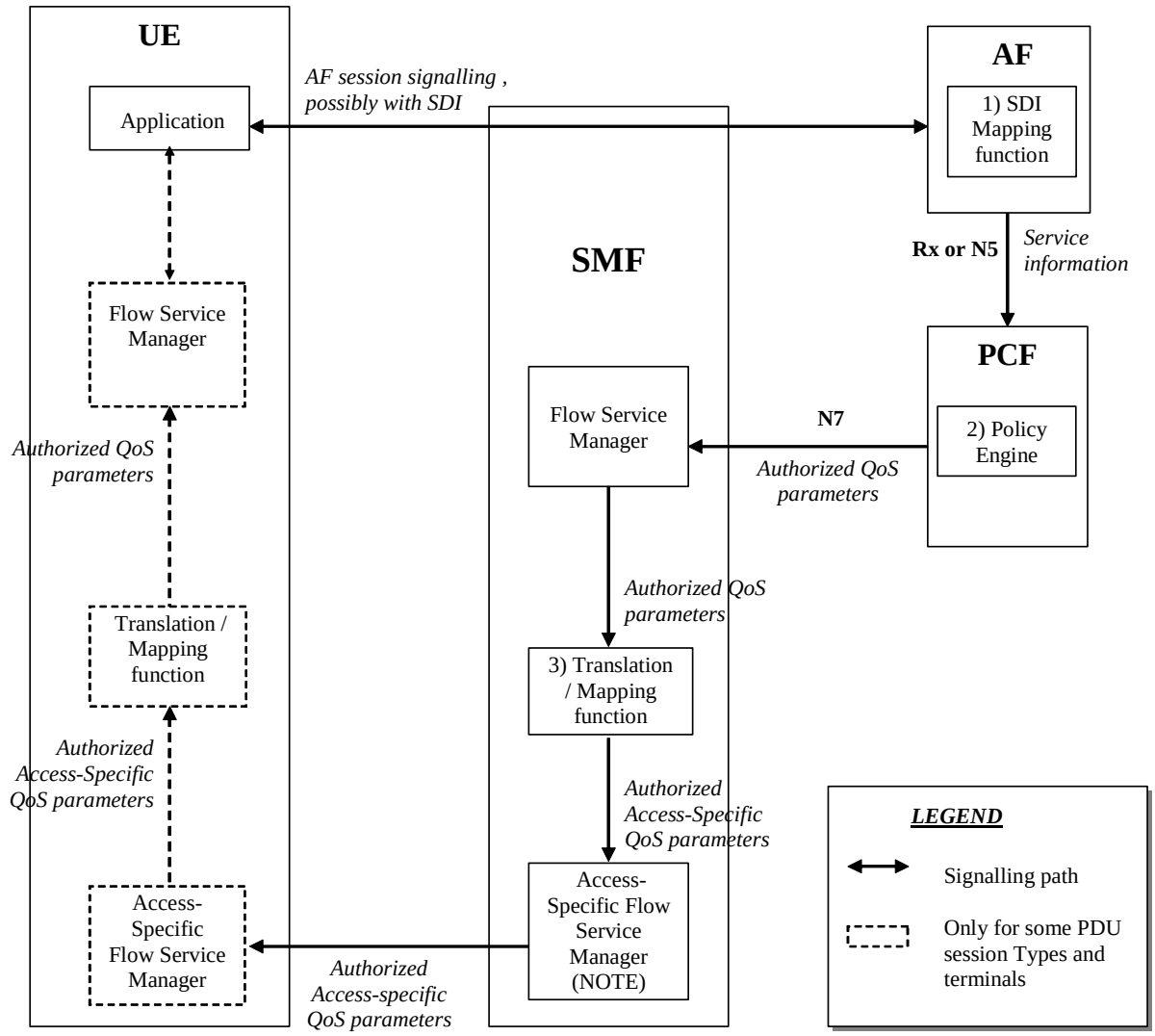
For IMS, the AF may pass service information to the PCF over the Rx interface or over the N5 interface if the PCF and the P-CSCF support the "IMS_SBI" feature. The AF derives information about the service from the SDI or from other sources. The mapping is application specific. If SDP (IETF RFC 4566 [16]) is used as SDI, the AF should apply the mapping described in clause 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]. Clause 7.2 specifies the QoS parameter mapping functions at the AF. For IMS, the mapping rules in clause 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. Clause 7.3 specifies the QoS mapping functions at the PCF applicable for all accesses.

The mapping functions located at SMF is specified in clause 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 clause 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 clause 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 for Rx interface or a "MediaComponent" attribute for N5 interface from the SDP Parameters. If the CHEM feature is supported, the P-CSCF may provide the maximum packet loss rate(s) for uplink and/or downlink direction(s) in the Max-PLR-DL AVP and/or

the Max-PLR-UL AVP for Rx interface respectively as defined in clause 7.2.2 or the "maxPacketLossRateUl" attribute and/or "maxPacketLossRateDl" attribute respectively as defined in clause 7.2.3.

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 clause 6.2 of 3GPP TS 29.213 [30].

7.2.3 AF supporting N5 interface

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 P-CSCF shall use the mapping rules in table 7.2.3-1 for each SDP media component to derive a media component entry of the "medComponents" attribute from the SDP Parameters. The mapping shall not apply to media components where the SDP payload is proposing to use a circuit-switched bearer (i.e. "c=" line set to "PSTN" and an "m=" line set to "PSTN", refer to 3GPP TS 24.292 [35]). Circuit-switched bearer related media shall not be included in the service information sent to the PCF.

Table 7.2.3-1: Rules for derivation of service information within Media Component Description from SDP media component

Service information per Media Component-Description (see NOTE 1 and NOTE 7)	Derivation from SDP Parameters (see NOTE 2)
Media Component Number	ordinal number of the position of the "m=" line in the SDP
AF Application Identifier	The "afAppId" attribute may be supplied or omitted, depending on the application. For IMS, if the "afAppId" attribute is supplied, its value should not demand application specific bandwidth or QoS characteristics handling unless the IMS application is capable of handling a QoS downgrading.
Media Type	The "medType" attribute shall be included with the same value as supplied for the media type in the "m=" line.

Flow Status	IF port in m-line = 0 THEN
	"fStatus" := REMOVED;
	ELSE
	IF Transport in m-line is "TCP" or "TCP/MSRP" THEN (NOTE 9)
	"fStatus" := ENABLED;
	ELSE /* UDP or RTP/AVP transport
	IF a=rtcp-mux is negotiated THEN
	"fStatus" :=ENABLED; (NOTE 12 and 13)
	ELSE
	IF a=recvonly THEN
	IF <SDP direction> = UE originated (NOTE 8) THEN
	"fStatus" := ENABLED-DOWNLINK; (NOTE 4)
	ELSE /* UE terminated (NOTE 8) */
	"fStatus" := ENABLED-UPLINK; (NOTE 4)
	ENDIF;
	ELSE
	IF a=sendonly THEN
	IF <SDP direction> = UE originated (NOTE 8) THEN
	"fStatus" := ENABLED-UPLINK; (NOTE 4)
	ELSE /* UE terminated (NOTE 8) */
	"fStatus" := ENABLED-DOWNLINK; (NOTE 4)
	ENDIF;
	ELSE
	IF a=inactive THEN
	"fStatus" :=DISABLED;
	ELSE /* a=sendrecv or no direction attribute */
	"fStatus" := ENABLED (NOTE 4)
	ENDIF;
	ENDIF;
	ENDIF;
	ENDIF;
	ENDIF;
	ENDIF;
	(NOTE 5)

Service information per Media Component-Description (see NOTE 1 and NOTE 7)	Derivation from SDP Parameters (see NOTE 2)

Max Requested Bandwidth-UL	IF <SDP direction> = UE terminated (NOTE 8) THEN
	  IF Transport in m-line is "TCP" or "TCP/MSRP" THEN (NOTE 9)
	  IF a=recvonly or a=sendrecv or no direction attribute THEN
	  IF b=AS:<bandwidth> is present and
	  (b=TIAS:<Tibandwidth> is not
	  present or is present but not supported) THEN
	  "marBwUl" := <bandwidth> * 1000; /* Unit bit/s
	  ELSE
	  IF b=TIAS:<Tibandwidth> is present and supported THEN
	  "marBwUl" := <Transport-dependent bandwidth>
	  (NOTE 11) /* Unit bit/s
	  ELSE
	  "marBwUl" := <Operator specific setting>;
	  ENDIF;
	  ENDIF;
	  ELSE
	  "marBwUl" := <Operator specific setting>,
	  (NOTE 10)
	  ENDIF;
	  ELSE /* UDP or RTP/AVP transport
	  IF b=AS:<bandwidth> is present and
	  (b=TIAS:<Tibandwidth> is not
	  present or is present but not supported) THEN
	  IF a=rtcp-mux is negotiated(NOTE 13) THEN
	  IF b=RR:<rrbandwidth> is present
	  OR b=RS:<rsbandwidth> is present THEN
	  "marBwUl" := <bandwidth> * 1000 +
	  <rrbandwidth> + <rsbandwidth>; (NOTE 3; NOTE 6)
	  ELSE
	  "marBwUl" := <bandwidth> * 1050;
	  /* Unit is bit/s
	  ENDIF
	  ELSE
	  "marBwUl" := <bandwidth> * 1000;
	  /* Unit is bit/s
	  ENDIF;
	  ELSE
	  IF b=TIAS:<Tibandwidth> is present and supported THEN
	  IF a=rtcp-mux is negotiated (NOTE 13) THEN
	  IF b=RR:<rrbandwidth> is present
	  OR b=RS:<rsbandwidth> is present THEN
	  "marBwUl" :=
	  <Transport-dependent bandwidth> (NOTE 11) +
	  <rrbandwidth> + <rsbandwidth>; (NOTE 3; NOTE 6)
	  ELSE
	  "marBwUl" :=
	  <Transport-dependent bandwidth>
	  * 1.05 (NOTE 11) /* Unit bit/s
	  ENDIF
	  ELSE
	  "marBwUl" := <Transport-dependent bandwidth>
	  (NOTE 11) /* Unit bit/s
	  ENDIF;
	  ELSE
	  "marBwUl" := <Operator specific setting>,
	  or attribute not supplied;
	  ENDIF;
	  ENDIF;
	  ENDIF
	ELSE
	  Consider SDP in opposite direction
	ENDIF

Service information per Media Component-Description (see NOTE 1 and NOTE 7)	Derivation from SDP Parameters (see NOTE 2)

Max Requested Bandwidth DL	IF <SDP direction> = UE originated (NOTE 8) THEN
	  IF Transport in m-line is "TCP" or "TCP/MSRP" THEN (NOTE 9)
	  IF a=recvonly or a=sendrecv or no direction attribute THEN
	  IF b=AS:<bandwidth> is present and
	  (b=TIAS:<Tibandwidth> is not present or
	
	  is present but not supported) THEN
	  "marBwDl" := <bandwidth> * 1000; /* Unit bit/s
	  ELSE
	  IF b=TIAS:<Tibandwidth> is present and supported THEN
	  "marBwDl" := <Transport-dependant bandwidth>
	  /* Unit bit/s (see NOTE 11)
	  OR Operator specific setting
	  ELSE
	  "marBwDl" := <Operator specific setting>;
	  ENDIF;
	  ELSE
	  "marBwDl" := <Operator specific setting>,
	  (NOTE 10)
	  ENDIF;
	  ELSE /* UDP or RTP/AVP transport
	  IF b=AS:<bandwidth> is present and b=TIAS:<Tibandwidth> is not present THEN
	  IF a=rtcp-mux is negotiated(NOTE 13) THEN
	  IF b=RR:<rrbandwidth> is present
	  OR b=RS:<rsbandwidth> is present THEN
	  "marBwDl" := <bandwidth> * 1000 +
	  <rrbandwidth> + <rsbandwidth>; (NOTE 3; NOTE 6)
	  ELSE
	  "marBwDl" := <bandwidth> * 1050;
	  /* Unit is bit/s
	  ENDIF
	  ELSE
	  "marBwDl" := <bandwidth> * 1000
	  ;/* Unit is bit/s
	  ENDIF;
	  ELSE
	  IF b=TIAS:<Tibandwidth> is present THEN
	  IF a=rtcp-mux is negotiated (NOTE 13) THEN
	  IF b=RR:<rrbandwidth> is present
	  OR b=RS:<rsbandwidth> is present THEN
	  "marBwDl" :=
	  <Transport-dependent bandwidth> (NOTE 11) +
	  <rrbandwidth> + <rsbandwidth>; (NOTE 3; NOTE 6)
	  ELSE
	  "marBwDl" :=
	  <Transport-dependent bandwidth>
	  * 1.05 (NOTE 11) /* Unit bit/s
	  ENDIF
	  ELSE
	  "marBwDl" := <Transport-dependent bandwidth>
	  (NOTE 11) /* Unit bit/s
	  ENDIF;
	  ELSE
	  "marBwDl":= <Operator specific setting>,
	  or attribute not supplied;
	  ENDIF;
	  ENDIF;
	  ENDIF
	ELSE
	  Consider SDP in opposite direction
	ENDIF

Max Supported Bandwidth-UL	IF a=bw-info is present and includes MaxSupBw: <bandwidth> and direction: recv (UE terminated) or send (UE originated) or sendrecv (NOTE 14) THEN
	  "maxSuppBwUl":= [supplied <bandwidth>] * 1000 /Unit bit/s/
	
	(NOTE 16)
	ELSE /* a=bw-info is not present or is present but MaxSupBw is not included or direction is the opposite
	  Attribute not supplied
	ENDIF;
	(NOTE 15)

Service information per Media Component-Description (see NOTE 1 and NOTE 7)	Derivation from SDP Parameters (see NOTE 2)
Max Supported Bandwidth-DL	IF a=bw-info is present and includes MaxSupBw : <bandwidth> and direction: send (UE terminated) or recv (UE originated) or sendrecv (NOTE 14)THEN "maxSuppBwDl":= [supplied <bandwidth>] * 1000 /Unit bit/s/ (NOTE 16) ELSE /* a=bw-info is not present or is present but MaxSupBw is not included or direction is the opposite Attribute not supplied ENDIF; (NOTE 15)

Min Desired Bandwidth UL	IF a=bw-info is present and includes MinDesBw : <bandwidth> and direction: recv (UE terminated) or send (UE originated) or sendrecv (NOTE 14) THEN
	"minDesBwUl" := supplied <bandwidth> * 1000 /Unit bit/s/
	
	(NOTE 16)
	ELSE /* a=bw-info is not present or is present but MinDesBw is not included or direction is the opposite
	Attribute not supplied
	ENDIF;

Min Desired Bandwidth DL	IF a=bw-info is present and includes MinDesBw : <bandwidth> and direction: send (UE terminated) or recv (UE originated) or sendrecv (NOTE 14) THEN
	"minDesBwDl":= [supplied <bandwidth>] * 1000 /Unit bit/s/
	(NOTE 16)
	ELSE /* a=bw-info is not present or is present but MinDesBw is not included or direction is the opposite
	Attribute not supplied
	ENDIF;

RR Bandwidth	IF b=RR:<bandwidth> is present THEN
	"rrBw":= <bandwidth>;
	ELSE
	Attribute not supplied
	ENDIF;
	(NOTE 3; NOTE 6)

RS Bandwidth	IF b=RS:<bandwidth> is present THEN
	"rsBw" := <bandwidth>;
	ELSE
	Attribute not supplied
	ENDIF;
	(NOTE 3: NOTE 6)

Service information per Media Component-Description (see NOTE 1 and NOTE 7)	Derivation from SDP Parameters (see NOTE 2)
Media SubComponent	Supply one attribute for bidirectional combination of two corresponding IP flows, if available, and for each single IP flow without a corresponding IP flow in opposite direction. If a media component comprises separate IP flows for RTP and RTCP, they are described in two separate Media SubComponent. However, if a=rtcp-mux is negotiated, RTP and RTCP use the same IP flow and shall be described in a single MediaSubComponent entry of the "medSubcomps" attribute. The encoding of the "medSubcomps" attribute is described in table 6.2.2
Reservation Priority	The AF may supply or omit the "resPrio" attribute. (NOTE 17)
Codec Data	The "codecs" are provisioned as specified in clause 5.6.2.7 of 3GPP TS 29.514 [10], including the codec-related information detailed in clause 5.6.3.2 of 3GPP TS 29.514 [10].

Maximum Packet Loss Rate DL	IF a= PLR_adapt line is NOT present in both SDP OFFER and ANSWER THEN
	/* As UE don't support CHEM feature, AF should not use packet loss rates in either the uplink or downlink direction */
	maxPacketLossRateDl attribute not supplied
	ELSE
	IF P-CSCF serving the OFFERER THEN
	FOR each RTP payload type of the same media line
	IF MAXimum-e2e-PLR line is present in the SDP OFFER THEN
	IF maxUL-PLR is present in the SDP ANSWER
	maxPacketLossRateDl = value of maxe2e-PLR in the SDP OFFER - maxUL-PLR
	in the SDP ANSWER
	ELSE /* maxUL-PLR is not present in the SDP ANSWER */
	MaxPacketLossRateDl = the default value is ½ maxe2e-PLR value present
	in the SDP OFFER
	ELSE /* MAXimum-e2e-PLR line is not present in the SDP OFFER */
	IF maxUL-PLR is present in the SDP ANSWER THEN
	maxPacketLossRateDl = (the default value is end-to-end Maximum End-to-End Packet Loss Rate for the decoder of the RTP payload type as recommended in 3GPP TS 26.114 [14] clause X.1.2 for application layer redundancy or X.1.1 for partial redundancy) - maxUL-PLR in the SDP ANSWER
	ELSE /* maxUL-PLR is not present in the SDP ANSWER */
	maxPacketLossRateDl = the default value is ½ end-to-end Maximum End-to-End
	Packet Loss Rate for the decoder of the RTP payload type as recommended in 3GPP TS 26.114 [14] clause X.1.2 for application layer redundancy or X.1.1 for partial redundancy
	ENDIF;
	ENDIF;
	END FOR LOOP of each RTP payload type of the same media
	maxPacketLossRateDl = maximum value of Max-PLR-DL among all the RTP payload
	types
	ELSE /* For P-CSCF serving the ANSWERER */
	FOR each RTP payload type of the same media line
	IF MAXimum-e2e-PLR line is present in the SDP ANSWER THEN
	IF maxDL-PLR is present in the SDP ANSWER
	maxPacketLossRateDl = value of maxDL-PLR in the SDP ANSWER
	ELSE /* maxDL-PLR is not present in the SDP ANSWER */
	maxPacketLossRateDl = the default value is ½ maxe2e-PLR value present
	in the SDP ANSWER
	ELSE /* MAXimum-e2e-PLR line is not present in the SDP ANSWER */
	maxPacketLossRateDl = the default value is ½ end-to-end Maximum End-to-End
	Packet Loss Rate for the decoder of the RTP payload type as recommended in 3GPP TS 26.114 [14] clause X.1.2 for application layer redundancy or X.1.1 for partial redundancy
	ENDIF;
	END FOR LOOP of each RTP payload type of the same media
	maxPacketLossRateDl = maximum value of Max-PLR-DL among all the RTP payload
	types
	ENDIF;
	ENDIF;
	ENDIF;

Service information per Media Component-Description (see NOTE 1 and NOTE 7)	Derivation from SDP Parameters (see NOTE 2)

Maximum Packet Loss Rate UL	IF a= PLR_adapt line is NOT present in both SDP OFFER and ANSWER THEN
	/* As UE don't support CHEM feature, AF should not use packet loss rates in either the uplink or downlink direction */
	maxPacketLossRateUl attribute not supplied
	ELSE
	IF P-CSCF serving the OFFERER THEN
	FOR each RTP payload type of the same media line
	IF MAXimum-e2e-PLR line is present in the SDP ANSWER THEN
	IF maxDL-PLR is present in the SDP ANSWER
	maxPacketLossRateUl = value of maxe2e-PLR in the SDP ANSWER - maxDL-PLR
	in the SDP ANSWER
	ELSE /* maxDL-PLR is not present in the SDP ANSWER */
	maxPacketLossRateUl = the default value is ½ maxe2e-PLR value present
	in the SDP ANSWER
	ELSE /* MAXimum-e2e-PLR line is not present in the SDP ANSWER */
	maxPacketLossRateUl = the default value is ½ end-to-end Maximum End-to-End
	Packet Loss Rate for the decoder of the RTP payload type as recommended in 3GPP TS 26.114 [14] clause X.1.2 for Application layer redundancy or X.1.1 for partial redundancy
	ENDIF;
	END FOR LOOP of each RTP payload type of the same media
	maxPacketLossRateUl = maximum value of Max-PLR-UL among all the RTP payload
	types
	ELSE /* For P-CSCF serving the ANSWERER */
	FOR each RTP payload type of the same media line
	IF MAXimum-e2e-PLR line is present in the SDP OFFER THEN
	IF maxUL-PLR is present in the SDP ANSWER
	maxPacketLossRateUl = value of maxUL-PLR in the SDP ANSWER
	ELSE /* maxUL-PLR is not present in the SDP ANSWER */
	maxPacketLossRateUl = the default value is ½ maxe2e-PLR value present
	in the SDP OFFER
	ELSE /* MAXimum-e2e-PLR line is not present in the SDP OFFER */
	maxPacketLossRateUl = the default value is ½ end-to-end Maximum End-to-End
	Packet Loss Rate for the decoder of the RTP payload type as recommended in 3GPP TS 26.114 [14] clause X.1.2 for Application layer redundancy or X.1.1 for partial redundancy
	ENDIF;
	END FOR LOOP of each RTP payload type of the same media
	maxPacketLossRateUl = maximum value of Max-PLR-UL among all the RTP payload
	types
	ENDIF;
	ENDIF;
	ENDIF;

Service information per Media Component-Description (see NOTE 1 and NOTE 7)	Derivation from SDP Parameters (see NOTE 2)

Desired-Max-Latency	IF <SDP direction> = UE originated (NOTE 8) THEN
	  IF a=3gpp-qos-hint is present and includes a qos-hint-property that indicates "latency"
	  IF qos-hint-split-value for "local" is not present
	  "desMaxLatency" = <qos-hint-end-to-end-value>*0.5
	  ELSE /* qos-hint-split-value for "local" is present
	  "desMaxLatency" = <qos-hint-split-value>
	  ENDIF
	  ELSE
	  Attribute not supplied
	  ENDIF
	ELSE /* <SDP direction> = UE terminated (NOTE 8)/
	  IF a=3gpp-qos-hint is present and includes a qos-hint-property that indicates "latency"
	  IF qos-hint-split-value for "local" is not present
	  "desMaxLatency" = <qos-hint-end-to-end-value>*0.5
	  ELSE /* qos-hint-split-value for "local" is present/
	  "desMaxLatency" = <qos-hint-end-to-end-value> - <qos-hint-split-value>
	  ENDIF
	  ELSE
	  Attribute not supplied
	  ENDIF
	ENDIF

Desired-Max-Loss	IF <SDP direction> = UE originated (NOTE 8) THEN
	  IF a=3gpp-qos-hint is present and includes a qos-hint-property that indicates "loss"
	  IF qos-hint-split-value for "local" is not present
	  "desMaxLoss" = <qos-hint-end-to-end-value>*0.5
	  ELSE /* qos-hint-split-value for "local" is present/
	  "desMaxLoss" = <qos-hint-split-value>
	  ENDIF
	  ELSE
	  Attribute not supplied
	  ENDIF
	ELSE /* <SDP direction> = UE terminated (NOTE 8)/
	  IF a=3gpp-qos-hint is present and includes a qos-hint-property that indicates "loss"
	  IF qos-hint-split-value for "local" is not present
	  "desMaxLoss" = < qos-hint-end-to-end-value>*0.5
	  ELSE /* qos-hint-split-value for "local" is present/
	  "desMaxLoss" = <qos-hint-end-to-end-value> - <qos-hint-split-value>
	  ENDIF
	  ELSE
	  Attribute not supplied
	  ENDIF
	ENDIF

Service information per Media Component-Description (see NOTE 1 and NOTE 7)	Derivation from SDP Parameters (see NOTE 2)

NOTE 1: The encoding of the service information is defined in 3GPP TS 29.514 [10].
NOTE 2: The SDP parameters are described in IETF RFC 4566 [16].
NOTE 3: The "b=RS:" and "b=RR:" SDP bandwidth modifiers are defined in IETF RFC 3556 [36].
NOTE 4: As an operator policy to disable forward and/or backward early media, for media with UDP as transport protocol only the "fStatus" attribute may be downgraded by using the gate control procedures defined in the annex B of 3GPP TS 29.514 [10] before a SIP confirmed dialogue is established, i.e. until a 200 (OK) response to an INVITE request is received.
NOTE 5: If the SDP answer is available when the session information is derived, the direction attributes and port number from the SDP answer shall be used to derive the flow status. However, to enable interoperability with SIP clients that do not understand the inactive SDP attribute, if "a=inactive" was supplied in the SDP offer, this shall be used to derive the flow status. If the SDP answer is not available when the session information is derived, the direction attributes from the SDP offer shall be used.
NOTE 6: Information from the SDP answer is applicable, if available.
NOTE 7: The attributes may be omitted if they have been supplied in previous service information and have not changed, as detailed in 3GPP TS 29.514 [10].
NOTE 8: "Uplink SDP" indicates that the SDP was received from the UE and sent to the network. This is equivalent to <SDP direction> = UE originated.
"Downlink SDP" indicates that the SDP was received from the network and sent to the UE. This is equivalent to <SDP direction> = UE terminated.
NOTE 9: Support for TCP at a P-CSCF acting as AF is only required if services with TCP transport are used in the corresponding IMS system.
As an operator policy to disable forward and/or backward early media, for media with TCP as transport protocol, the "marBwUl"/"maxBwDl" attribute values may be downgraded before a SIP confirmed dialogue is established, i.e. until a 200 (OK) response to an INVITE request is received. Only a small bandwidth in both directions is required in this case in order for TCP control packets to flow.
NOTE 10: TCP uses IP flows in the directionality opposite to the transferred media for feedback. To enable these flows, a small bandwidth in this direction is required.
NOTE 11: TIAS is defined in IETF RFC 3890 [37]. IETF RFC 3890 clause 6.4 provides procedures for converting TIAS to transport-dependant values. This procedure relies on the presence of maxprate (also defined in IETF RFC 3890).
NOTE 12: Multiplexed RTP/RTCP flows need to have "fStatus" attribute set to "ENABLED" in order to always permit the RTCP traffic.
NOTE 13: RTP/RTCP multiplexing is defined in IETF RFC 5761 [38].
NOTE 14: This attribute is derived from the SDP answer information and is omitted if E2EQOSMTSI feature is not supported.
NOTE 15: When both "b =" line and "a=bw-info" including MaxSupBw are present when sending the SDP, it is expected that the values are aligned.
NOTE 16: When the supplied bandwidth does not correspond to the bandwidth applicable to the IP version used by the UE, the AF shall re-compute it considering the IP version used by the UE as defined in 3GPP TS 26.114 [14].
NOTE 17: When the AF recognizes the need to request prioritized access to system resources, the AF shall include the "resPrio" attribute as described in 3GPP TS 29.514 [10]. Various mechanisms used by the P-CSCF to determine if the request is eligible for priority treatment are specified in clause 4.11 of 3GPP TS 24.229 [41] (e.g. based on the Resource Priority header field as described in IETF RFC 4412 [42] or a special dialstring contained in the SIP message).

Table 7.2.3-2: Rules for derivation of Media SubComponent from SDP media component

Service information per Media SubComponent (see NOTE 1 and NOTE 5)	Derivation from SDP Parameters (see NOTE 2)
Flow Number	The AF shall assign a number to the media subcomponent that is unique within the surrounding media component entries included in a "medComponents" attribute and for the entire lifetime of the AF session. The AF shall select the ordinal number of the IP flow(s) within the "m=" line assigned in the order of increasing downlink destination port numbers, if downlink destination port numbers are available. For uplink or inactive unicast media IP flows, a downlink destination port number is nevertheless available, if SDP offer-answer according to IETF RFC 3264 [43] is used. The AF shall select the ordinal number of the IP flow(s) within the "m=" line assigned in the order of increasing uplink destination port numbers, if no downlink destination port numbers are available.
Flow Status	Attribute not supplied
Max Requested Bandwidth UL	Attribute not supplied
Max Requested Bandwidth DL	Attribute not supplied

Flow Description	For uplink and downlink direction, a Flow Description entry within the "fDescs" attribute shall be provided unless no IP Flows in this direction are described within the media component.
	
	If UDP is used as transport protocol, the SDP direction attribute (NOTE 4) indicates the direction of the media IP flows within the media component as follows:
	IF a=recvonly THEN (NOTE 3)
	IF <SDP direction> = UE originated (NOTE 7) THEN
	Provide only downlink entry within the "fDescs" attribute
	ELSE /* UE terminated (NOTE 7) */
	Provide only uplink entry within "fDescs" attribute
	ENDIF;
	ELSE
	IF a=sendonly THEN (NOTE 3)
	IF <SDP direction> = UE originated (NOTE 7) THEN
	Provide only uplink entry within the "fDescs" attribute
	ELSE /* UE terminated (NOTE 7) */
	Provide only downlink entry within the "fDescs" attribute
	ENDIF;
	ELSE /* a=sendrecv or a=inactive or no direction attribute */
	Provide uplink and downlink for "fDescs" attribute
	ENDIF;
	ENDIF;
	However, for RTCP and RTP/RTCP multiplexed IP flows uplink and downlink Flow Description entries within "fDescs" attribute shall be provided irrespective of the SDP direction attribute.
	
	If TCP is used as transport protocol (NOTE 8), IP flows in uplink and downlink direction are described in SDP irrespective of the SDP direction attribute, as TCP uses an IP flow for feedback even if contents are transferred only in the opposite direction. Thus, both uplink and downlink Flow Description entries within "fDescs" attribute shall be provided.
	
	The uplink destination address shall be copied from the "c=" line of downlink SDP. (NOTE 6) (NOTE 7)
	The uplink destination port shall be derived from the "m=" line of downlink SDP. (NOTE 6) (NOTE 7) However, for TCP transport the uplink destination port shall be wildcarded, if the local UE is the passive endpoint (NOTE 9)
	
	The downlink destination address shall be copied from the "c=" line of uplink SDP. (NOTE 6) However, a P-CSCF acting as AF and applying NAT traversal procedures in Annex C shall derive the downlink destination address using those procedures.
	The downlink destination port shall be derived from the "m=" line of uplink SDP. (NOTE 6) (NOTE 7) However, for TCP transport the downlink destination port shall be wildcarded, if the local UE is the active endpoint (NOTE 9). A P-CSCF acting as AF and applying NAT traversal procedures in Annex C shall derive the downlink destination port using those procedures.
	
	For IPv6, uplink and downlink source addresses shall either be derived from the prefix of the destination address or be wildcarded by setting to "any", as specified in 3GPP TS 29.514 [10]. However, a P-CSCF acting as AF and applying NAT traversal procedures in Annex B shall derive the uplink source address using those procedures.
	If IPv4 is being utilized, the uplink source address shall either be set to the address contained in the "c=" line of the uplink SDP or be wildcarded, and the downlink source address shall either be set to the address contained in the "c=" line of the downlink SDP or be wildcarded. However, for TCP transport, if the local UE is the passive endpoint (NOTE 9), the uplink source address shall not be wildcarded. If the local UE is the active endpoint (NOTE 9), the downlink source address shall not be wildcarded. A P-CSCF acting as AF and applying NAT traversal procedures in Annex C shall derive the uplink source address using those procedures.
	
	Source ports shall not be supplied. However, for TCP transport, if the local UE is the passive end point (NOTE 9), the uplink source port shall be derived from the "m=" line of the uplink SDP. If the local UE is the active end point (NOTE 9), the downlink source port shall be derived from the "m=" line of the downlink SDP. A P-CSCF acting as AF and applying NAT traversal procedures in Annex B shall derive the downlink source ports using those procedures.
	
	Proto shall be derived from the transport of the "m=" line. For "RTP/AVP" proto is 17(UDP). For "TCP", as defined in IETF RFC 4145 [39], or "TCP/MSRP", as defined in IETF RFC 4975 [40], proto is 6(TCP).

Flow Usage	The "flowUsage" attribute shall be supplied with value "RTCP" if the IP flow(s) described in the Media SubComponent are used to transport RTCP

Service information per Media SubComponent (see NOTE 1 and NOTE 5)	Derivation from SDP Parameters (see NOTE 2)
	only. Otherwise the "flowUsage" attribute shall not be supplied. IETF RFC 4566 [16] specifies how RTCP flows are described within SDP. If the IP flows(s) are used to transport signalling the value should be "AF-SIGNALLING"

NOTE 1: The encoding of the service information is defined in 3GPP TS 29.514 [10].
NOTE 2: The SDP parameters are described in IETF RFC 4566 [16].
NOTE 3: If the SDP direction attribute for the media component negotiated in a previous offer-answer exchange was sendrecv, or if no direction attribute was provided, and the new SDP direction attribute sendonly or recvonly is negotiated in a subsequent SDP offer-answer exchange, uplink and downlink within the "fDescs" attribute shall be supplied.
NOTE 4: If the SDP answer is available when the session information is derived, the direction attributes from the SDP answer shall be used to derive the flow description. However, to enable interoperability with SIP clients that do not understand the inactive SDP attribute, if "a=inactive" was supplied in the SDP offer, this shall be used. If the SDP answer is not available when the session information is derived, the direction attributes from the SDP offer shall be used.
NOTE 5: The attributes may be omitted if they have been supplied in previous service information and have not changed, as detailed in 3GPP TS 29.514 [10].
NOTE 6: If the session information is derived from an SDP offer, the required SDP may not yet be available. The corresponding "fDescs" attribute shall nevertheless be included and the unavailable fields (possibly all) shall be wildcarded.
NOTE 7: "Uplink SDP" indicates that the SDP was received from the UE and sent to the network. This is equivalent to <SDP direction> = UE originated.
"Downlink SDP" indicates that the SDP was received from the network and sent to the UE. This is equivalent to <SDP direction> = UE terminated.
NOTE 8: Support for TCP at a P-CSCF acting as AF is only required if services with TCP transport are used in the corresponding IMS system.
NOTE 9: For TCP transport, the passive endpoints are derived from the SDP "a=setup" attribute according to the rules in IETF RFC 4145 [39], or, if that attribute is not present, from the rules in IETF RFC 4975 [40].

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, 7,14, 15 and 17)	IF an operator special policy exists THEN
	5QI:= as defined by operator specific algorithm; (NOTE 18)
	
	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 FLUS-Identifier AVP demands specific QoS Class handling THEN
	5QI:= as defined by specific algorithm; (NOTE 16)
	
	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 ;

Authorized QoS Parameter	Derivation from service information (see 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 29.214 [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 clause 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].	
NOTE 15: In a network where SRVCC is enabled, the 5QI=1 shall be used for IMS services in accordance to 3GPP TS 23.216 [44]. Non-IMS services using 5QI=1 may suffer service interruption and/or inconsistent service experience if SRVCC is triggered. Triggering SRVCC for WebRTC IMS session will cause service interruption and/or inconsistent service experience when using 5QI=1. Operator policy (e.g. use of specific AF application identifier) may be used to avoid using 5QI 1 for a voice service, e.g. WebRTC IMS session.	
NOTE 16: The "live" uplink streaming algorithm may consider various inputs, including the received FLUS-Identifier AVP, Desired-Max-Latency AVP, Desired-Max-Loss AVP, AF-Application-Identifier and Media-Type AVP for deriving the 5QI. When Desired-Max-Latency AVP and/or Desired-Max-Loss AVP are present, non-authority 5QI mapping may be done according to table 5.7.4-1 in 3GPP TS 23.501 [2].	
NOTE 17: The algorithm to support applications with specific QoS hints (e.g. loss and/or latency demands) may consider various inputs, including the received Desired-Max-Latency AVP, Desired-Max-Loss AVP and AF-Application-Identifier AVP for deriving the 5QI, as shown in table E.0 in 3GPP TS 26.114 [14]. Non-authority 5QI mapping may be done according to table 5.7.4-1 in 3GPP TS 23.501 [2].	
NOTE 18: Operator specific policies may consider access information for policy decision. E.g., in a network where the PDU session can be carried over NR satellite access or satellite backhaul, the PCF may take this information into account (together with any delay requirements provided by the AF) to determine the applicable policy decision, as e.g. the 5QI value.	

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: For home-routed scenarios, if the "VPLMN-QoS-Control" feature as defined in 3GPP TS 29.512 [9] is supported, if the PCF applies the rules in table 7.3.2-2 to calculate the authorized QoS to be transported within the PDU session, the PCF can adapt the authorized QoS associated to the PDU session to take into account the values that can be accepted by the VPLMN.

NOTE 2: QoS Information related to Maximum Authorized UL/DL Data Rate provided at PDU session level is not derived based on mapping tables in this clause, but based on subscription and operator specific policies.

NOTE 3: 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, Maximum Authorized QoS Class and other authorized QoS parameters 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 the qosReference attribute of MediaComponent data type corresponds to a pre-defined QoS information set THEN
	Max_DR_UL:= as configured by operator
	Max_DR_DL:= as configured by operator;
	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;

Authorized QoS Parameter	Derivation from service information (NOTE 4)
	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;
	
	ELSE IF 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 the qosReference attribute of MediaComponent data type corresponds to a pre-defined QoS information set THEN
	Gua_DR_UL:= as configured by operator
	Gua_DR_DL:= as configured by operator;
	ELSE IF the altSerReqs attribute of MediaComponent data type corresponds to a list of pre-defined QoS information set THEN for each pre-defined QoS information set:
	Gua_DR_UL:= as configured by operator;
	Gua_DR_DL:= as configured by operator; (NOTE 16)
	ELSE IF the altSerReqsData attribute of MediaComponent data type corresponds to a list of alternative service requirements that include Requested Alternative QoS parameter Set(s) THEN for each QoS information set:
	Gua_DR_UL:= gbrUl value;
	Gua_DR_DL:= gbrDl value (NOTE 16);
	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 QoS Parameter	Derivation from service information (NOTE 4)

Authorized 5G QoS Identifier (5QI) (see NOTE 1, 2, 3, 7 ,12, 14 and 17)	IF an operator special policy exists THEN
	5QI:= as defined by operator specific algorithm; (NOTE 18)
	ELSE IF mpsId attribute demands MPS specific QoS Class handling THEN
	5QI:= as defined by MPS specific algorithm (NOTE 11);
	ELSE IF mcsId attribute demands MCS specific QoS Class handling THEN
	5QI:= as defined by MCS specific algorithm (NOTE 13);
	ELSE IF AF Application Identifier demands application specific QoS Class handling THEN
	5QI:= as defined by application specific algorithm;
	ELSE IF flusId attribute demands specific QoS Class handling THEN
	5QI:= as defined by specific algorithm; (NOTE 15)
	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 IF the qosReference attribute of MediaComponent data type corresponds to a pre-defined QoS information set THEN
	5QI:= as configured by operator;
	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 */
	ENDIF;
	ENDIF;
	ENDIF;

Authorized Packet Delay Budget (PDB) for Alternative QoS parameter Sets	IF the altSerReqs attribute of MediaComponent data type corresponds to a list of pre-defined QoS information set THEN for each pre-defined QoS information set: PDB:= as configured by operator; (NOTE 16) ELSE IF the altSerReqsData attribute of MediaComponent data type corresponds to a list of alternative service requirements that include Requested Alternative QoS parameter Set(s) THEN for each QoS information set: PDB:= pdb value; ENDIF;
Authorized Packet Error Rate (PER) for Alternative QoS parameter Sets	IF the altSerReqs attribute of MediaComponent data type corresponds to a list of pre-defined QoS information set THEN for each pre-defined QoS information set: PER:= as configured by operator; (NOTE 16) ENDIF;

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 clause 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].
NOTE 13: The MCS specific algorithm shall consider various inputs, including the received mcsId and resPrio attributes, for deriving the 5QI.
NOTE 14: In a network where SRVCC is enabled, the 5QI=1 shall be used for IMS services in accordance to 3GPP TS 23.216 [44]. Non-IMS services using 5QI=1 may suffer service interruption and/or inconsistent service experience if SRVCC is triggered. Triggering SRVCC for WebRTC IMS session will cause service interruption and/or inconsistent service experience when using 5QI=1. Operator policy (e.g. use of specific AF application identifier) may be used to avoid using 5QI 1 for a voice service, e.g. WebRTC IMS session.
NOTE 15: The "live" uplink streaming algorithm may consider various inputs, including the received flusId attribute, desMaxLatency attribute, desMaxLoss attribute, afAppId attribute and medType attribute for deriving the 5QI. When desMaxLatency attribute and/or desMaxLoss attribute are present, non-authority 5QI mapping may be done according to table 5.7.4-1 in 3GPP TS 23.501 [2].
NOTE 16: The PCF may authorize one or more alternative parameter set(s) if the alternative QoS reference(s) or Requested Alternative QoS parameter Set(s) is received.
NOTE 17: The algorithm to support applications with specific QoS hints (e.g. loss and/or latency demands) may consider various inputs, including the received desMaxLatency attribute, desMaxLoss attribute and afAppId attribute for deriving the 5QI, as shown in table E.0 in 3GPP TS 26.114 [14]. Non-authority 5QI mapping may be done according to table 5.7.4-1 in 3GPP TS 23.501 [2].
NOTE 18: Operator specific policies may consider access information for policy decision. E.g., in a network where the PDU session can be carried over NR satellite access or satellite backhaul, the PCF may take this information into account (together with any delay requirements provided by the AF) to determine the applicable policy decision, as e.g. the 5QI value.

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: For home-routed scenarios, if the "VPLMN-QoS-Control" feature as defined in 3GPP TS 29.512 [9] is supported, if the PCF applies the rules in table 7.3.2-2 to calculate the authorized QoS to be transported within the PDU session, the PCF can adapt the authorized QoS associated to the PDU session to take into account the values that can be accepted by the VPLMN.

NOTE 2: QoS Information related to Maximum Authorized UL/DL Data Rate provided at PDU session level is not derived based on mapping tables in this clause, but based on subscription and operator specific policies.

NOTE 3: 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 mcsId attribute demands MCS specific ARP handling THEN
	ARP:= as defined by MCS specific algorithm (NOTE 4);
	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;
	ELSE IF the qosReference attribute of MediaComponent data type corresponds to a pre-defined QoS information set THEN
	ARP:= as configured by operator
	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. NOTE 4: The MCS specific algorithm shall consider various inputs, including the received mcsId and resPrio attributes, for deriving the ARP.	

7.4 QoS parameter mapping Functions at SMF

7.4.1 QoS parameter mapping Functions in 5GC

Table 7.4.1.1: 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. For PCC rules which are bound to the same QoS flow and have the same sharing key value, the highest MBR value among those PCC rules may be used as input for calculating the common MBR value based on internal logic as defined in clause 4.2.6.2.8 of 3GPP TS 29.512 [9].
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. For PCC rules which are bound to the same QoS flow and have the same sharing key value, the highest GBR value among those PCC rules shall be used as input for calculating the common GBR value as defined in clause 4.2.6.2.8 of 3GPP TS 29.512 [9].
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 or delay critical 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 delay critical GBR QoS flow.
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.	

7.4.2 QoS parameter mapping Functions at SMF+PGW-C for interworking scenario

Table 7.4.2.1: Rules for derivation of the Authorized QoS Parameters per EPS bearer from the Authorized QoS Parameters in SMF+PGW-C

Authorized QoS Parameter per EPS bearer	Derivation from Authorized QoS Parameters (NOTE 2)
Maximum Authorized Bandwidth DL and UL per EPS bearer	Maximum Authorized Bandwidth DL/UL per EPS bearer = Sum of Maximum Authorized Data Rate DL/UL for all PCC rules bound to that EPS bearer as described in clause 4.5.5.3 of 3GPP TS 29.212 [53]. For PCC rules which are bound to the same EPS bearer and have the same sharing key value, the highest MBR value among those PCC rules may be used as input for calculating the common MBR value based on internal logic as defined in clause 4.5.5.11 of 3GPP TS 29.212 [53].
Guaranteed Authorized Data Rate DL and UL per QoS flow	Guaranteed Authorized Data Rate DL/UL per EPS bearer = Sum of Guaranteed Authorized Data Rate DL/UL for all PCC rules bound to that EPS bearer as described in clause 4.5.5.3 of 3GPP TS 29.212 [53]. For PCC rules which are bound to the same EPS bearer and have the same sharing key value, the highest GBR value among those PCC rules shall be used as input for calculating the common GBR value as defined in clause 4.5.5.11 of 3GPP TS 29.212 [53].
APN-AMBR DL and UL	Set according to the operator policy.
QCI (NOTE 1)	For standardized 5QIs, the authorized QCI is one to one mapped from the 5QI; For non-standarized 5QIs, the authorized QCI is derived based on the authorized 5QI and operator policy; For the subscribed default 5QI, one to one map the subscribed default QCI to the subscribed default 5QI.
ARP	One to one mapping to the value derived as described in table 7.4.1.1.
Maximum Packet Loss Rate DL and UL per EPS bearer	One to one mapping to the value derived as described in table 7.4.1.1.
NOTE 1 The delay critical 5QI mapping to QCI is upspecified in the present specification. NOTE 2 Other Authorized QoS parameters that do not have a corresponding mapping in EPS remain unchanged in the SMF+PGW-C for possible future access of the UE to 5GC.	

7.5 QoS Parameters Mapping in MBS deployments

7.5.1 Introduction

QoS parameters mapping functions are located at the PCF and MB-SMF.

7.5.2 QoS parameter mapping Functions at PCF

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 DL. And such process also includes the derivation of the Priority Level (PL), Averaging Window (AW) and Maximum Data Burst Volume (MDBV).

The PCF shall derive Authorized QoS parameters from the service information received:

- from an AF/NEF/MBSF that interacts with the PCF via the Npcf_MBSPolicyAuthorization service; and
- from an MB-SMF that interacts with the PCF via the Npcf_MBSPolicyControl service.

Table 7.5.2-1: Rules for derivation of the Maximum Authorized Data Rates, Authorized Guaranteed Data Rates, Maximum Authorized QoS Class and other authorized QoS parameters per service data flow in the PCF

Authorized QoS Parameter	Derivation from service information (NOTE 3)

Maximum Authorized Data Rate DL (Max_DR_DL)	IF operator special policy exists THEN;
	-Max_DR_DL:= as defined by operator specific algorithm;
	(NOTE 7 and 10)
	ELSE IF afAppId attribute of MbsServiceInfo data type demands application specific data rate handling THEN
	-Max_DR_DL:= as defined by application specific algorithm;
	ELSE IF mbsMediaInfo attribute is received
	IF codecs attribute of MbsMediaInfo data type provides Codec information for a codec that is supported by a specific algorithm (NOTE 4) THEN
	Max_DR_DL:= as defined by specific algorithm;
	ELSE IF maxReqMbsBwDl attribute is present THEN
	Max_DR_DL:= maxReqMbsBwDl value;
	ELSE
	Max_DR_DL:= as set by the operator;
	ENDIF;
	ELSE IF mbsQosReq attribute is received
	IF maxBitRate attribute is present THEN
	Max_DR_DL:= maxBitRate value;
	ELSE
	Max_DR_DL:= as set by the operator;
	ENDIF;
	ELSE IF the qosRef attribute is present THEN
	Max_DR_DL:= as configured by operator;
	ENDIF;

Authorized Guaranteed Data Rate DL (Gua_DR_DL)	IF operator special policy exists THEN;
	-Gua_DR_DL:= as defined by operator specific algorithm;
	(NOTE 7 and 8)
	ELSE IF afAppId attribute of MbsServiceInfo data type demands application specific data rate handling THEN
	-Gua_DR_DL:= as defined by application specific algorithm;
	ELSE IF mbsMediaInfo attribute is received
	IF codecs attribute of MbsMediaInfo data type provides Codec information for a codec that is supported by a specific algorithm (NOTE 4) THEN
	Gua_DR_DL:= as defined by specific algorithm;
	ELSE IF minReqMbsBwDl attribute is present THEN
	Gua_DR_DL:= minReqMbsBwDl value;
	ELSE IF correspnding operator policy exists
	Gua_DR_DL:= as set by the operator;
	ELSE IF service corresponds to a GBR 5QI THEN
	Gua_DR_DL:= Max_DR_DL;
	ELSE
	Gua_DR_DL:= 0; (NOTE 5)
	ENDIF;
	ELSE IF mbsQosReq attribute is received
	IF guarBitRate attribute is present THEN
	Gua_DR_DL:= guarBitRate value;
	ELSE IF correspnding operator policy exists
	Gua_DR_DL:= as set by the operator;
	ELSE IF service corresponds to a GBR 5QI THEN
	Gua_DR_DL:= Max_DR_DL;
	ELSE
	Gua_DR_DL:= 0; (NOTE 5)
	ENDIF;
	ELSE IF the qosRef attribute is present THEN
	Gua_DR_DL:= as configured by operator;
	ENDIF;

Authorized QoS Parameter	Derivation from service information (NOTE 3)

Authorized 5G QoS Identifier (5QI) (see NOTE 1, 2, 6 and 9)	IF an operator special policy exists THEN
	5QI:= as defined by operator specific algorithm; (NOTE 10)
	ELSE IF afAppId attribute of MbsServiceInfo data type demands application specific QoS Class
	handling THEN
	5QI:= as defined by application specific algorithm;
	ELSE IF mbsMediaInfo attribute is received
	IF codecs attribute of MbsMediaInfo data type provides Codec information for a codec that is supported by a specific algorithm (NOTE 4) THEN
	5QI:= as defined by specific algorithm;
	ELSE
	/* The following 5QI derivation is an example of how to obtain the 5QI values in a 5GS network */
	IF the mbsMedType attribute is present THEN
	CASE mbsMedType value OF
	"audio": 5QI := 1;
	"video": 5QI := 2;
	"application": 5QI := 1 OR 2;
	OTHERWISE: 5QI := 9; /*e.g. for TCP-based generic traffic */
	ENDIF;
	ELSE IF mbsQosReq attribute is received
	5QI:= 5qi attribute value;
	ELSE IF the mbsQosRef attribute is received THEN
	5QI:= as configured by operator;
	ENDIF;

NOTE 1: When audio or video IP flow(s) are removed from a session, the 5QI shall keep the originally assigned value.
NOTE 2: 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 3: The encoding of the service information is defined in 3GPP TS 29.537 [55].
NOTE 4: The support of any codec specific algorithm in the PCF is optional.
NOTE 5: Authorized Guaranteed Data Rate DL shall not be derived for non-GBR 5QI values.
NOTE 6: Recommended 5QI values for standardised 5QI characteristics are shown in table 5.7.4-1 in 3GPP TS 23.501 [2].
NOTE 7: 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 8: The PCF shall assign an Authorized Guaranteed Data Rate DL value within the limit supported by the serving network.
NOTE 9: The PCF may authorize a non-standardized 5QI with explicitly signalled QoS characteristics as defined in clause 5.2.3.2.3 of 3GPP TS 29.537 [55] 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]. Averaging Window may also be derived from averWindow attribute when mbsQosReq is received in the PCF.
NOTE 10: Operator specific policies may consider access information for policy decision.

The PCF should per ongoing MBS session store the Authorized QoS parameters for each service data flow (as described within a mbsMedComps attribute).

If the PCF provides a QoS information associated to an MBS PCC rule it may apply the rules in table 7.5.2-2 to combine the Authorized QoS per service data flow (as derived according to table 7.5.2-1) for all service data flows described by the corresponding MBS PCC rule.

NOTE 1: QoS Information related to MBS Session-AMBR is not derived based on mapping tables in this clause, but based on subscription and operator specific policies.

NOTE 2: ARP is always calculated at MBS PCC rule level according to table 7.5.2-2.

Table 7.5.2-2: 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	Maximum Authorized Data Rate DL is the sum of all Maximum Authorized Data Rate DL for all the service data flows (as according to table 7.5.2-1).
Guaranteed Authorized Data Rate DL	Guaranteed Authorized Data Rate DL is the sum of all Guaranteed Authorized Data Rate DL for all the service data flows (as according to table 7.5.2-1). (NOTE 2)
5QI	5QI = MAX [needed QoS parameters per service data flow (as operator's defined criteria) among all the service data flows]

ARP	IF an operator special policy exists THEN
	ARP:= as defined by operator specific algorithm;
	ELSE IF afAppId attribute of MbsServiceInfo data type demands application specific ARP
	handling THEN
	ARP:= as defined by application specific algorithm;
	ELSE IF mbsQosReq attribute is received
	IF reqMbsArp attribute is present THEN
	ARP:= reqMbsArp value;
	ENDIF;
	ELSE IF mbsSdfResPrio is received and it demands application specific ARP handling THEN
	ARP:= as defined by application specific algorithm;
	ELSE IF mbsQosReq attribute is received
	ARP:= as configured by operator
	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 PCF may check that the Guaranteed Authorized Data Rate DL does not exceed the subscribed maximum aggregated bitrate that can be provided across all the GBR QoS Flows for an MBS session.	

7.5.3 QoS parameter mapping Functions at MB-SMF

Table 7.5.3-1: Rules for derivation of the Authorized QoS Parameters per QoS flow from the Authorized QoS Parameters in SMF

Authorized QoS Parameter per QoS flow	Derivation from Authorized QoS Parameters
Maximum Authorized Bandwidth DL per QoS flow	Maximum Authorized Bandwidth DL per QoS flow = Sum of Maximum Authorized Data Rate DL for all MBS PCC rules bound to that QoS flow.
Guaranteed Authorized Data Rate DL per QoS flow	Guaranteed Authorized Data Rate DL per QoS flow = Sum of Guaranteed Authorized Data Rate DL for all MBS PCC rules bound to that QoS flow.
Session-AMBR DL	For all non-GBR QoS flows, Session-AMBR DL is applied.
5QI	5QI from MBS PCC rules having the same value combination of 5QI/ARP/PL/AW/MDBV is used.
ARP	ARP from MBS PCC rules having the same value combination of 5QI/ARP/PL/AW/MDBV is used.
Priority Level (PL)	PL from MBS PCC rules having the same value combination of 5QI/ARP/PL/AW/MDBV is used.
Averaging Window (AW)	AW from MBS PCC rules having the same value combination of 5QI/ARP/PL/AW/MDBV is used. Applicable for GBR or delay critical GBR QoS flow.
Maximum Data Burst Volume (MDBV)	MDBV from MBS PCC rules having the same value combination of 5QI/ARP/PL/AW/MDBV is used. Applicable for delay critical GBR QoS flow.

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 or an SNPN. It is also possible that a PCF may serve only specific DN(s).

For PCC deployments not supporting MBS, PCF discovery and selection procedures are described in this clause clauses 8.2, 8.3, 8.4 and 8.5.

PCF discovery and selection procedures related to MBS PCC deployments as defined in 3GPP TS 23.247 [54] are described in clause 8.6.

These procedures correlate the AF service session establishment over N5 or Rx with the associated PDU session (Session binding) handled over N7. They also correlate the AF service request over N5 with the associated AM policy context or, in the case the AF is a 5G DDNMF, with the associated UE policy context, handled over N15.

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

These procedures enable a consumer NF (e.g. an AF, NEF or PCF for a UE) to address the PCF for a PDU Session or the PCF for the UE (see clause 8.4).

The SCP is involved in the case of delegated discovery and selection.

8.2 PCF discovery and selection by the AMF

PCF discovery and selection functionality is implemented in the AMF and the SCP, and follows the principles described in 3GPP TS 23.501 [2], clause 6.3.1. The AMF uses the PCF services for a UE.

When the AMF performs discovery and selection 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 in the

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) and 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 for PCF discovery and selection for Access and Mobility policies and UE policies:

- 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 the NRF using the UE's SUPI as an input for PCF discovery.
- GPSI; the AMF selects a PCF instance based on the GPSI range the UE's GPSI belongs to or based on the results of a discovery procedure with the NRF using the UE's GPSI as an input for PCF discovery.
- S-NSSAI(s). In the roaming case, the AMF selects the V-PCF instance based on the S-NSSAI(s) of the VPLMN and selects the H-PCF instance based on the S-NSSAI(s) of the HPLMN.
- PCF Set ID.
- PCF Group ID of the UE's SUPI.

NOTE 1: The AMF can infer the PCF Group ID the UE's SUPI belongs to or UE's GPSI belongs to based on the results of PCF discovery procedures with the NRF. The AMF can provide the PCF Group ID to other PCF NF consumers as described in 3GPP TS 23.502 [3].

- The features supported by the PCF (e.g. the PCF supporting the "DNNReplacementControl" feature is selected by the AMF supporting DNN replacement).
- The V2X support stored in the NRF.
- The ProSe support stored in the NRF.
- PCF Selection Assistance Info and PCF Instance Id(s) serving the established PDU Sessions/PDN Connections received from UDM. In case PCF Selection Assistance Info and PCF Instance Id(s) are received from the UDM, the AMF selects a PCF instance that matches one of the received PCF instance Id(s) serving a combination of DNN and S-NSSAI that is included in the the PCF Selection Assistance Info. If multiple DNN and S-NSSAI combinations are provided, the AMF selects the DNN, S-NSSAI using local configuration. In case PCF instance Id(s) are not received, e.g. EPS interworking is not supported, the AMF selects the PCF instance by considering other above factors.

In the case of delegated discovery and selection in the SCP, the AMF shall include in the first request to the PCF the above factors, if available, within the "3gpp-Sbi-Discovery-*" request headers, as specified in 3GPP TS 29.500 [5], clause 6.10.3.2.

In the following scenarios, information about the PCF instance that has been selected by the AMF (e.g. the selected PCF instance Id, the PCF set ID, and if the PCF set ID is not available, the PCF Group ID, if available) can be forwarded to another NF consumer of the PCF:

- During AMF relocation, the target AMF may receive from the source AMF a resource URI of AM Policy association and/or a resource URI of UE Policy association, a PCF instance ID, a PCF set ID, and if the PCF set ID is not available, a PCF Group ID (if available) to enable the target AMF to reuse the same PCF instance (i.e. reuse the AM Policy association resource and/or UE Policy association resource), and the target AMF may decide based on operator policy either to re-use the AM/UE Policy Association in 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 a 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.

In these scenarios, if the target AMF performs discovery and selection, the target AMF may use the received PCF information instead of performing PCF selection interacting with the NRF 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)

In addition, in the case of delegated discovery and selection in the SCP, the following applies:

a) The selected PCF instance may include the PCF instance ID, the PCF set ID, and if the PCF set ID is not available, the PCF Group ID (if available) in the response to the AMF.

NOTE 2: The selected (V-)PCF instance can include a binding indication, including the (V-)PCF ID and possibly the PCF Set ID in the response to the AMF.

b) The AMF first establishes an AM policy association; when forwarding the related request message, the SCP discovers and selects a (V-)PCF instance for AM policy association. Unless binding information is provided in the response of the PCF to that request, the SCP adds the PCF instance ID it selected into the response to the AMF, as per clause 6.10.3.4 of 3GPP TS 29.500 [5]. The AMF uses the received (V-)PCF instance Id for the AM policy association and/or the available binding information within the "3gpp-Sbi-Discovery-*" request headers for the request to establish the UE policy association. The SCP selects the corresponding (V-)PCF instance for UE policy association based on the received discovery and selection parameters.

c) During AMF relocation, the target AMF may receive a resource URI of AM Policy association and/or a resource URI of UE Policy association, a PCF instance ID, a PCF set ID, and if the PCF set ID is not available, a PCF Group ID (if available) from the source AMF to enable it to reuse the same PCF instance. The AMF may decide based on operator policy either to use the old PCF instance or select another PCF instance (i.e. reuse the AM Policy association resource and/or UE Policy association resource). If the target AMF decides to reuse the old PCF instance, the AMF includes the {apiRoot} of the resource URI within the "3gpp-Sbi-Target-apiRoot" request header, the PCF instance ID, the PCF set ID, and if the PCF set ID is not available, the PCF Group ID (if available) within the "3gpp-Sbi-Discovery-*" request header as received from the source AMF in the AM policy update request and/or the UE policy update request to the PCF via the SCP.

d) In the roaming case, the AMF performs discovery and selection of the H-PCF from NRF as described in this clause. The AMF may indicate the maximum number of H-PCF instances to be returned from NRF, i.e. H-PCF selection at NRF. The AMF uses the received V-PCF instance Id for AM Policy association and/or the available binding information received during the AM policy association procedure as described in bullet b) above to send the UE policy association establishment request, which also includes the selected H-PCF instance Id, to the V-PCF via the SCP. The SCP discovers and selects the V-PCF instance. The V-PCF sends an UE policy association establishment request towards the HPLMN, which includes the selected H-PCF instance Id within the "3gpp-Sbi-Discovery-*" request header as a discovery and selection parameter to the H-PCF via the SCP.

8.3 PCF discovery and selection by the SMF

PCF discovery and selection functionality is implemented in the SMF and the SCP, and follows the principles described in 3GPP TS 23.501 [2], clause 6.3.1. The SMF uses the PCF services for a PDU session. The selected PCF instance may be the same or a different one than the PCF instance used by the AMF.

When the SMF performs discovery and selection for a PDU session, 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 in the 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. In the LBO roaming case, the SMF selects the PCF instance based on the S-NSSAI of the VPLMN. In the home routed roaming case, the H-SMF selects the H-PCF instance based on the S-NSSAI of the HPLMN.
- the features supported by the PCF (e.g. a PCF supporting the "ATSSS" feature is selected for an MA 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 an input for PCF discovery.
- GPSI; the SMF selects a PCF instance based on the GPSI range the UE's GPSI belongs to or based on the results of a discovery procedure with NRF using the UE's GPSI as an input for PCF discovery.
- PCF instance ID selected by the AMF for the UE, if available.

- The PCF Group ID provided by the AMF to the SMF, if available.
- PCF Set ID, if available.
- Same PCF Selection Indication provided by the AMF to the SMF, if available.

In the case of delegated discovery and selection in SCP, the SMF shall include the above factors except the local operator policies if available in the first request, within the "3gpp-Sbi-Discovery-*" request headers as specified in 3GPP TS 29.500 [5], subclause 6.10.3.2.

The AMF may, based on operator policies, forward the selected PCF instance ID, the PCF set ID, and if the PCF set ID is not available, the PCF Group ID (if available) to the SMF during the PDU Session Establishment procedure to enable the usage of the same PCF instance for the AMF and the SMF. In this scenario, when the SMF performs discovery and selection, the SMF may decide based on operator policy either to use the same PCF instance or select a new PCF instance.

If the combination of the DNN and S-NSSAI of the PDU session matches one of the combination(s) of the DNN and S-NSSAI included in the PCF Selection Assistance info received from UDM, the AMF shall forward the Same PCF Selection Indication together with the selected PCF instance Id, the PCF set ID, and if the PCF set ID is not available, the PCF Group ID (if available) to the SMF during the PDU Session Establishment procedure. In case that the Same PCF Selection Indication is received together with the PCF instance Id, the PCF set ID, and if the PCF set ID is not available, the PCF Group ID (if available), the SMF shall select the same PCF instance for SM Policy Control.

If the same PCF instance is selected by the SMF, the PCF discovery and selection procedure described above is not performed (discovery may still be needed to obtain the address of the PCF instance).

In the case of delegated discovery and selection in the SCP, the SMF may include the received PCF instance ID, the PCF set ID, and if the PCF set ID is not available, the PCF Group ID (if available) within the "3gpp-Sbi-Discovery-*" request headers in the request to the PCF via the SCP. The SCP may decide based on operator policy either to use the indicated PCF instance or select another PCF instance.

When the feature "SamePcf" is supported, the selected PCF instance may indicate redirection for the SM Policy Control association creation to a different PCF instance, including the redirection URI with the FQDN or IP endpoint of the target Npcf_SMPolicyControl service in a different PCF instance. The SMF shall behave as follows:

- For direct communication scenarios, at the reception of the redirection request, the SMF shall terminate the current SM Policy Control association creation and reselect a PCF instance based on the received redirection information. The SMF shall then establish an SM Policy Control association with the reselected PCF instance.
- For indirect communication scenarios with delegated discovery and selection, the SCP, based on local policies, as specified in 3GPP TS 29.500 [5], clause 6.10.9.1, may send the request towards the new PCF instance instead of forwarding the redirect request to the SMF. If the redirect request is received by the SMF, the SMF shall terminate the current SM Policy Control association creation and reselect a PCF instance based on the received redirection information. The SMF shall then establish an SM Policy Control association with the reselected PCF instance using the same or a different SCP and including the {apiRoot} of the received URI within the "3gpp-Sbi-Target-apiRoot" request header.

NOTE: A single PCF can be used for the monitoring and limitation of the data rate per network slice. To enable this, the SMF has to select the same PCF instance for all PDU Sessions of the UE to the S-NSSAI. This is achieved with the mechanisms described in this clause, for example by using local operator policies in the SMF or SUPI ranges.

8.4 PCF discovery and selection by the AF

8.4.1 General

When multiple and separately addressable PCFs have been deployed, the BSF, as described in clause 8.4.2, is required in order to ensure that a consumer NF (e.g. an AF, NEF, or 5G DDNMF) for a certain PDU session reaches over N5/Rx the PCF holding the PDU session information, and that a consumer NF (e.g. an AF or NEF) for a certain UE context reaches over N5 the PCF holding the UE context information. The AF can also select a PCF based on local configuration for Ethernet PDU sessions.

For the integration with TSC networks the AF is either the TSN AF (integration with IEEE TSN networks) or the TSCTSF (integration with other TSC networks than IEEE TSN).

8.4.2 Binding Support Function (BSF)

The BSF has the following characteristics:

a) The BSF stores internally information about the corresponding selected PCF.

- For a certain PDU session, the BSF stores internally information about the user identity, the DNN, the UE (IP or MAC) address(es), S-NSSAI, the IPv4 address domain (if applicable) and the selected PCF address, and if available the associated PCF instance ID, PCF set ID and the level of SBA binding.

- For a certain UE, the BSF stores internally information about the user identity, the selected PCF address and if available the associated PCF instance ID, PCF set ID and the level of SBA binding.

NOTE 1: Only NF instance or NF set of level of binding is supported at the BSF for SBA binding level of Npcf_PolicyAuthorization service.

NOTE 2: How to ensure the routing of the Npcf_SMPolicyControl_Create service operation to the appropriate PCF instance when the "SamePcf" feature or the "ExtendedSamePcf" feature are supported depends on the implementation.

b) The PCF utilizes the Nbsf_Management service of the BSF to register, update or remove the stored information in the BSF.

   - For a PDU Session, 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 or, each time the PCF instance is changed.

   - For a UE, the PCF ensures that it is updated each time the AMF selects a new PCF instance.

   - Based on operator's policies and configuration and if the "ExtendedSamePcf" feature is supported or the "SamePcf" feature is supported, the PCF determines whether the same PCF shall be selected for the SM Policy associations to a parameter combination (e.g. same SUPI, S-NSSAI and DNN combination) in the non-roaming or home-routed scenario. If yes, the PCF includes the parameter combination in the register request. If no such PCF is found the BSF stores the information in the request; otherwise, the BSF rejects the register request and includes the existing PCF address information hosting the Npcf_SMPolicyControl service in the response (see clause 4.2.2.2 of 3GPP TS 29.521 [22]).

c) For the retrieval of binding information, any NF, such as NEF or AF, uses the Nbsf_Management service as defined in 3GPP TS 29.521 [22] to discover or subscribe to the notification of the selected PCF address(es), and if available, the associated PCF instance ID, PCF set ID and the level of SBA binding for:

   i. the tuple (UE address, DNN, SUPI, GPSI, S-NSSAI, IPv4 address domain) (or for a subset of this tuple), when the target is the PCF for the PDU session; or

   ii. the tuple (SUPI, GPSI) (or for a subset of this tuple), when the target is the PCF for the UE.

d) If the NF received a PCF set ID or a PCF instance ID with a level of SBA binding as result of the Nbsf management service discovery service operation or in the request of the Nbsf management service notification service operation or in the response of the Nbsf management subscribe service operation, it should use that information as NF set level or NF instance level SBA Binding Indication to route requests to the PCF.

e) For an ongoing NF service session, the PCF may provide SBA Binding Indication to the NF (see clause 6.3.1.0 of 3GPP TS 23.501 [2]). This SBA Binding Indication shall then be used instead of any PCF information received from the BSF.

f) 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.

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

NOTE 3: Collocation allows combined implementation.

h) 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 IP domain list, the Range(s) of UE IPv4 addresses, Range(s) of UE IPv6 prefixes, Range(s) of SUPIs, the Range(s) of GPSIs or the BSF Group Id supported by the BSF may be provided to NRF, as described in clause 6.1.6.2.21 of TS 29.510 [51].

i) The BSF verifies whether to provide the address of a PCF for a PDU Session or a PCF for a UE based on the explicit NF service request to the resource collection representing the binding information for the PCF for a PDU Session or the PCF for a UE as specified in 3GPP TS 29.521 [22].

8.4.3 Void

8.4A PCF for a PDU session discovery and selection by the PCF for a UE

When the PCF for a UE determines that the AM policy, e.g. service area restriction, depends on PDU session traffic events, e.g. the application start and application stop for an application Id, the PCF for a UE needs to discover the PCF for a PDU session handling the concerned PDU session(s) to subscribe to the notification of the PDU session traffic related event(s) using the Npcf_PolicyAuthorization service. The following alternatives are specified for the discovery and selection of the PCF for a PDU session by the PCF for a UE:

1) The PCF for a UE may subscribe with the BSF to the notification of the binding information registration/deregistration of the PCF for a PDU session as defined in 3GPP TS 29.521 [22]; or

2) The PCF for a UE may subscribe with the PCF for the PDU session to the notification of PDU session established/terminated events for certain DNN and S-NSSAI combination(s) as follows:

    1. The PCF for a UE provides to the AMF the PCF for a UE callback information (e.g. callback URI information where it listens to notifications of PDU session established/terminated events) and the matching S-NSSAI and DNN combination(s), as specified in 3GPP TS 29.507 [7].

    2. The AMF forwards to the SMF, for the PDU session(s) matching the received S-NSSAI and DNN combination(s), the PCF for a UE callback information, as specified in 3GPP TS 29.502 [52].

    3. The SMF notifies the PCF for a PDU session of the received PCF for a UE callback information, as specified in 3GPP TS 29.512 [9].

    4. When the PCF for a PDU session becomes aware that a SM Policy Association is receiving the callback URI for the PCF for a UE, the PCF for a PDU session sends the Npcf_PolicyAuthorization_Notify service operation to the received PCF for a UE callbck URI to notify the PCF for a UE of the PCF for a PDU session address(es) and SBA binding information as specified in clause 4.2.5.22 of 3GPP TS 29.514 [10].

8.5 BSF procedures

8.5.1 General

These procedures concern the storage of binding information in the BSF, the retrieval of binding information from the BSF and the subscription to the notification of PCF registration/deregistration events from the BSF.

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

8.5.2 Binding information Creation

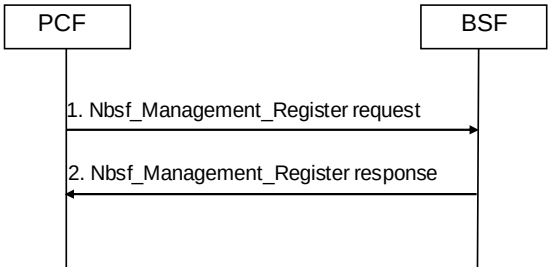


Figure 8.5.2-1: Binding information Creation procedure

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 for a PDU session invokes the Nbsf_Management_Register service operation by sending an HTTP POST request with Resource URI of the resource "PCF for a PDU Session Bindings" to store the binding information in the BSF. The binding information provided in the HTTP POST request is defined in clause 4.2.2.2 of 3GPP TS 29.521 [22].

   When an AM Policy Association or an UE Policy Association is established, and the PCF for a UE determines that binding information needs to be created, the PCF for a UE invokes the Nbsf_Management_Register service operation by sending an HTTP POST request with Resource URI of the resource "PCF for a UE Bindings" as defined in clause 4.2.2.3 of 3GPP TS 29.521 [22] to store the binding information in the BSF.

2. Once the BSF created the resource correspondingly, the BSF shall send an HTTP "201 Created" response to the PCF and store the binding information.

8.5.3 Binding information Deletion

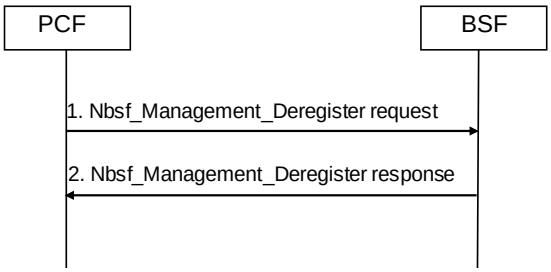


Figure 8.5.3-1: Binding information Deletion procedure

1. When the IP address is released or the MAC address is not used for a certain PDU session and there is no IP address or MAC address applicable to a corresponding binding information (e.g. the IP address or the MAC address is the unique address for the PDU session), the PCF for a PDU Session invokes the Nbsf_Management_Deregister service operation by sending an HTTP DELETE request with Resource URI of the resource "Individual PCF for a PDU Session Binding" to request the BSF to remove the binding information as defined in clause 4.2.3.2 of 3GPP TS 29.521 [22].

   When the AM Policy Association or the UE Policy Association is terminated, and the PCF for a UE determines that binding information needs to be terminated, the PCF for a UE invokes the Nbsf_Management_Deregister service operation by sending an HTTP DELETE request with Resource URI of the resource "Individual PCF for a UE Binding" to request the BSF to remove the binding information as defined in clause 4.2.3.3 of 3GPP TS 29.521 [22].

2. Upon success, the BSF shall send an HTTP "204 No Content" response to the PCF and remove the stored binding information.

8.5.4 Binding information Retrieval

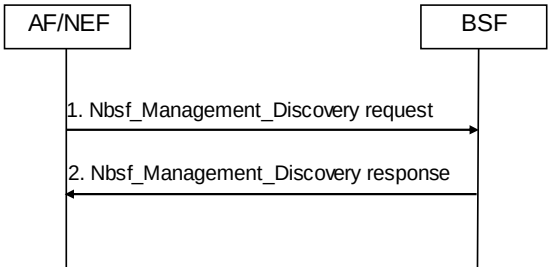


Figure 8.5.4-1: Binding information Retrieval procedure

1. The NF service consumer (e.g., NEF, AF, NWDAF) invokes the Nbsf_Management_Discovery service operation by sending an HTTP GET request with Resource URI of the resource "PCF for a PDU 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 clause 4.2.4.2 of 3GPP TS 29.521 [22].

   The NF service consumer (e.g., NEF, AF, NWDAF) invokes the Nbsf_Management_Discovery service operation by sending an HTTP GET request with Resource URI of the resource "PCF for a UE Bindings" to the BSF to obtain the address information of the selected PCF for a certain UE. The URI query parameters in the HTTP GET request are specified in clause 4.2.4.3 of 3GPP TS 29.521 [22].2. Once the request is accepted and a binding resource matching the query parameters exists, the BSF shall send an HTTP "200 OK" response to the NF service consumer with the address information of the selected PCF (e.g. Npcf_PolicyAuthorization service FQDN and/or IP Endpoint(s) of the selected PCF, or if the PCF supports the Rx interface the Diameter host and realm for the selected PCF), and if available with the associated PCF set ID, the PCF instance ID and the SBA binding level.

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

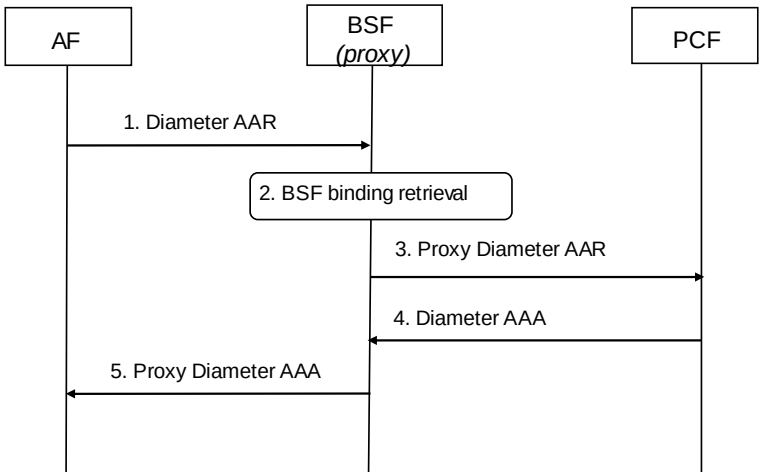


Figure 8.5.5.2-1: Rx Session Establishment procedure using BSF (proxy)

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

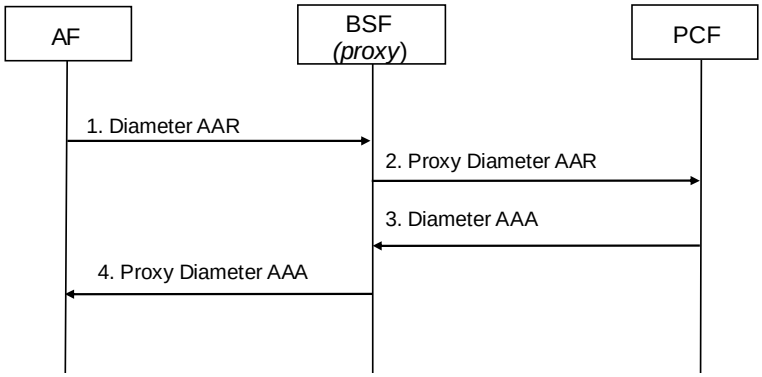


Figure 8.5.5.3.1-1: AF-initiated Rx Session Modification procedure using BSF (proxy)

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

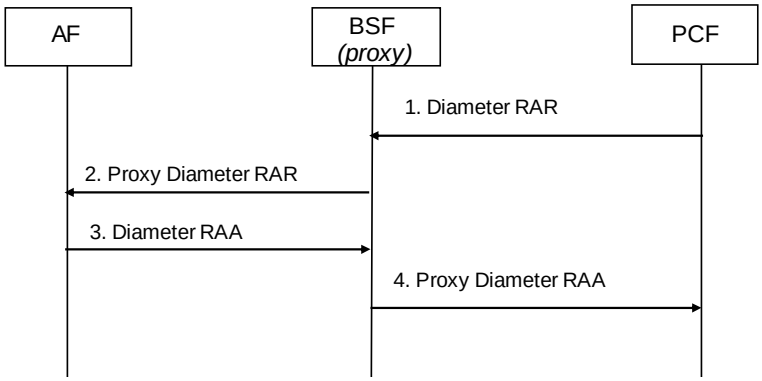


Figure 8.5.5.3.2-1: PCF-initiated Rx Session Modification procedure using BSF (proxy)

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

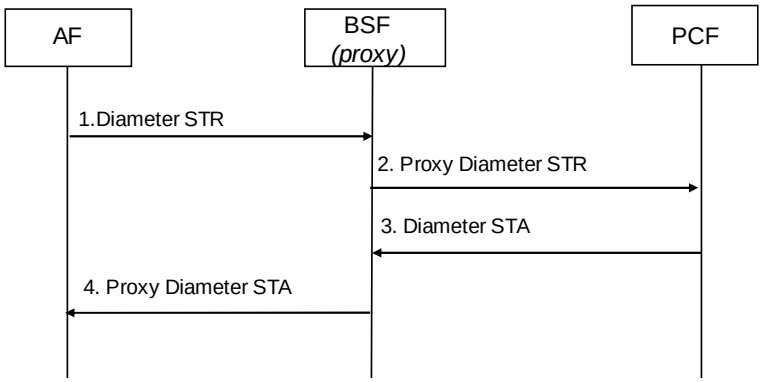


Figure 8.5.5.4.1-1: AF-initiated Rx Session Termination procedure using BSF (proxy)

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

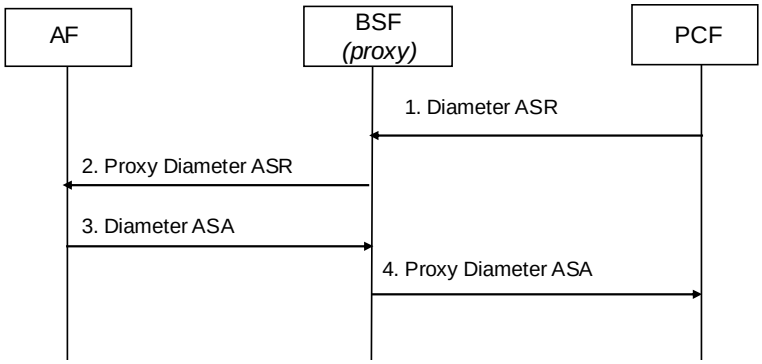


Figure 8.5.5.4.2-1: PCF-initiated Rx Session Termination procedure using BSF (proxy)

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 clause 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 clause 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 clause 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

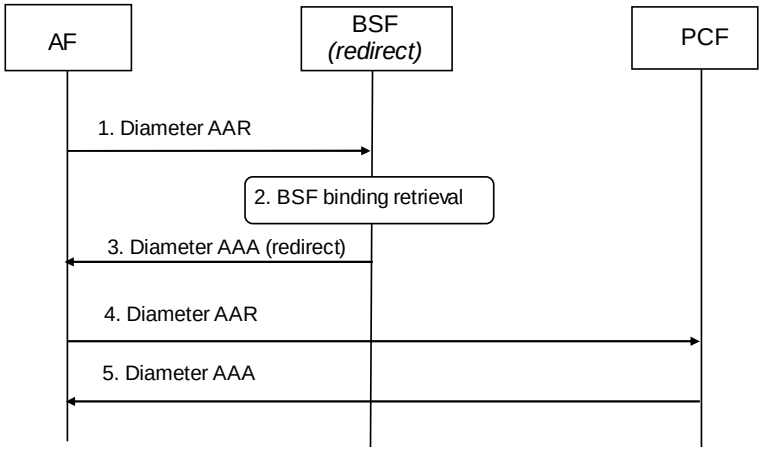


Figure 8.5.6.2-1: Rx Session Establishment procedure using BSF (redirect)

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.

8.5.7 Binding information Update

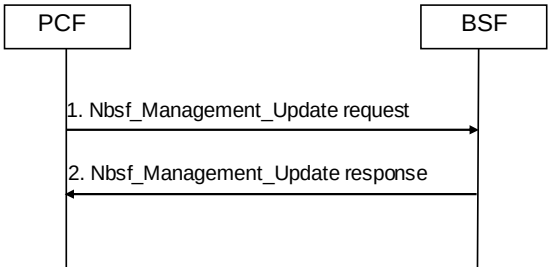


Figure 8.5.7-1: Binding information Update procedure

1. If the binding information has been previously registered in the BSF, and if the BindingUpdate feature defined in 3GPP TS 29.521 [22] is supported, the PCF for a PDU Session invokes the Nbsf_Management_Update service operation by sending an HTTP PATCH request with Resource URI of the resource "Individual PCF for a PDU Session Binding" as defined in clause 4.2.5.2 of 3GPP TS 29.521 [22] to update the binding information in the BSF in the following cases:

   - for the IP address information of the served UE:

     - for the IPv4v6 address case, when one of the addresses is released or a new IP address is allocated; and/or

     - for the multiple address case, if the MultiUeAddr feature defined in 3GPP TS 29.521 [22] is supported, when a new IP address (e.g. IPv6 prefix) is allocated or an IP address which is not the last one is released for the IP PDU session,

   - for the MAC address information of the served UE:

     - if the MultiUeAddr feature defined in 3GPP TS 29.521 [22] is supported, when a new MAC address is used or a MAC address which is not the last one is not used for the Ethernet PDU session ; and/or

   - if a new PCF instance is selected, the PCF instance ID and the associated PCF address(es).

   If the binding information has been previously registered in the BSF, and if a new PCF instance for a UE is selected, the PCF for a UE invokes the Nbsf_Management_Update service operation by sending an HTTP PATCH request with Resource URI of the resource "Individual PCF for a UE Binding" as defined in clause 4.2.5.3 of 3GPP TS 29.521 [22] to update the binding information in the BSF.

2. Upon success, the BSF shall send an HTTP "200 OK" response to the PCF and update the binding information.

8.5.8 Binding information Subscription

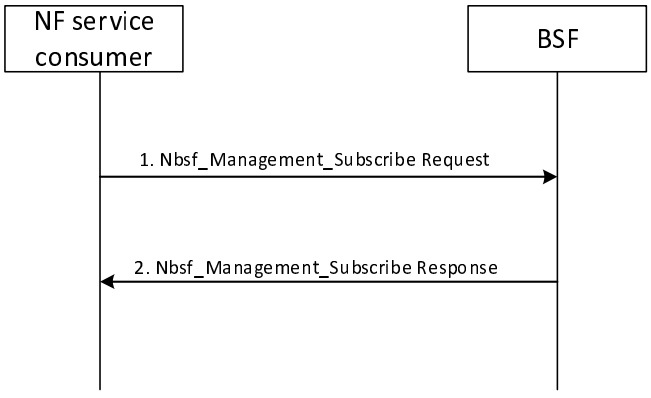


Figure 8.5.8-1: Binding information Subscription procedure

1. The NF service consumer (e.g. PCF for a UE, AF, NEF) invokes the Nbsf_Management_Subscribe service operation by sending an HTTP POST request with the Resource URI of the "Binding Subscriptions" resource as

defined in clause 4.2.6.2 of 3GPP TS 29.521 [22] to subscribe to the notifications of registration/deregistration events for the PCF for a PDU Session or PCF for a UE.

2. Upon success, the BSF shall create and store the subscription, and send an HTTP "201 Created" response to the NF service consumer including the created subscription resource and the available binding information related to the subscription.

8.5.9 Binding information Unsubscription

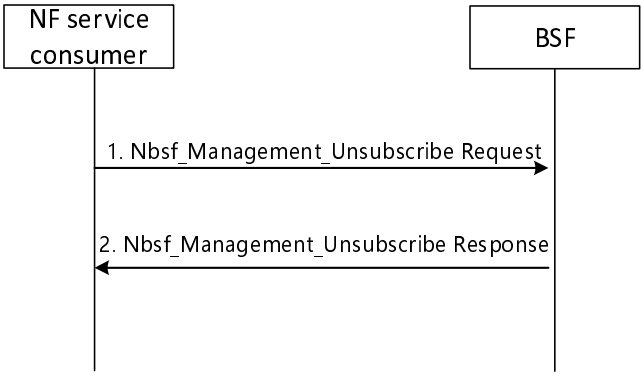


Figure 8.5.9-1: Binding information Unsubscription procedure

1. The NF service consumer (e.g. PCF, AF, NEF) invokes the Nbsf_Management_Unsubscribe service operation by sending an HTTP DELETE request with the Resource URI of the "Individual Binding Subscription" resource to request the BSF to remove the corresponding subscription.

2. Upon success, the BSF shall remove the corresponding subscription and send an HTTP "204 No Content" response to the NF service consumer.

8.5.10 Binding information Notification

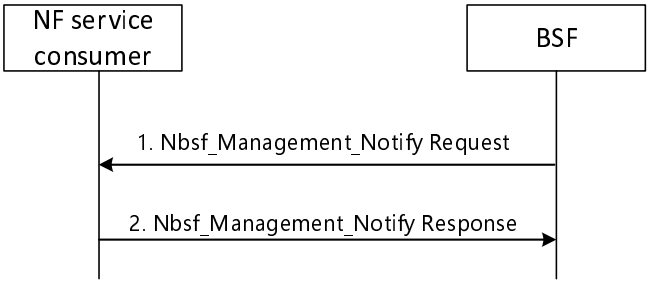


Figure 8.5.10-1: Binding information Notification procedure

1. If the notification has been previously subscribed in the BSF, the BSF invokes the Nbsf_Management_Notify service operation by sending the HTTP POST request with Resource URI as defined in clause 4.2.8.2 of 3GPP TS 29.521 [22] to notify the newly subscribed or unsubscribed events.

2. Once the NF consumer accepts the request, it sends an HTTP "204 No Content" response to the BSF.

8.6 PCF discovery and selection procedures in MBS deployments

8.6.1 PCF discovery and selection by the MB-SMF

PCF discovery and selection functionality is implemented in the MB-SMF and follows the principles described in 3GPP TS 23.501 [2], clause 6.3.1. The MB-SMF uses the PCF services for the handling of the MBS session.

When the MB-SMF performs discovery and selection for an MBS session, the MB-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 in the MB-SMF. The MB-SMF selects a PCF instance based on the available PCF instances (obtained from the NRF or locally configured in the MB-SMF). The following factors may be considered during the PCF selection.

- Local operator policies.
- the features supported by the PCF
- PCF Set ID, if available.

NOTE 1: A single PCF can be deployed in the network. In this case the information is preconfigured in the MB-SMF.

NOTE 2: A single PCF can be used for the handling of location dependent MBS sessions. To enable this, the MB-SMF has to select the same PCF instance for all the MBS session establishments applicable for the same MBS Session Id.

8.6.2 PCF discovery and selection by the AF/NEF/MBSF

8.6.2.1 General

When the AF/NEF/MBSF decides to interact with the PCF the AF/NEF/MBSF performs discovery and selection for an MBS session, the NEF/MBSF 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 in the AF/NEF/MBSF. The NEF/MBSF selects a PCF instance based on the available PCF instances (obtained from the NRF or locally configured in the NEF/MBSF) and depending on operator's policies.

When multiple and separately addressable PCFs have been deployed, the BSF, as described in clause 8.6.2.2, is required in order to ensure that a consumer NF (e.g. an AF, NEF, or MBSF) for a certain MBS session reaches over N5/N30 the PCF holding the MBS session information for MBS location dependent services.

NOTE: This mechanism is not necessary in a deployment with a single PCF.

8.6.2.2 Binding Support Function (BSF)

The BSF has the following characteristics:

a) The BSF stores internally information about the corresponding selected PCF.

- For a certain MBS session, the BSF stores internally information about the MBS Session Id and the selected PCF address, and if available the associated PCF instance ID, PCF set ID and the level of SBA binding.

NOTE 1: Only NF instance or NF set of level of binding is supported at the BSF for SBA binding level of Npcf_MBSPolicyAuthorization service.

b) The PCF determines whether the same PCF shall be selected for the MBS Policy associations related to the same MBS Session Id and uses the BSF for that purpose. The PCF utilizes the Nbsf_Management service of the BSF to register, update or remove the stored information in the BSF. The PCF ensures that the binding information is updated each time the PCF instance is changed.

The BSF checks whether there is already a PCF handling the MBS Policy associations related to the same MBS Session Id. If no such PCF is found the BSF stores the information in the request; otherwise, the BSF rejects the register request and includes the existing PCF address information hosting the Npcf_MBSPolicyControl service in the response (see clause 4.2.2.4 of 3GPP TS 29.521 [22]).

c) For the retrieval of binding information, any NF, such as NEF, MBSF or AF, uses the Nbsf_Management service as defined in 3GPP TS 29.521 [22] to discover the selected PCF address(es), and if available, the associated PCF instance ID, PCF set ID and the level of SBA binding for the MBS Session Id.

d) If the NF received a PCF set ID or a PCF instance ID with a level of SBA binding as result of the Nbsf management service discovery service operation, it should use that information as NF set level or NF instance level SBA Binding Indication to route requests to the PCF.

e) For an ongoing NF service session, the PCF may provide SBA Binding Indication to the NF (see clause 6.3.1.0 of 3GPP TS 23.501 [2]). This SBA Binding Indication shall then be used instead of any PCF information received from the BSF.

8.6.3 BSF procedures

8.6.3.1 General

These procedures concern the storage, update and removal of MBS session binding information in the BSF and the retrieval of binding information from the BSF.

8.6.3.2 Binding information Creation

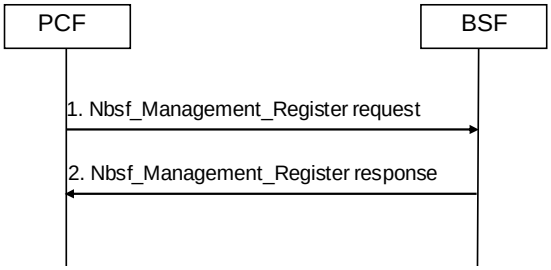


Figure 8.6.3.2-1: Binding information Creation procedure

1. When a new MBS Policy Association is created in the PCF and if the PCF decides that the same PCF needs to handle the MBS Policy Associations related to the same MBS Session Id, it invokes the Nbsf_Management_Register service operation by sending an HTTP POST request with Resource URI of the resource "PCF for an MBS Session Bindings" to check whether there is already stored binding information in the BSF. If it is not, the information is stored. The binding information provided in the HTTP POST request is defined in clause 4.2.2.4 of 3GPP TS 29.521 [22].

2. Once the BSF created the resource correspondingly, the BSF shall send an HTTP "201 Created" response to the PCF and store the binding information.

8.6.3.3 Binding information Update

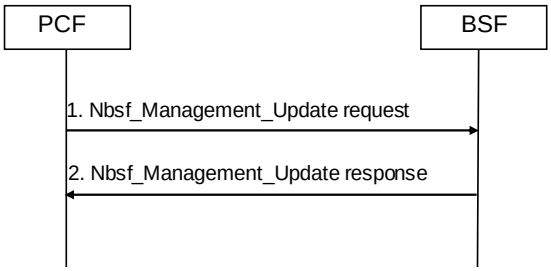


Figure 8.6.3.3-1: Binding information Update procedure

1. If the binding information has been previously registered in the BSF, the PCF invokes the Nbsf_Management_Update service operation by sending an HTTP PATCH request with Resource URI of the resource "Individual PCF for an MBS Session Binding" as defined in clause 4.2.5.4 of 3GPP TS 29.521 [22] to update the binding information in the BSF if a new PCF instance is selected. In this case, the PCF instance ID and the associated PCF address(es) are provided.

2. Upon success, the BSF shall send an HTTP "200 OK" response to the PCF and update the binding information

8.6.3.4 Binding information Deletion

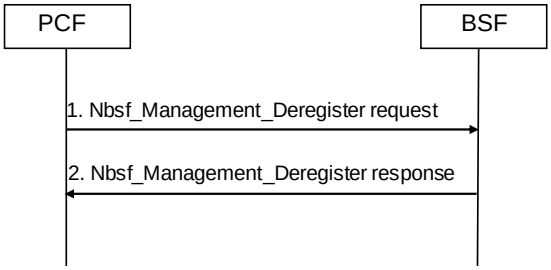


Figure 8.6.3.4-1: Binding information Deletion procedure

1. When the MBS Policy Association in the PCF is deleted and the PCF determines that binding information needs to be terminated, the PCF invokes the Nbsf_Management_Deregister service operation by sending an HTTP DELETE request with Resource URI of the resource "Individual PCF for an MBS Session Binding" to request the BSF to remove the binding information as defined in clause 4.2.3.4 of 3GPP TS 29.521 [22].

2. Upon success, the BSF shall send an HTTP "204 No Content" response to the PCF and remove the stored binding information.

8.6.3.5 Binding information Retrieval

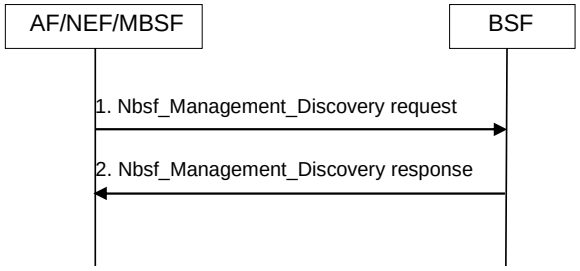


Figure 8.6.3.5-1: Binding information Retrieval procedure

1. The NF service consumer (e.g., NEF, AF, MBSF) invokes the Nbsf_Management_Discovery service operation by sending an HTTP GET request with Resource URI of the resource "PCF for an MBS Session Bindings" to the

BSF to obtain the address information of the selected PCF for a certain MBS session. The URI query parameters in the HTTP GET request are specified in clause 4.2.4.4 of 3GPP TS 29.521 [22].

2. Once the request is accepted and a binding resource matching the query parameters exists, the BSF shall send an HTTP "200 OK" response to the NF service consumer with the address information of the selected PCF, and if available with the associated PCF set ID, the PCF instance ID and the SBA binding level.

9 Race condition handling

9.1 Overview

Certain PCC Services (e.g., Npcf_SMPolicyControl service, Ncpf_AMPolicyControl service) allow the NF producer (e.g. PCF) to update the policy association in two ways: unsolicited and solicited. The PCF can push policy decisions (e.g. PCC rule) to the NF consumer (e.g. SMF) in an unsolicited fashion (e.g. using UpdateNotify service operation for Npcf_SMPolicyControl service). It can also install policy decisions in a solicited manner by responding to the NF consumer (e.g. using the response of the Update service operation for Npcf_SMPolicyControl service).

The NF producer and the NF consumer can initiate transactions that modify the policy independently (e.g. Update service operation from the NF consumer and UpdateNotify service operation from the NF producer) and potentially concurrently. Additionally, there may be HTTP proxy in between the NF consumer and NF producer that could cause messages to be delivered out of order. This can lead to race conditions that may result in the wrong information maintained by the NF consumer or NF producer of a policy association.

Note that race conditions occur in different ways based on the application. Also, their impact is specific to the application.

9.2 Procedures

This clause describes the optional procedures for handling race conditions in a deterministic manner. These procedures apply to the SMF (Npcf_SMPolicyControl service), AMF (Npcf_AMFPolicyControl service and Npcf_UEPolicyControl service), and PCF (Npcf_SMPolicyControl service, Npcf_AMFPolicyControl service and Npcf_UEPolicyControl service).

In this clause, the terms NF consumer and NF producer are relative to the service. As an example, for the Npcf_SMPolicyControl service, the NF consumer is the SMF and the NF producer is the PCF. The term NF can refer to either a NF consumer or a NF producer. The term "transaction" refers to a HTTP request and its associated response. The term "ongoing transaction" refers to a transaction that has an outstanding response.

A node that supports the procedures defined in this clause and is configured to comply with them, shall advertise such support by including the corresponding "PendingTransaction" feature within the attribute of SupportedFeatures data type during the policy association establishment.

On receipt of a HTTP request for an existing policy association, the recipient NF shall check if it has an ongoing transaction on that policy association:

1. If there are no ongoing transactions on the policy association, the NF shall process the incoming request normally.

2. If there is an ongoing transaction on the policy association and optionally, if the recipient NF cannot determine that the incoming request can be safely handled without creating a state mismatch:

   a. The NF consumer shall reject the incoming request and include in an HTTP "400 Bad Request" response message the "cause" attribute of the ProblemDetails data structure set to "PENDING_TRANSACTION".

   b. The NF producer shall either reject the incoming request and include in an HTTP "400 Bad Request" response message the "cause" attribute of the ProblemDetails data structure set to "PENDING_TRANSACTION" or shall wait for one of the following conditions to occur:

i. The ongoing transaction completes. In this case, the policy association is updated at the NF producer on the completion of the ongoing transaction and afterwards, the incoming request (e.g. HTTP POST) is processed normally based on the updated policy association state.

ii. The waiting period has exceeded its allotted time. In this case, the NF producer shall reject the incoming request and include in an HTTP "400 Bad Request" response message the "cause" attribute of the ProblemDetails data structure set to "PENDING_TRANSACTION".

3. On receipt of a "PENDING_TRANSACTION" error code, an NF consumer shall retry the request. On the other hand, if an NF producer had rejected a request from an NF consumer with a "PENDING_TRANSACTION" error code, the NF producer should not retry the failed request until it responds to the re-attempted request from the NF consumer. This is to avoid having both the NF consumer and NF producer concurrently retry their requests. In all other cases, if the policy association on the NF consumer still needs to be updated, the NF producer shall retry the request.

4. The NF consumer or NF producer should limit the number of times they re-attempt the same request due to receipt of a "PENDING_TRANSACTION" error code.

5. The only exception to the rules above is a policy association termination request initiated by the NF consumer (e.g. HTTP POST with request URI to "{apiRoot}/npcf-smpolicycontrol/<apiVersion>/sm-policies/{smPolicyId}/delete") or a request for policy association termination initiated by the NF producer (e.g. HTTP POST with request URI to "/{notificationUri}/terminate"). In both cases, the request should be handled as follows:

   a. When receiving a request for a policy association termination initiated by the NF producer that requires new transactions to be initiated or existing transactions to be finished, a NF consumer shall acknowledge the request immediately (e.g. a HTTP POST message with request URI to "./{NotificationUri}/terminate" shall be acknowledged with a 204 No Content response). The NF consumer shall wait for the current transaction to complete (either by the NF producer acknowledging the request or rejecting it with the "PENDING_TRANSACTION" application error code) before completing the policy association termination procedure (e.g. before sending the HTTP POST with request URI to "{apiRoot}/npcf-smpolicycontrol/<apiVersion>/sm-policies/{smPolicyId}/delete").

NOTE: The client needs to wait for the outcome of the policy association modification to determine if the policy association termination procedure will be used to report information that could not be reported as part of the policy association modification procedure.

   b. When receiving a request for a policy association termination initiated by the NF consumer, the NF producer shall handle it immediately.

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.

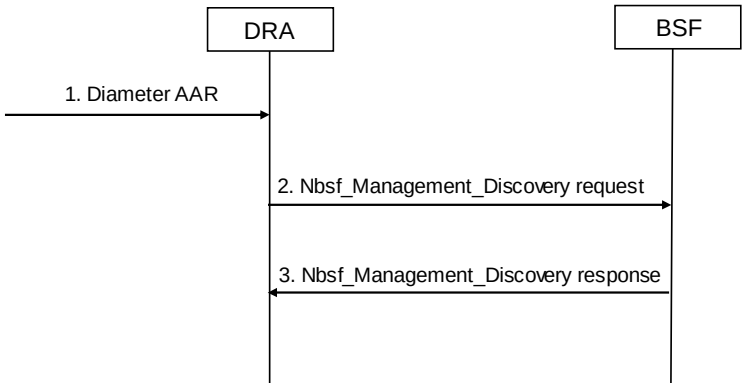


Figure A-1: PCF discovery by DRA via BSF

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 (normative): Signalling Flows for IMS

The signalling flows in clause 5 are also applicable for IMS services provided for a PLMN or an SNPN. This Annex adds flows that show interactions with SIP/SDP signalling of the IMS when the Npcf_PolicyAuthorization service is used by the P-CSCF and both, the PCF and the P-CSCF support the "IMS_SBI" feature, and when the P-CSCF uses the Rx reference point with the PCF.

NOTE 1: In PLMNs or SNPNs where both Rx and Npcf_PolicyAuthorization are used it is implementation specific how the P-CSCF determines the applicable interface/protocol to use with the PCF - e.g. Separate P-CSCF's used for Rx and Npcf_PolicyAuthorization, local routing configuration in the P-CSCF.

NOTE 2: In this Release only IMS voice and emergency services are provided for SNPN.

B.1 General

The following is applicable for Emergency Services and PSAP call back request:

- The P-CSCF includes an Emergency indication when service information is sent over N5/Rx and when required by the IMS deployment. The P-CSCF may also indicate that it requires UE identities as defined in 3GPP TS 29.514 [10] for N5 and 3GPP TS 29.214 [18] for Rx.
- The PCF only allows Emergency Sessions that are bound to a PDU session established to an Emergency DNN.
- Upon request from the P-CSCF, the PCF provides the P-CSCF with UE identities corresponding to the established PDU session.

The following is not applicable for Emergency Services and PSAP call back request:

- Pre-authorization for a UE terminated IMS session establishment with UE initiated resource reservation.
- Subscription to notification of Signalling Path Status at IMS Registration, subscription to notification of changes of access type at IMS Registration and Provisioning of SIP Signalling flow information at IMS Registration procedures.

B.2 IMS Session Establishment

B.2.1 Provisioning of service information at Originating P-CSCF and PCF

This clause covers the PCC procedures for the provisioning of service information, the retrieval of network provided location information (UE location and/or time zone) and the report of EPS fallback indication at the originating P-CSCF and PCF at IMS session establishment.

In figure B.2.1-1 the P-CSCF derives the provisioning of service information to the PCF from the SDP offer/answer exchange.

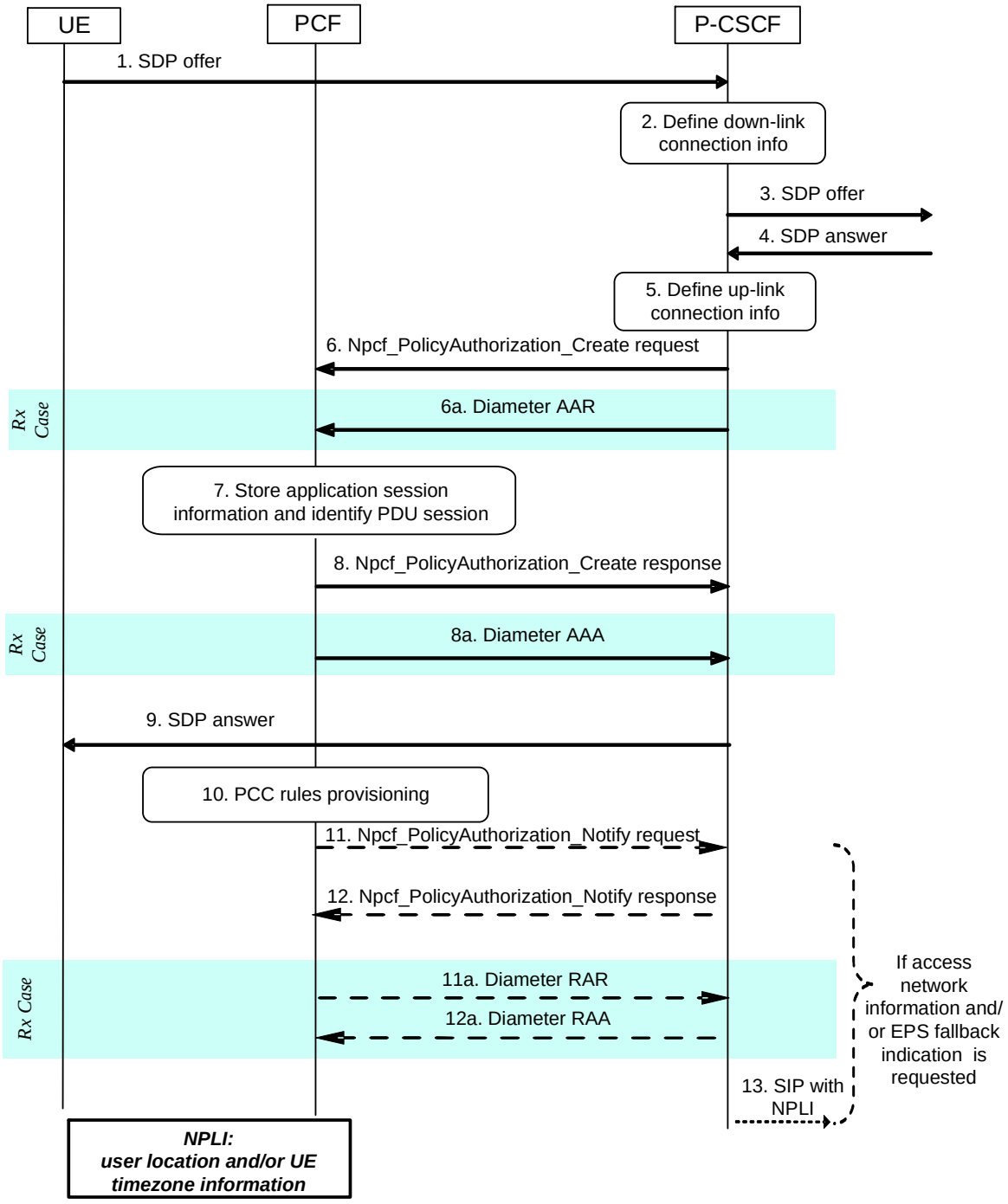


Figure B.2.1-1: PCC Procedures for IMS Session Establishment at originating P-CSCF and PCF

1. The P-CSCF receives the SDP parameters defined by the originator within an SDP offer in SIP signalling.
2. The P-CSCF identifies the connection information needed (IP address of the down link IP flow(s), port numbers to be used, etc.).
3. The P-CSCF forwards the SDP offer in SIP signalling.
4. The P-CSCF gets the negotiated SDP parameters from the terminating side through SIP signalling interaction.
5. The P-CSCF identifies the connection information needed (IP address of the up-link media IP flow(s), port numbers to be used, etc.).

6. The P-CSCF invokes the Npcf_PolicyAuthorization_Create service operation to forward the derived session information to the PCF by sending an HTTP POST request to the "Application Sessions" resource.

   6a. The P-CSCF provides session information to the PCF by sending a Diameter AAR for a new Rx Diameter session.

7. The PCF stores application session information and performs session binding. For N5 interface, the PCF creates an "Individual Application Session Context" resource to store the received application session information.

8. The PCF replies to the P-CSCF with a HTTP "201 Created" response and includes the URI of the "Individual Application Session Context" resource in the Location header field.

   8a. The PCF sends a Diameter AAA to the P-CSCF.

9. Upon reception of the acknowledgement from the PCF, the SDP parameters are passed to the UE in SIP signalling.

10. The PCF executes interactions according to figure 5.2.2.2-1. This step implies provisioning of PCC rules and is executed in parallel with steps 8 and 9 (steps 8a and 9a for Rx case).

11. If the P-CSCF requested access network information and/or EPS fallback indication in step 6, the PCF invokes the Npcf_PolicyAuthorization_Notify service operation to forward the EPS fallback indication, if received in step 10, and/or the access network information received in step 10 in an HTTP POST request sent to the Notification URI received in step 6.

    11a. If the P-CSCF requested access network information and/or EPS fallback indication in step 6a, the PCF forwards the EPS fallback indication, if received in step 10, and the access network information received in step 10 in a Diameter RAR.

12. If step 11 occurs, the P-CSCF acknowledges the receipt of the notification request with an HTTP "204 No Content" response to the PCF.

    12a. If step 11a occurs, the P-CSCF acknowledges the receipt of Diameter RAR.

13. If step 11 occurs (step 11a for Rx case), the P-CSCF forwards the network provided location information in a subsequent SIP message to IMS core network. The P-CSCF, based on local configuration, may also include the EPS fallback indication, if received.

Optionally, the provisioning of service information may be derived already from the SDP offer:

- to enable a possible rejection of the service information by the PCF, obtained by the P-CSCF in time to reject the service with appropriate SIP signalling;
- to allow the P-CSCF to request network provided location information for inclusion in the SDP offer;
- to support authentication of roaming users in deployments with no IMS-level roaming interfaces; or
- to support PSAP callback functionality for anonymous IMS emergency sessions.

This is described in figure B.2.1-2.

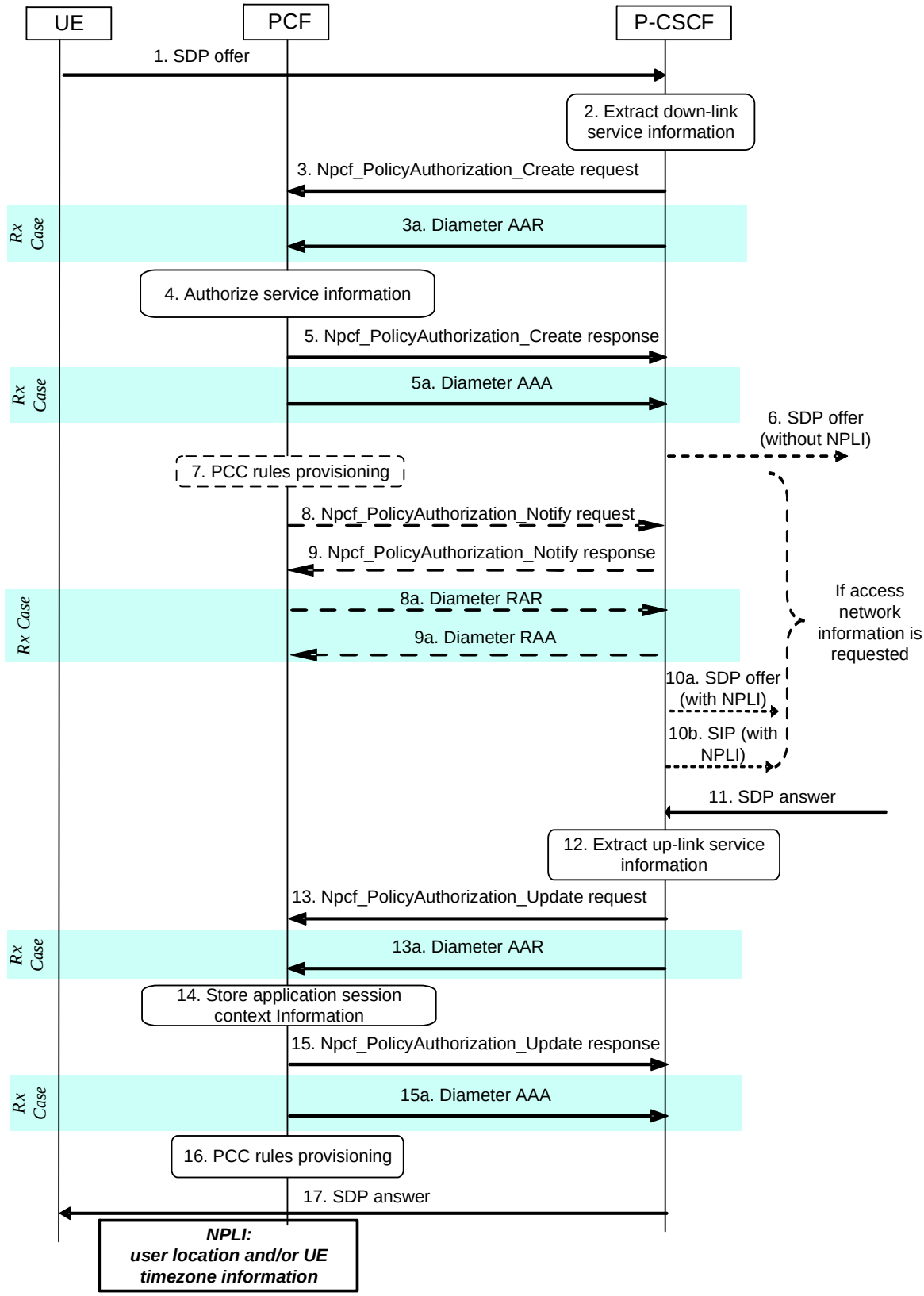


Figure B.2.1-2: PCC Procedures for IMS Session Establishment at originating P-CSCF and PCF, provisioning of service information derived from SDP offer and answer

1. The P-CSCF receives the first SDP offer for a new SIP dialogue within a SIP INVITE request.

2. The P-CSCF extracts service information from the SDP offer (IP address of the down link IP flow(s), port numbers to be used, etc.).

3. The P-CSCF invokes the Npcf_PolicyAuthorization_Create service operation to forward the derived service information to the PCF by sending an HTTP POST request to the "Application Sessions" resource. It indicates that only an authorization check of the service information is requested.

   3a. The P-CSCF forwards the derived service information to the PCF by sending a Diameter AAR for a new Rx Diameter session. It indicates that only an authorization check of the service information is requested.

4. The PCF checks and authorizes the service information, stores session information, performs session binding, but does not provision PCC rules at this stage. In case of N5 interface, the PCF creates an "Individual Application Session Context" resource to store the application session information.

5. The PCF replies to the P-CSCF with an HTTP "201 Created" response and includes the URI of the "Individual Application Session Context" resource in the Location header field.

   5a. The PCF replies to the P-CSCF with a Diameter AAA.

6. If the P-CSCF did not request access network information in step 3 (or step 3a for Rx case), or if the P-CSCF requested access network information but does not require the access network information for inclusion in the SDP offer, or the P-CSCF requested user information in step 3 (or step 3a for Rx case) the P-CSCF forwards the SDP offer in SIP signalling.

7. If the P-CSCF requested access network information in step 3 (or step 3a for Rx case), the PCF executes interactions according to figure 5.2.2.2-1. This step implies provisioning of PCC rules.

8. If the P-CSCF requested access network information in step 3, the PCF invokes the Npcf_PolicyAuthorization_Notify service operation to forward the access network information received in step 7 in an HTTP POST request sent to the Notification URI received in step 3.

   8a. If the P-CSCF requested access network information in step 3a, the PCF forwards the access network information received in step 7 in a Diameter RAR.

9. If step 8 occurs, the P-CSCF acknowledges the receipt of the notification request with an HTTP "204 No Content" response to the PCF.

   9a. If step 8a occurs, the P-CSCF acknowledges the receipt of Diameter RAR.

10a. If step 8 occurs (or step 8a for Rx case), and if the P-CSCF requires to send the access network information and the SDP offer together, the P-CSCF includes the SDP offer and the network provided location information in the next SIP message the P-CSCF sends towards the IMS core network.

10b. If step 8 occurs (or step 8a for Rx case), and if it is allowed for the P-CSCF to handle the access network information independently of the SDP offer, the P-CSCF includes the network provided location information in a subsequent SIP message the P-CSCF sends towards the IMS core network. Typically, network provided information is sent after step 17 rather than at step 10.

11. The P-CSCF receives the negotiated SDP parameters from the terminating side within a SDP answer in SIP signalling.

12. The P-CSCF extracts service information from the SDP answer (IP address of the up-link media IP flow(s), port numbers to be used, etc.).

13. The P-CSCF invokes the Npcf_PolicyAuthorization_Update service operation to modify the "Individual Application Session Context" resource in the PCF by sending an HTTP PATCH request to the URI of the "Individual Application Session Context" resource with the derived service information. Access network information is not requested if done in step 7.

    13a. The P-CSCF forwards the derived service information to the PCF by sending a Diameter AAR over the existing Rx Diameter session. Access network information is not requested if done in step 7.

14. The PCF stores the received information. In case of N5 interface, the PCF updates the "Individual Application Session Context" with the received application session information.

15. The PCF replies to the P-CSCF with an HTTP "204 No Content" response.

15a. The PCF replies the P-CSCF with a Diameter AAA.

16. The PCF authorizes the session information. The PCF executes interactions according to figure 5.2.2.2-1. This step implies provisioning of PCC rules and authorized QoS.

17. Upon successful authorization of the session, the SDP parameters are passed to the UE in SIP signalling. This step is executed in parallel with step 16.

B.2.2 Provisioning of service information at terminating P-CSCF and PCF

This clause covers the PCC procedures for the provisioning of service information, the retrieval of network provided location information (UE location and/or time zone) and the report of EPS fallback indication at the terminating P-CSCF and PCF at IMS session establishment.

In figure B.2.2-1 the P-CSCF derives the provisioning of service information to the PCF from the SDP offer/answer exchange.

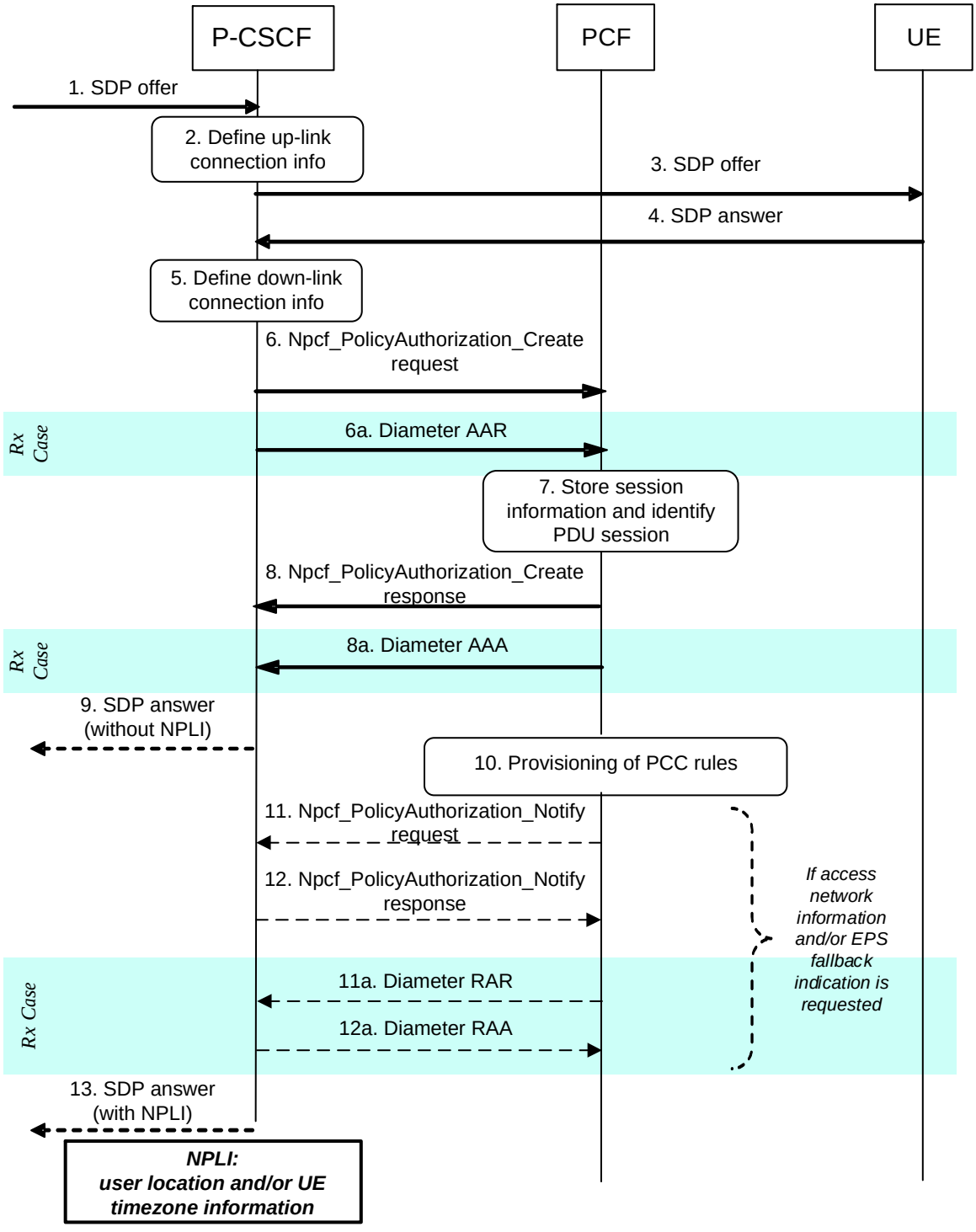


Figure B.2.2-1: PCC Procedures for IMS Session Establishment at terminating P-CSCF and PCF

1. The P-CSCF receives the SDP parameters defined by the originator.
2. The P-CSCF identifies the connection information needed (IP address of the up-link IP flow(s), port numbers to be used, etc.).
3. The P-CSCF sends the SDP offer to the UE.

4. The P-CSCF receives the negotiated SDP parameters from the UE.

5. The P-CSCF identifies the connection information needed (IP address of the down-link IP flow(s), port numbers to be used, etc.).

6. The P-CSCF invokes the Npcf_PolicyAuthorization_Create service operation to forward the derived service information to the PCF by sending an HTTP POST request to the "Application Sessions" resource.

   6a. The P-CSCF forwards the derived service information to the PCF by sending a Diameter AAR for a new Rx Diameter session.

7. The PCF stores the received session information, and performs session binding. For the N5 interface, the PCF creates an "Individual Application Session Context" resource to store the received application session information.

8. The PCF sends an HTTP "201 Created" response to the P-CSCF and includes the URI of the "Individual Application Session Context" resource in the Location header field.

   8a. The PCF sends a Diameter AAA to the P-CSCF.

9. If the P-CSCF did not request access network information in step 6 (or step 6a for the Rx case), upon reception of the acknowledgement from the PCF, the SDP parameters in the SDP answer are passed to the originator.

10. The PCF executes interactions according to clause 5.2.2.2.1 This step implies provisioning of PCC rules and is executed in parallel with steps 8 (or step 8a for the Rx case) and 9.

11. If the P-CSCF requested access network information and/or EPS fallback indication in step 6, the PCF invokes the Npcf_PolicyAuthorization_Notify service operation to forward EPS fallback indication, if received in step 10, and/or the the access network information received in step 10 by sending an HTTP POST request to the Notification URI received in step 6.

    11a. If the P-CSCF requested access network information and/or EPS fallback in step 6a, the PCF forwards the EPS fallback indication, if received in step 10, and/or the access network information received in step 10 in a Diameter RAR.

12. If step 11 occurs, the P-CSCF acknowledges the receipt of the notification request with an HTTP "204 No Content" response.

    12a. If step 11a occurs, the P-CSCF acknowledges the receipt of Diameter RAR.

13. If step 11 occurs (or step 11a for the Rx case), the P-CSCF forwards the SDP answer and includes the network provided location information in the next SIP message the P-CSCF sends towards the IMS core network. The P-CSCF, based on local configuration, may include the EPS fallback indication in outgoing SIP messages towards other IMS nodes, if received.

Optionally, the provisioning of service information may be derived already from the SDP offer:

- to enable that a possible rejection of the service information by the PCF is obtained by the P-CSCF in time to reject the service with appropriate SIP signalling; or

- to enable pre-authorization for a UE terminated IMS session establishment with UE initiated resource reservation.

This is described in figure B.2.2-2.

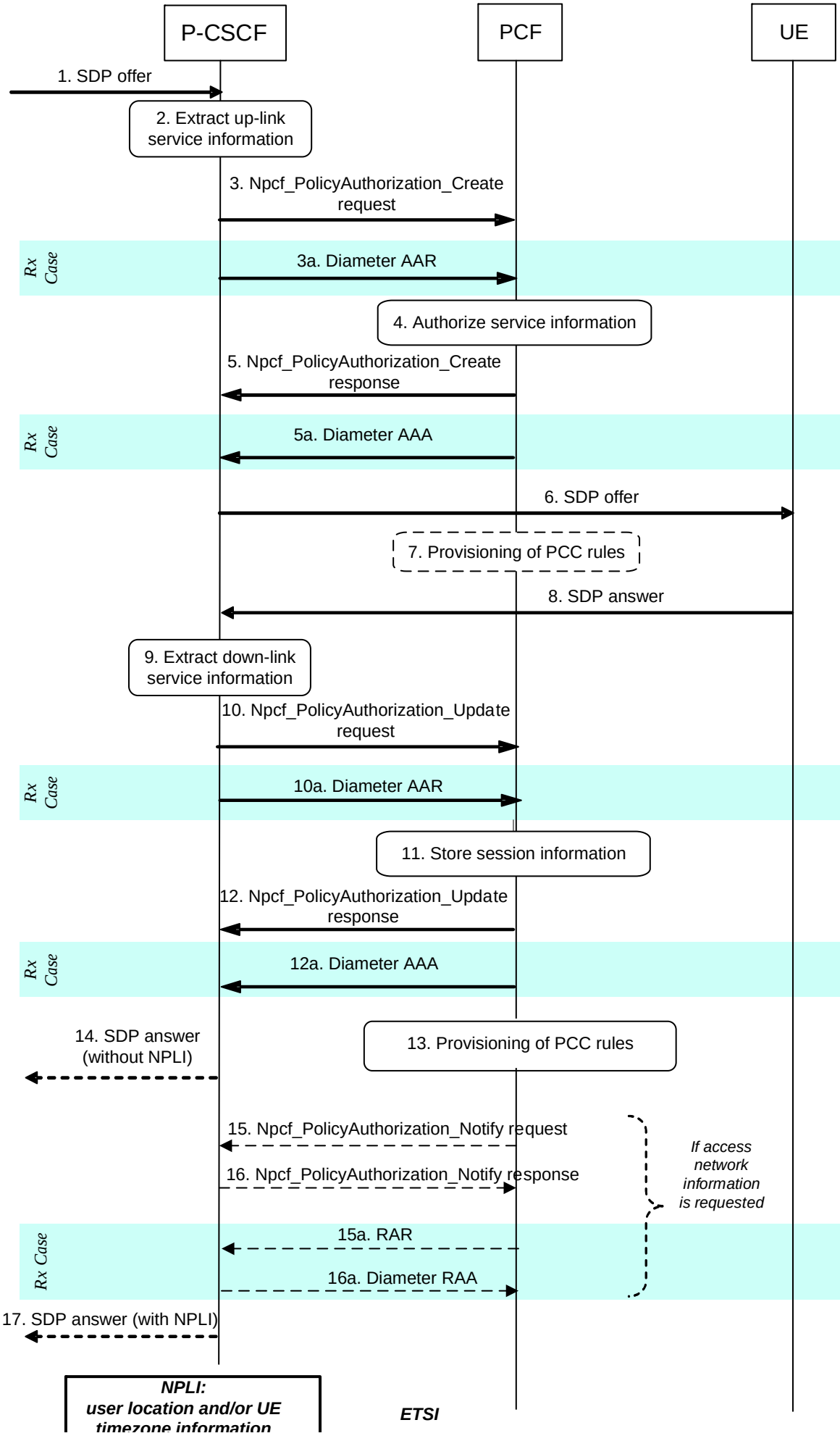

P-CSCF
PCF
UE
1. SDP offer
2. Extract up-link service information
3. Npcf_PolicyAuthorization_Create request
Rx Case
3a. Diameter AAR
4. Authorize service information
5. Npcf_PolicyAuthorization_Create response
Rx Case
5a. Diameter AAA
6. SDP offer
7. Provisioning of PCC rules
8. SDP answer
9. Extract down-link service information
10. Npcf_PolicyAuthorization_Update request
Rx Case
10a. Diameter AAR
11. Store session information
12. Npcf_PolicyAuthorization_Update response
Rx Case
12a. Diameter AAA
14. SDP answer (without NPLI)
13. Provisioning of PCC rules
15. Npcf_PolicyAuthorization_Notify request
16. Npcf_PolicyAuthorization_Notify response
If access network information is requested
Rx Case
15a. RAR
16a. Diameter RAA
17. SDP answer (with NPLI)
NPLI:
user location and/or UE timezone information

Figure B.2.2-2: PCC Procedures for IMS Session Establishment at terminating P-CSCF and PCF, provisioning of service information derived from SDP offer and answer

1. The P-CSCF receives the first SDP offer for a new SIP dialogue within SIP signalling, e.g. within a SIP INVITE request.

2. The P-CSCF extracts the service information from the SDP offer (IP address of the up-link IP flow(s), port numbers to be used, etc.).

3. The P-CSCF invokes the Npcf_PolicyAuthorization_Create service operation to forward the derived session information to the PCF by sending an HTTP POST request to the "Application Sessions" resource.

   3a. The P-CSCF forwards the derived service information to the PCF by sending a Diameter AAR for a new Rx Diameter session.

   The P-CSCF indicates to the PCF that the service information that the AF has provided to the PCF is preliminary and needs to be further negotiated between the two ends. The P-CSCF may request access network information and/or EPS fallback indication.

4. The PCF checks and authorizes the session information, performs session binding, but does not provision PCC rules at this stage. In case of N5 interface, the PCF creates an "Individual Application Session Context" resource,

5. The PCF replies to the P-CSCF with an HTTP "201 Created" response and includes the URI of the "Individual Application Session Context" resource in the Location header field.

   5a. The PCF replies to the P-CSCF with a Diameter AAA.

6. The P-CSCF sends the SDP offer to the UE.

7. If the UE initiates a QoS flow modification request, the PCF provides the SMF with PCC rules according to figure 5.2.2.2-1 based on the SDP offer.

NOTE: Step 7 is not applicable for IMS Emergency Sessions.

8. The P-CSCF receives the negotiated SDP parameters from the UE within an SDP answer in SIP signalling.

9. The P-CSCF extracts service information from the SDP answer (IP address of the down-link IP flow(s), port numbers to be used, etc.).

10. The P-CSCF invokes the Npcf_PolicyAuthorization_Update service operation to modify the "Individual Application Session Context" resource by sending to the PCF an HTTP PATCH request to the URI of the "Individual Application Session Context" resource with the derived service information. The P-CSCF may request access network information and/or EPS fallback information if not requested in step 3.

    10a. The P-CSCF forwards the derived service information to the PCF by sending a Diameter AAR over the existing Rx Diameter session. The P-CSCF may request access network information and/or EPS fallback information if not requested in step 3a.

11. The PCF stores the received session information. In case of N5 interface, the updates the "Individual Application Session Context" resource with the received session information.

12. The PCF sends an HTTP "204 No Content" response to the P-CSCF.

    12a. The PCF replies to the P-CSCF with a Diameter AAA.

13. The PCF authorizes the session information. The PCF executes interactions according to figure 5.2.2.2-1. This step implies provisioning of PCC rules and authorized QoS.

14. If the P-CSCF did not request access network information in step 3 or 10 (step 3a or 10a for Rx case), upon successful authorization of the session the SDP parameters in the SDP answer are passed to the originator. This step is executed in parallel with step 12 (step 12a for Rx case).

15. If the P-CSCF requested access network information and/or EPS fallback indication in step 3 or 10, the PCF invokes the Npcf_PolicyAuthorization_Notify service operation to forward the EPS fallback indication, if

received in step 13, and the access network information received in step 13 in an HTTP POST request to the Notification URI received in in step 3 or 10.

15a. If the P-CSCF requested access network information and/or EPS fallback indication in step 3a or 10a, the PCF forwards the EPS fallback indication, if received in step 13, and the access network information received in step 13 in a Diameter RAR.

16. If step 15 occurs, the P-CSCF acknowledges the receipt of the notification request with an an HTTP "204 No Content" response to the PCF.

16a. If step 15a occurs, the P-CSCF acknowledges the recepeit of Diameter RAR.

17. If step 15 occurs (step 15a for Rx case), the P-CSCF forwards the SDP answer and includes the network provided location information in the next SIP message the P-CSCF sends towards the IMS core network. The P-CSCF, based on local configuration, may include the EPS fallback indication in outgoing SIP messages towards other IMS nodes, if received.

B.3 IMS Session Modification

B.3.1 Provisioning of service information

This clause covers the provisioning of service information, the retrieval of network provided location information (UE location and/or time zone) and the report of EPS fallback indication at IMS session modification both at the originating and terminating side.

In figure B.3.1-1 the P-CSCF derives the provisioning of service information to the PCF from the SDP offer/answer exchange.

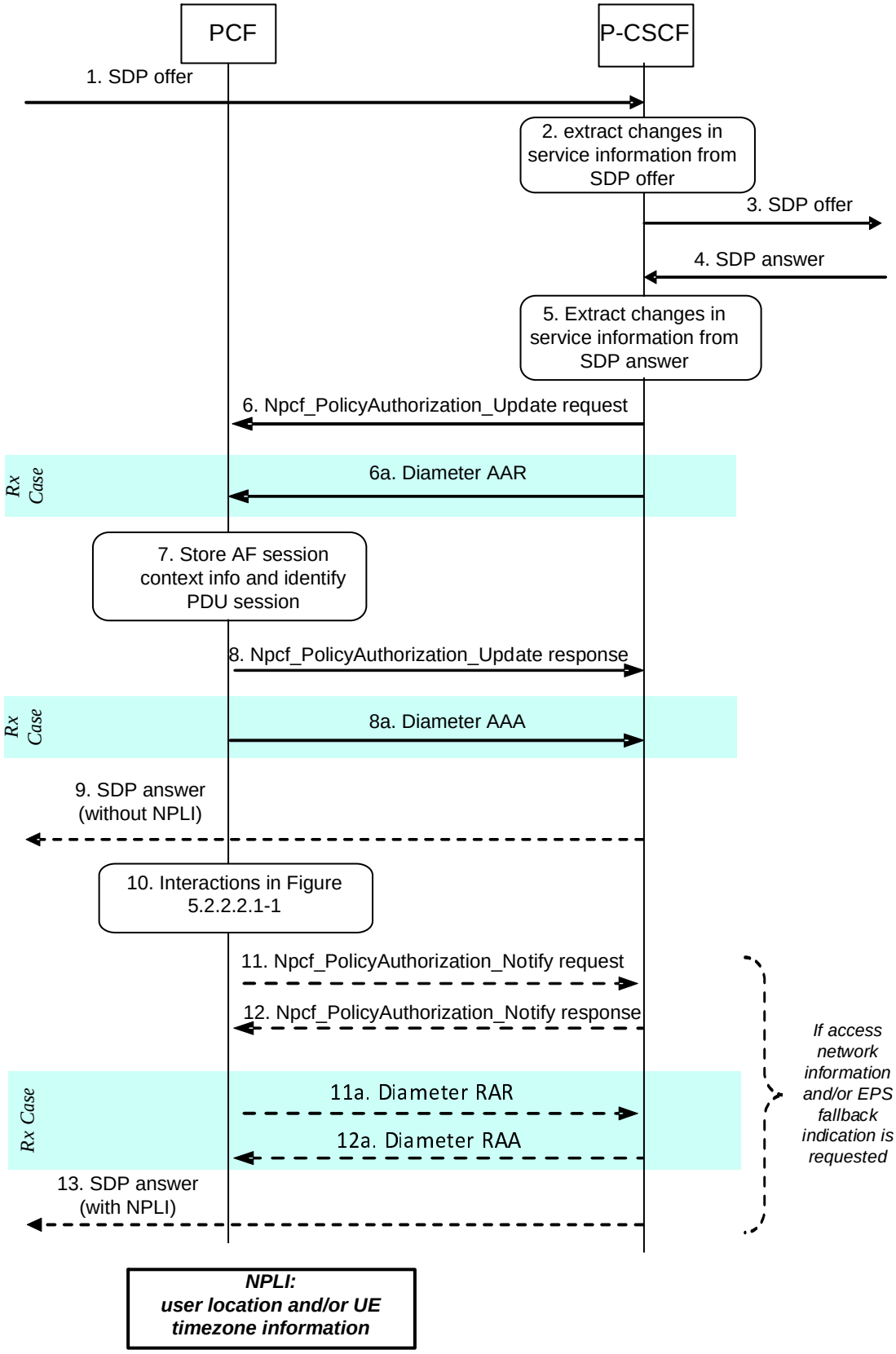


Figure B.3.1-1: Provisioning of service information at IMS session modification

1. The P-CSCF receives the SDP parameters defined by the originator within an SDP offer in SIP signalling.
2. The P-CSCF identifies the relevant changes in the SDP.

3. The P-CSCF forwards the SDP offer in SIP signalling.
4. The P-CSCF gets the negotiated SDP parameters from the terminating side through SIP signalling interaction.
5. The P-CSCF identifies the relevant changes in the SDP.
6. The P-CSCF invokes the Npcf_PolicyAuthorization_Update service operation by sending an HTTP PATCH request to the "Individual Application Session Context" resource, and includes the derived updated information.

   6a. The P-CSCF sends a Diameter AAR for an existing Diameter session and includes the derived updated service information.

7. The PCF stores the received updated session information and identifies the affected established PDU Session. For N5 interface, the PCF updates the "Individual Application Session Context" resource.
8. The PCF replies to the P-CSCF with a HTTP "200 OK" response.

   8a. The PCF answers with a Diameter AAA.

9. If the P-CSCF did not request access network information in step 6 (step 6a for Rx case), the P-CSCF forwards the SDP answer in SIP signalling.
10. The PCF executes interactions according to figure 5.2.2.2.1-1. Due to the updated service information, this step may imply provisioning of PCC rules or the need to enable or disable IP Flows (see clauses B.3.2 and B.3.3, respectively).
11. If the P-CSCF requested access network information and/or EPS fallback indication in step 6, the PCF invokes the Npcf_PolicyAuthorization_Notify service operation to forward the EPS fallback indication, if received in step 10, and/or the access network information received in step 10 in an HTTP POST request sent to the Notification URI received in step 6

    11a. If the P-CSCF requested access network information and/or EPS fallback indication in step 6a, the PCF forwards the EPS fallback indication, if received in step 10, and/or the access network information received in step 10 in a Diameter RAR.

12. If step 11 occurs, the P-CSCF acknowledges the receipt of the notification request with an HTTP "204 No Content" response to the PCF.

    12a. If step 11 occurs, the P-CSCF acknowledges the receipt of Diameter RAR.

13. If step 11 occurs (step 11a for Rx case), the P-CSCF includes the SDP answer and the network provided location information in the next SIP message the P-CSCF sends towards the IMS core network.

Optionally, the provisioning of service information may be derived already from the SDP offer to:

- enable that a possible rejection of the service information by the PCF is obtained by the P-CSCF in time to reject the service with appropriate SIP signalling; or
- enable pre-authorization for a UE terminated IMS session establishment with UE initiated resource reservation.

This is described in figure B.3.1-2.

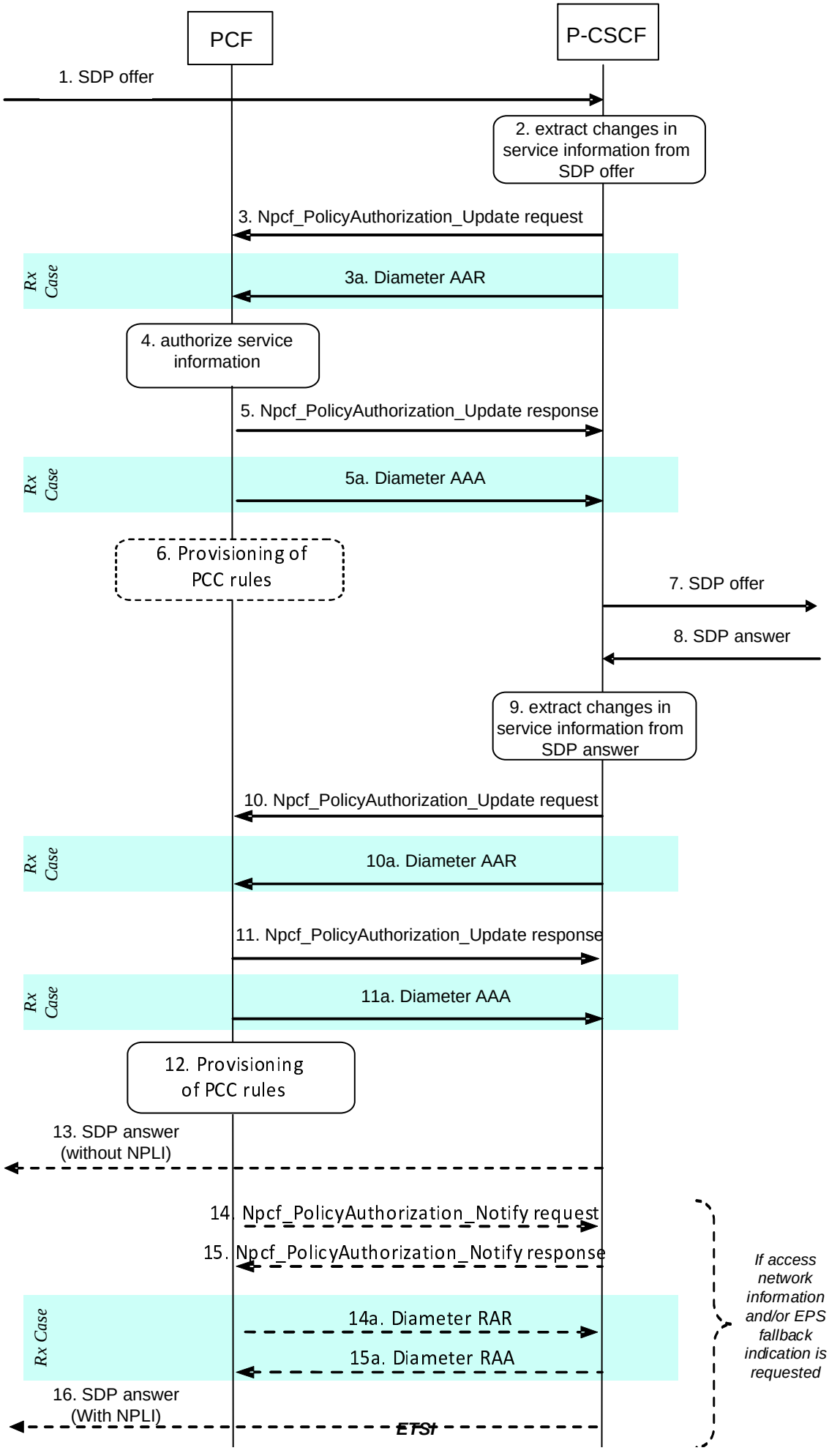

PCF
P-CSCF
1. SDP offer
2. extract changes in service information from SDP offer
3. Npcf_PolicyAuthorization_Update request
Rx Case
3a. Diameter AAR
4. authorize service information
5. Npcf_PolicyAuthorization_Update response
Rx Case
5a. Diameter AAA
6. Provisioning of PCC rules
7. SDP offer
8. SDP answer
9. extract changes in service information from SDP answer
10. Npcf_PolicyAuthorization_Update request
Rx Case
10a. Diameter AAR
11. Npcf_PolicyAuthorization_Update response
Rx Case
11a. Diameter AAA
12. Provisioning of PCC rules
13. SDP answer (without NPLI)
14. Npcf_PolicyAuthorization_Notify request
15. Npcf_PolicyAuthorization_Notify response
Rx Case
14a. Diameter RAR
15a. Diameter RAA
16. SDP answer (With NPLI)
If access network information and/or EPS fallback indication is requested
ETSI

Figure B.3.1-2: Provisioning of service information derived from SDP offer and answer at IMS session modification

1. The P-CSCF receives an SDP offer in SIP signalling for an exiting SIP dialogue.
2. The P-CSCF identifies the relevant changes in the SDP and extracts the corresponding service information.
3. The P-CSCF invokes the Npcf_PolicyAuthorization_Update service operation by sending an HTTP PATCH request to the "Individual Application Session Context" resource created for the corresponding SIP session, and updates the PCF with the derived updated information.

   3a. The P-CSCF forwards the derived service information to the PCF by sending a Diameter AAR over the existing Rx Diameter session for the corresponding SIP session.

   The P-CSCF request indicates that the service information that the AF has provided to the PCF is preliminary and needs to be further negotiated between the two ends.
4. The PCF checks and authorizes the session information, but does not provision PCC rules at this stage.
5. The PCF replies to the P-CSCF with a HTTP "200 OK" response

   5a. The PCF answers with a Diameter AAA.
6. If the UE initiates a QoS flow resource modification request, the PCF provides the SMF with PCC rules according to figure 5.2.2.3-1 based on the SDP offer.

NOTE: Step 6 is not applicable for IMS Emergency Sessions.

7. The P-CSCF forwards the SDP offer in SIP signalling.
8. The P-CSCF receives the negotiated SDP parameters within an SDP answer in SIP signalling from the terminating side.
9. The P-CSCF identifies the relevant changes in the SDP and extracts the corresponding service information.
10. The P-CSCF invokes the Npcf_PolicyAuthorization_Update service operation by sending an HTTP PATCH request to the "Individual Application Session Context" resource, and includes the derived updated information.

    10a. The P-CSCF sends a Diameter AAR for an existing Diameter session and includes the derived updated service information.
11. The PCF replies to the P-CSCF with a HTTP "200 OK" response

    11a. The PCF answers with a Diameter AAA.
12. The PCF interacts with the SMF according to figure 5.2.2.2.2.2-1. This step may imply provisioning of PCC rules and authorized QoS. The PCF may need to enable or disable IP Flows (see clauses B.3.2 and B.3.3, respectively) due to the updated service information.
13. If the P-CSCF did not request access network information in step 3 (step 3a for the Rx case) or step 10 (step 10a for the Rx case), the P-CSCF forwards the SDP answer in SIP signalling. This step is executed in parallel with step 12.
14. If the P-CSCF requested access network information and/or EPS fallback indication in step 3 or 10, the PCF invokes the Npcf_PolicyAuthorization_Notify service operation to forward the EPS fallback indication, if received in step 12, and/or the access network information received in step 12.

    14a. If the P-CSCF requested access network information in step 3a or 10a, the PCF forwards the EPS fallback indication, if received in step 10, and/or the access network information received in step 12 in a Diameter RAR.
15. If step 14 occurs, the P-CSCF acknowledges the notification with a HTTP "204 No Content" response.

    15a. If step 14a occurs, the P-CSCF acknowledges the receipt of Diameter RAR.
16. If step 14 occurs (or step 14a for the Rx case), the P-CSCF includes the SDP answer and the network provided location information in the next SIP message the P-CSCF sends towards the IMS core network.

B.3.2 Enabling of IP Flows

The PCF makes a final decision to enable the allocated QoS resource for the authorized IP flows of the media component(s) if the QoS resources are not enabled at the time they are authorized by the PCF (e.g. because of gate control of early media) or if the media IP flow(s) previously placed on hold are resumed, i.e. the media IP flow(s) of the media component that was placed on hold at the time of the resource authorization or at a later stage is reactivated (with SDP direction sendrecv, sendonly, recvonly or none direction).

The Enabling of IP Flows procedure is triggered during the early dialog by the P-CSCF receiving the SIP message (e.g. 18x response on initial INVITE request) with the P-Early-Media header field indicating request for authorization of early media as described in clause B.2.2 of 3GPP TS 29.514 [10].

NOTE: Enabling of IP Flows is also possible as part of preliminary responses in order to support SIP Forking scenarios. See clause B.3.1 of 3GPP TS 29.514 [10].

The Enabling of IP Flows procedure is triggered during the confirmed dialog by the P-CSCF receiving SIP 2xx response to an INVITE request or a 2xx response to an in-dialog UPDATE request in an established dialog (in both cases a 200 OK response is usually received). When receiving such responses, the P-CSCF shall take the SDP direction attribute in the latest received SDP (either within the 2xx response or a previous SIP message) into account when deciding, which gates shall be opened:

- For a unidirectional SDP media component, IP flows in the opposite direction shall not be enabled.
- For an inactive SDP media component, no IP flows shall be enabled.

Figure B.3.2-1 is applicable to the originating and terminating sides for a confirmed dialog.

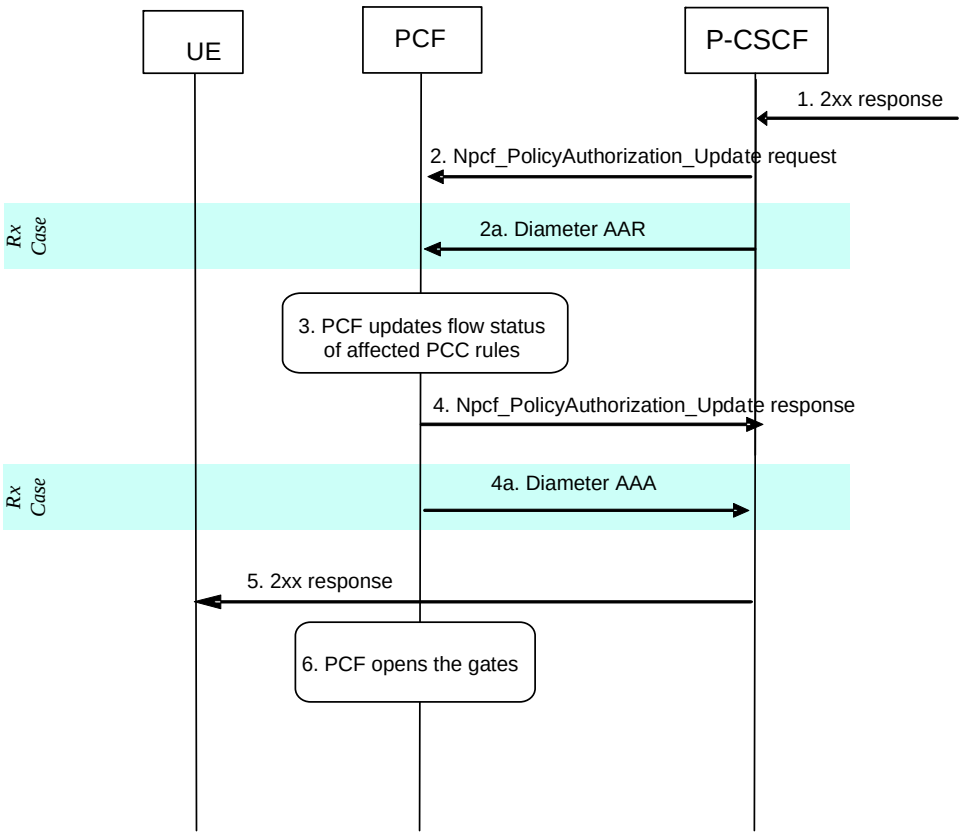


Figure B.3.2-1: Enabling of IP Flows

1. The P-CSCF receives the SIP 2xx response complying with the conditions specified in the paragraphs above.

2. The P-CSCF invokes the Npcf_PolicyAuthorization_Update service operation by sending an HTTP PATCH request to the "Individual Application Session Context" resource to the PCF requesting that gates shall be opened.

   2a. The P-CSCF sends a Diameter AAR message to the PCF, requesting that gates shall be opened.

3. The PCF approves the enabling of IP flows and PCF updates flow status of affected PCC rules.

4 The PCF replies to the P-CSCF with a HTTP "200 OK" response.

   4a. The PCF sends a Diameter AAA to the P-CSCF.

5 The P-CSCF forwards the SIP 2xx response to the UE.

6. The PCF executes interactions according to figure 5.2.2.2.2.2-1. This step implies opening the "gates" by updating the flow status of PCC rules.

B.3.3 Disabling of IP Flows

The Disabling of IP Flows procedure is used when media IP flow(s) of a session are put on hold (e.g. in case of a media re-negotiation or call hold).

NOTE 1: Disabling of IP Flows is also possible as part of preliminary responses in order to support SIP Forking scenarios. See clause B.3.1 of 3GPP TS 29.514 [10].

Media is placed on hold as specified in IETF RFC 3264 [43]. Media modified to become inactive (SDP direction attribute) shall also be considered to be put on hold.

If a bidirectional media component is placed on hold by making it unidirectional, the IP flows shall only be disabled in the deactivated direction. If a media component is placed on hold by making it inactive, the IP flows shall be disabled in both directions.

Figure B.3.3-1 presents the Disabling of IP Flows procedure at media on hold for both the originating and terminating sides.

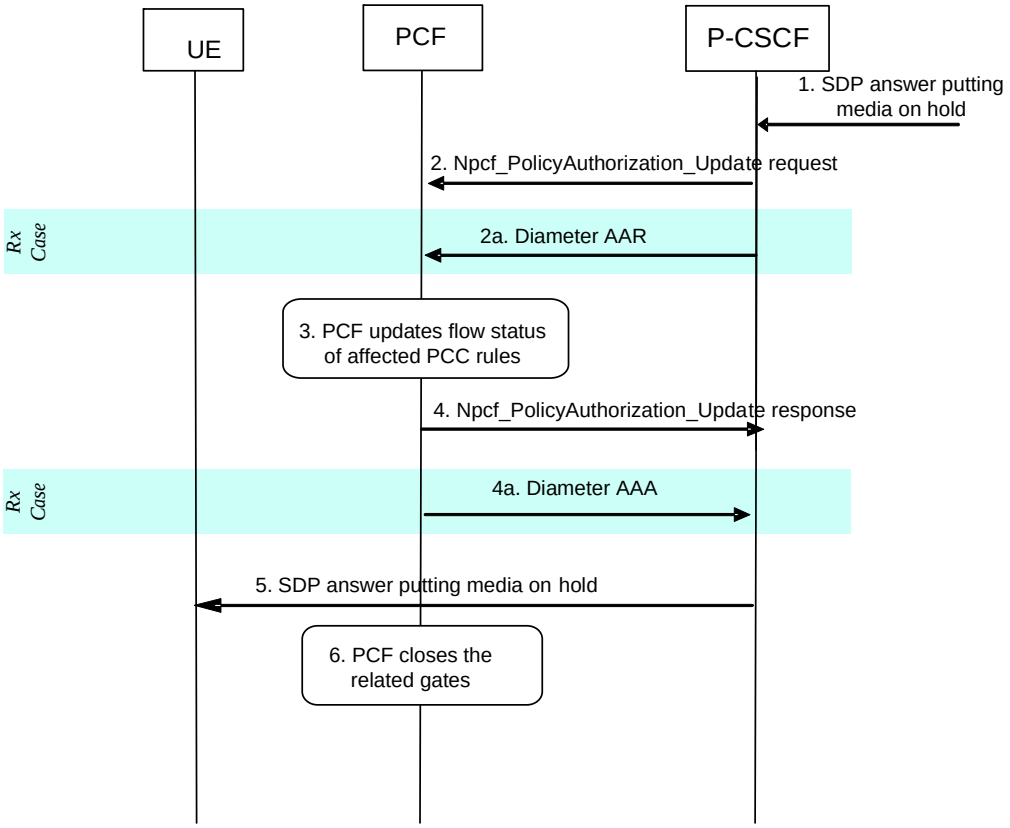


Figure B.3.3-1: Disabling of IP Flows at Media on Hold

1. The P-CSCF receives an SDP answer putting media on hold within a SIP message. (NOTE 2)
2. The P-CSCF invokes the Npcf_PolicyAuthorization_Update service operation by sending an HTTP PATCH request to the "Individual Application Session Context" resource to the PCF requesting that gates shall be closed.

   2a. The P-CSCF sends a Diameter AAR request to the PCF, requesting that gates shall be closed.
3. The PCF updates flow status of affected PCC rules for the media on hold.
4. The PCF replies to the P-CSCF with a HTTP "200 OK" response.

   4a. The PCF sends a Diameter AAA message back to the P-CSCF.
5. The P-CSCF forwards the SDP answer putting media on hold within a SIP message.
6. The PCF executes interactions according to figure 5.2.2.2.2.2-1. This step implies closing the relevant media IP flow gate(s), leaving the possible related RTCP gate(s) open to keep the connection alive.

NOTE 2: This procedure occurs whenever a bidirectional media is made unidirectional or when a media is changed to inactive.

B.3.4 Media Component Removal

Figure B.3.4-1 presents the flows of PCC procedures at the removal of media component(s) from an IMS session which is not being released for both the originating and terminating sides.

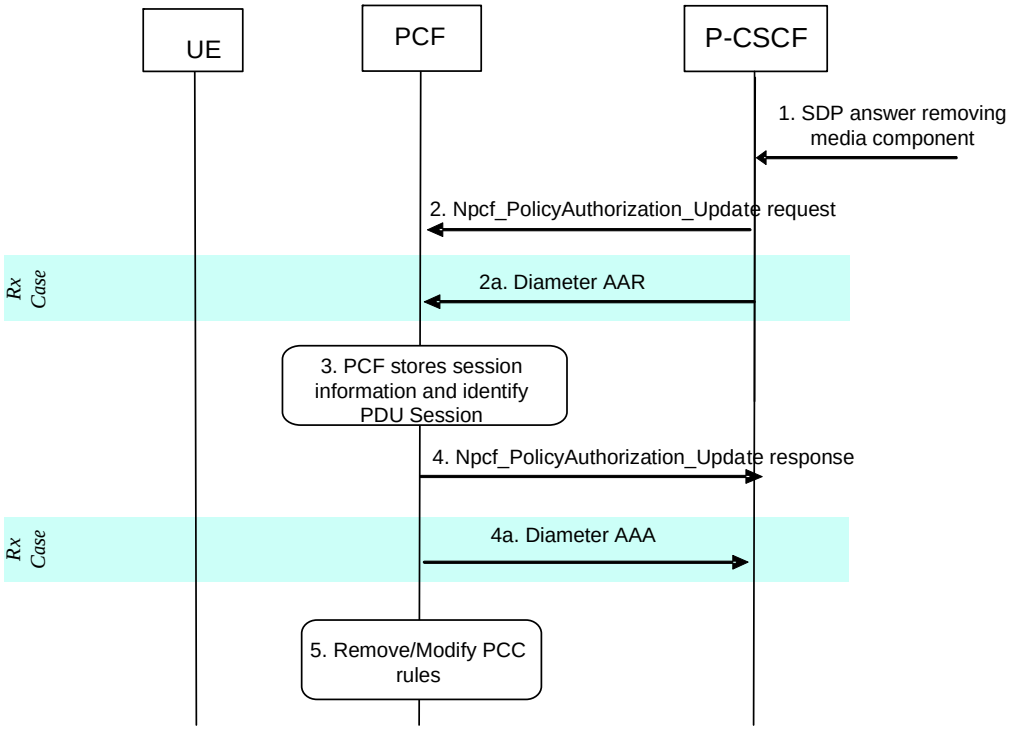


Figure B.3.4-1: Revoke authorization for IP resources at media component removal for both originating and terminating sides

1. A SIP message containing SDP indicating the removal of media component(s) is received by the P-CSCF.
2. The P-CSCF invokes the Npcf_PolicyAuthorization_Update service operation by sending an HTTP PATCH request to the "Individual Application Session Context" resource to the PCF with modified service information.

   2a. The P-CSCF sends Diameter AAR to the PCF with modified service information.
3. The PCF stores the AF session information and identifies the affected PDU session.
4. The PCF replies to the P-CSCF with a HTTP "200 OK" response.

   4a. The PCF sends a Diameter AAA message back to the P-CSCF.
5. The P-CSCF forwards the SDP answer removing a media component.
6. The PCF makes a decision on what PCC rules need to be modified or removed and executes interactions according to figure 5.2.2.2.2.2-1.

B.4 IMS Session Termination

B.4.1 Mobile initiated session release / Network initiated session release

Figure B.4.1-1 represents the mobile or network initiated IMS session release without access network information retrieval. The session release may be signalled by a SIP BYE request, or any SIP 3xx redirect response, or any 4xx, 5xx, or 6xx SIP final error response to an initial INVITE request. If any 4xx, 5xx, or 6xx SIP final error response to Re-INVITE or UPDATE request just terminates the transaction, then the session is not released, otherwise if the error response terminates the dialog then the session is released.

Figures B.4.1-2 and B.4.1-3 presents the network initiated and the mobile initiated IMS session release with access network information retrieval, respectively.

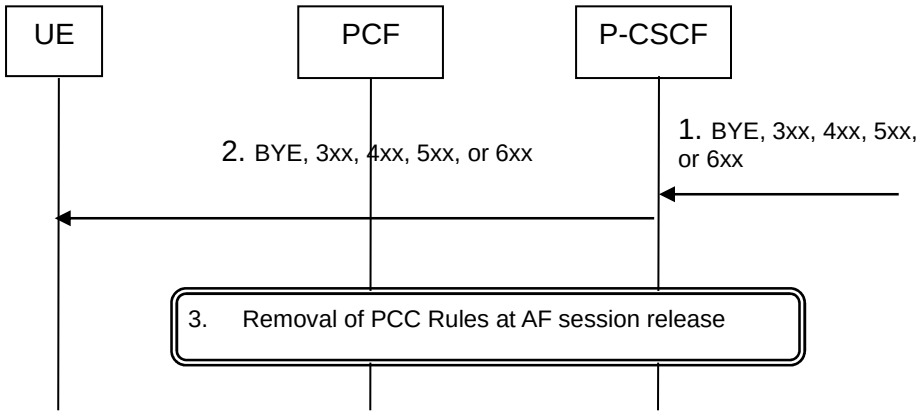


Figure B.4.1-1: IMS session termination without access network information retrieval

1. SIP BYE request, a SIP 3xx redirect response, or any 4xx, 5xx, or 6xx SIP final error response to an initial INVITE or any 4xx, 5xx, or 6xx SIP final error response to Re-INVITE or UPDATE which terminates the dialog is received by the P-CSCF.
2. P-CSCF forwards the BYE request, or the SIP 3xx redirect response, or any 4xx, 5xx, or 6xx SIP final error response.
3. The interactions in Figure 5.2.2.2.2.3-1 are applicable.

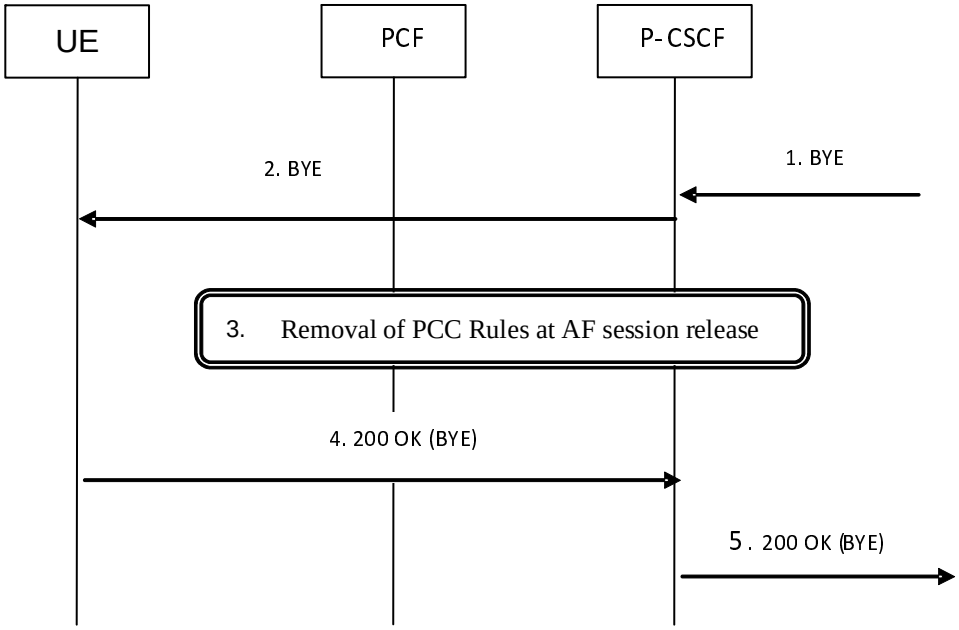


Figure B.4.1-2: network initiated IMS session termination with access network information retrieval

1. SIP BYE request is received by the P-CSCF.
2. The P-CSCF forwards the BYE request.
3. In parallel to step 2, the interactions in Figure 5.2.2.2.2.3-1 take place. Within those interactions, the P-CSCF requests and receives the access network information.
4. The P-CSCF receives the SIP 200 OK (BYE) response.
5. The P-CSCF forwards the SIP 200 OK (BYE) response. It includes the access networking information obtained in step 3 as the network provided location information.

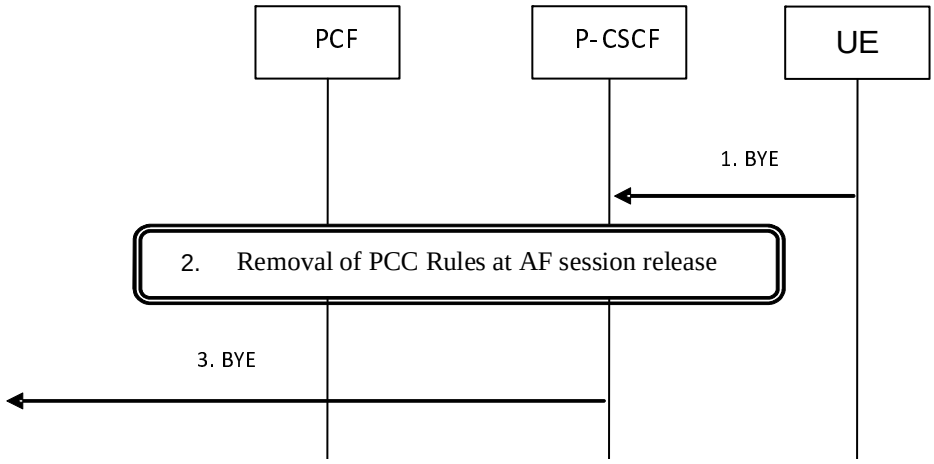


Figure B.4.1-3: mobile initiated IMS session termination with access network information retrieval

1. SIP BYE request is received by the P-CSCF.
2. The interactions in Figure 5.2.2.2.2.3-1 are applicable. Within those interactions, the P-CSCF requests and receives the access network information.
3. The P-CSCF forwards the BYE request. It includes the access network information obtained in step 2 as the network provided location information.

B.4.2 QoS Flow Release/Loss

A QoS flow release may affect all IP-Flows within an IMS Session. Flows in Figure 5.2.2.3-1 apply.

B.5 Subscription to Notification of Signalling Path Status at IMS Registration

This clause covers the optional Subscription to Notifications of IMS Signalling Path Status upon an initial successful IMS Registration procedure.

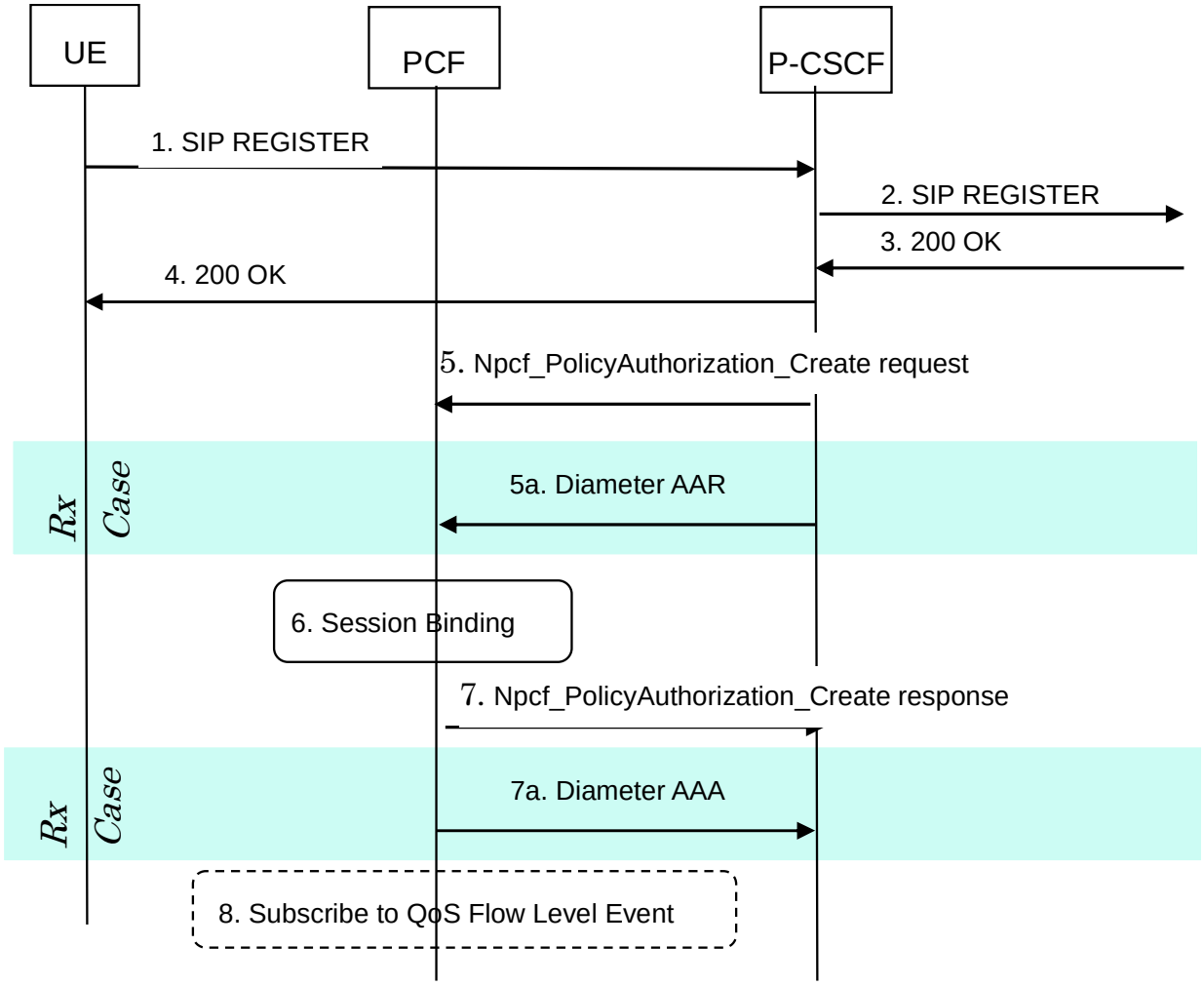


Figure B.5-1: Subscription to Notification of IMS Signaling Path Status at initial IMS Registration

1-4. The user initiates an initial SIP Registration procedure. The SIP Registration procedure is completed successfully (user has been authenticated and registered within the IMS Core NW).

5. The P-CSCF requests the creation of a new "Individual Application Session Context" resource with the intention to subscribe to the status of the IMS Signaling path. The P-CSCF sends an HTTP POST request message to the PCF.

5a. The P-CSCF requests the establishment of a new Diameter Rx session with the intention to subscribe to the status of the IMS Signaling path. The P-CSCF sends a Diameter AAR command to the PCF.

6. The PCF performs session binding and identifies corresponding PCC Rules related to IMS Signalling.

7. The PCF confirms the subscription to IMS Signaling path status and replies with an HTTP "201 Created" message back to the P-CSCF.

7a. The PCF confirms the subscription to IMS Signaling path status and replies with a Diameter AAA command back to the P-CSCF.

8. If the PCF had not previously subscribed to the required QoS level events from the PDU session for the affected PCC Rules, then the PCF shall do so now. The PCR initiates procedures according to figure 5.2.2.2.1-1.

B.6 Provisioning of SIP signalling flow information at IMS Registration

This clause covers the optional Provisioning of SIP signalling flow information upon an initial successful IMS Registration procedure.

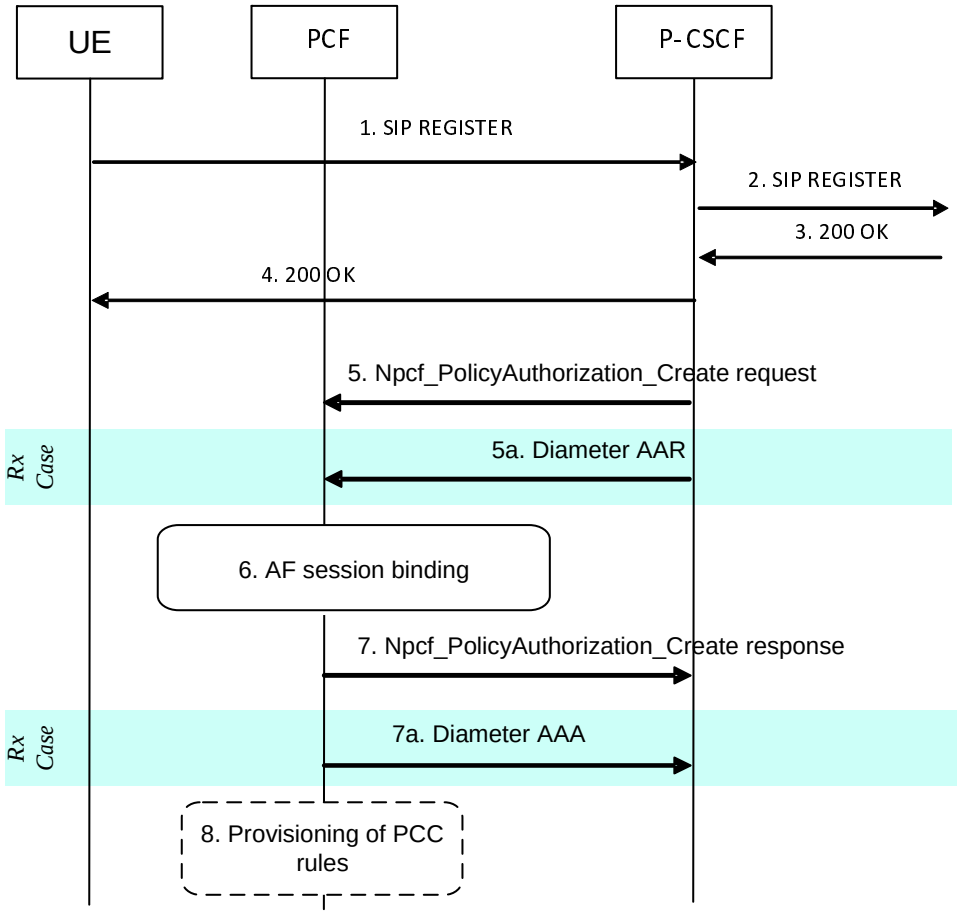


Figure B.6-1: Provisioning of SIP Signalling Flow Information at initial IMS Registration

1-4. The user initiates an initial SIP Registration procedure. The SIP Registration procedure is completed successfully (user has been authenticated and registered within the IMS Core NW).

5. The P-CSCF requests the creation of a new "Individual Application Session Context" resource with the intention to provision the information about the SIP signalling flows established between the UE and the P-CSCF. The P-CSCF invokes the Npcf_PolicyAuthorization_Create service operation to the PCF by sending an HTTP POST request to the "Application Sessions" resource.

   5a. The P-CSCF requests the establishment of a new Diameter Rx session with the intention to provision the information about the SIP signalling flows established between the UE and the P-CSCF. The P-CSCF sends a Diameter AAR command to the PCF.

6. The PCF performs session binding and identifies corresponding PCC Rules related to IMS Signalling.

7. The PCF replies to the P-CSCF with a HTTP "201 Created" response and includes the URI of the "Individual Application Session Context" resource in the Location header field.

   7a. The PCF replies to the P-CSCF with a Diameter AAA.

8. If the PCF had not previously provisioned PCC rules corresponding to the received SIP signalling flows, then the PCF executes interactions according to figure 5.2.2.2.2.1-1. This step implies provisioning of PCC rules.

B.7 Subscription to Notification of Change of Access Type at IMS Registration

This clause covers the optional Subscription to Notifications of change in the access type upon an initial IMS Registration procedure.

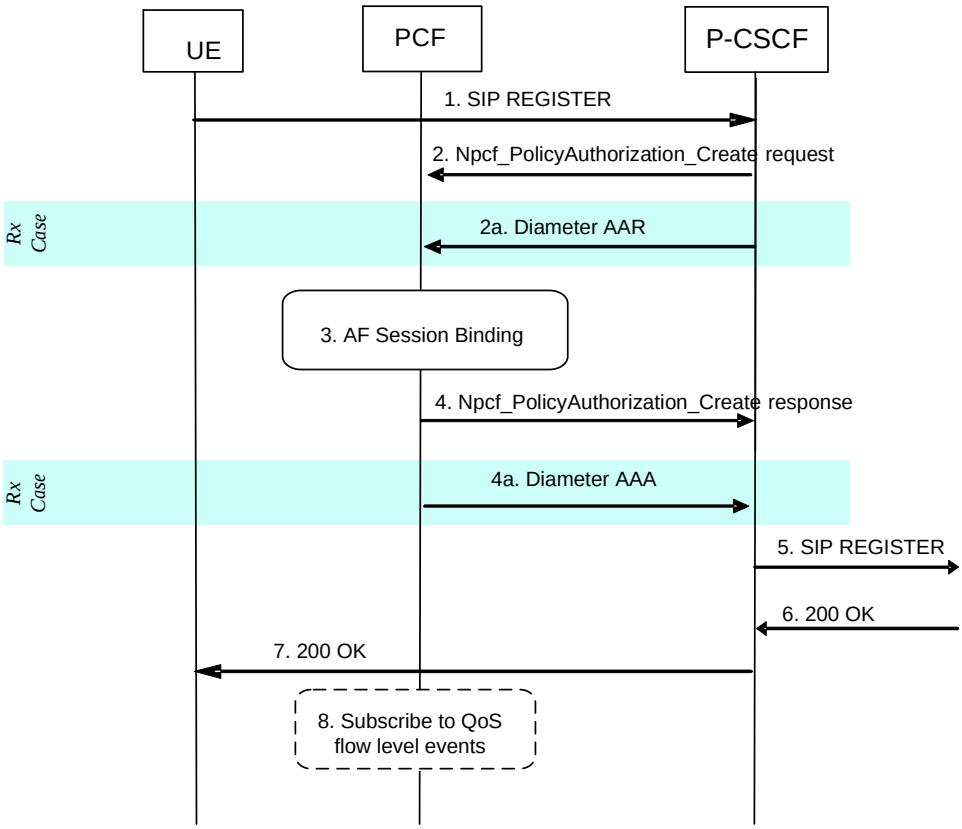


Figure B.7-1: Subscription to Notification of change of IP-CAN Type at initial IMS Registration

1.- The user initiates an initial SIP Registration procedure.

2. The P-CSCF requests the creation of a new "Individual Application Session Context" resource with the intention to subscribe to the notification of access type change by invoking the Npcf_PolicyAuthorization_Create service operation to the PCF. The P-CSCF sends an HTTP POST request to the "Application Sessions" resource.

   2a. The P-CSCF requests the establishment of a new Diameter Rx session with the intention to subscribe to the notification of access type change. The P-CSCF sends a Diameter AAR command to the PCF.

NOTE: It should be possible for the P-CSCF to request the subscription to notification of IMS Signalling path status and PLMN changes also in this step.

3. The PCF performs session binding and identifies corresponding PCC Rules related to IMS Signalling.

4. The PCF confirms the subscription to notification of access type change and replies to the P-CSCF with a HTTP "201 Created" response and includes the URI of the "Individual Application Session Context" resource in the Location header field.

   4a. The PCF confirms the subscription to notification of change of access type and replies with a Diameter AAA command back to the P-CSCF.

   The PCF includes in the response the type of access type currently in use.

5-7. The SIP Registration procedure is completed successfully (user has been authenticated and registered within the IMS Core NW).

8. If the PCF had not previously subscribed to the required QoS flow level event from the access type (i.e. access type change and RAT type change, if applicable), then the PCF shall do so now. The PCF initiates procedures according to figure 5.2.2.2.2.1-1.

B.8 Subscription to Notification of Change of PLMN Identifier at IMS Registration

This clause covers the optional Subscription to Notifications of change in the PLMN identifier upon an initial IMS Registration procedure. The PLMN identifier or SNPN identifier where the UE is currently located is provided within the Notification of change in the PLMN identifier. n2

NOTE 1: The SNPN identifier consists of the PLMN identifier and the NID.

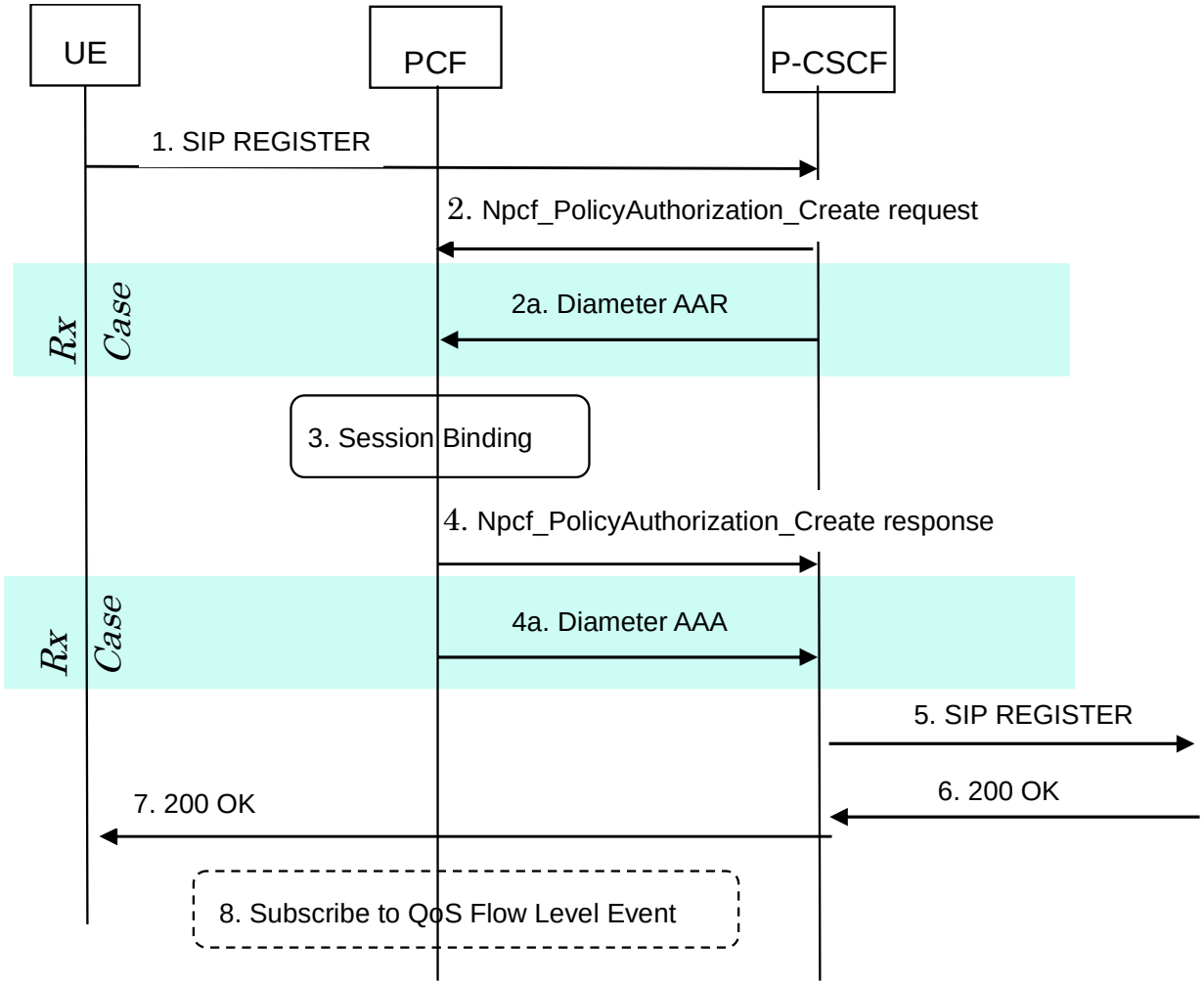


Figure B.8-1: Subscription to Notification of change of PLMN Identifier at initial IMS Registration

1. The user initiates an initial SIP Registration procedure.

2. The P-CSCF requests the creation of a new "Individual Application Session Context" resource with the intention to subscribe to notification of PLMN Identifier Change. The P-CSCF sends an HTTP POST request message to the PCF.

2a. The P-CSCF requests the establishment of a new Diameter Rx session with the intention to subscribe to notification of PLMN Identifier Change. The P-CSCF sends a Diameter AAR command to the PCF.

NOTE 2: It should be possible for the P-CSCF to request the subscription to notification of IMS Signalling path status and IP-CAN Type changes also in this step.

3. The PCF performs session binding and identifies corresponding PCC Rules related to IMS Signalling.

4. The PCF confirms the subscription to notification of PLMN Identifier Change and replies with an HTTP "201 Created" message back to the P-CSCF.

4a. The PCF confirms the subscription to notification of PLMN Identifier Change and replies with a Diameter AAA command back to the P-CSCF.

5-7. The SIP Registration procedure is completed successfully (user has been authenticated and registered within the IMS Core NW).

8. If the PCF had not previously subscribed to the required QoS level events from the PDU session for the affected PCC Rules, then the PCF shall do so now. The PCRF initiates procedures according to figure 5.2.2.2.1-1.

NOTE 3: If the PLMN identifier is not available in step 4 (step 4a for Rx case), the P-CSCF will wait to get it in step 8 before progressing the SIP Register, i.e. steps 5, 6 and 7 will occur after step 8.

B.9 P-CSCF Restoration

This clause is applicable if P-CSCF Restoration is to be performed.

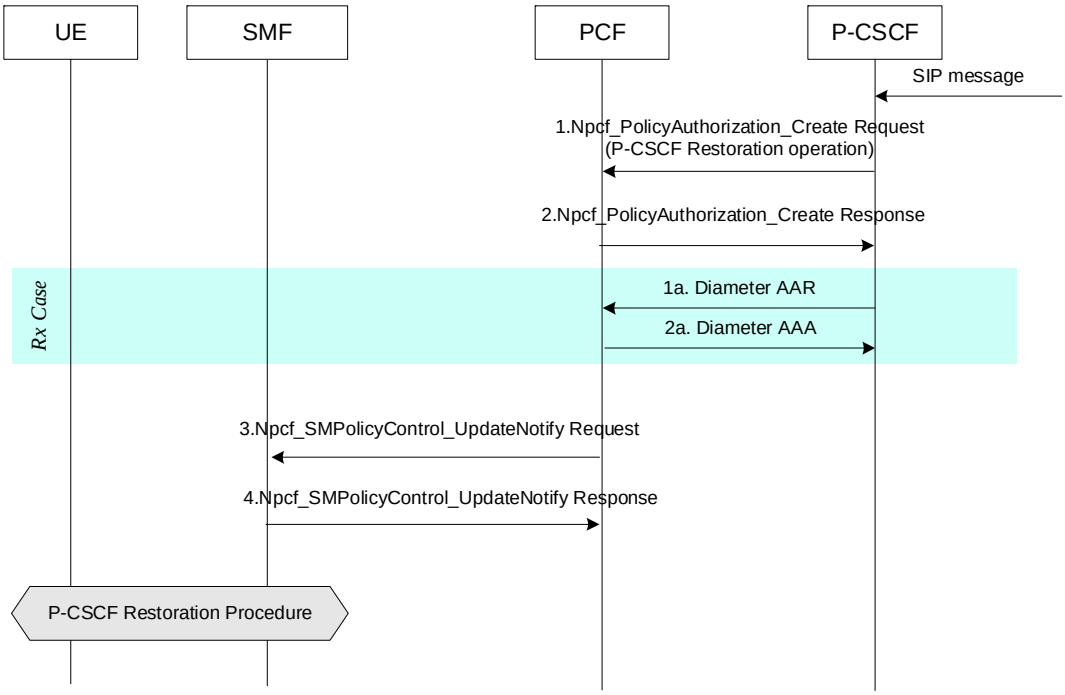


Figure B.9-1: P-CSCF Restoration

1. The P-CSCF invokes the "P-CSCF restoration" custom operation to initiate a P-CSCF Restoration procedure, as defined in 3GPP TS 23.380 [45], by sending an HTTP POST request to the "…/pcscf-restoration" URI, which can contain the IP address of the UE within the "ueIpv4" attribute or "ueIpv6" attribute, and, if required to solve private IPv4 case, the "ipDomain" attribute or the "sliceInfo" attribute if available, The SUPI in the "supi"

attribute and the DNN in the "dnn" attribute are provided if the UE IP address is not available, or if available, IP address is not unique and the ipDomain" attribute and/or the "sliceInfo" attribute are not available.

1a. sends an AAR command to PCF to initiate a P-CSCF Restoration procedure, as defined in the 3GPP TS 23.380 [45]. The AAR command contains a Rx-Request-Type AVP with value set to PCSCF_RESTORATION and can contain the IP address of the UE within Framed-IP-Address AVP (if available) or the Framed-Ipv6-Prefix AVP (if available), IMSI (if available) within the Subscription-Id AVP, the IMS DNN (if available) within the Called-Station-Id AVP and/or the IP address domain (if available) within the IP-Domain-Id AVP.

2. The PCF acknowledges the received HTTP POST request with a HTTP "204 No content" response.

2a. When receiving the AAR command for P-CSCF Restoration from the P-CSCF, the PCF acknowledges the AAR by sending an AAA command to the P-CSCF.

3. When receiving the request for the "P-CSCF restoration" custom operation via N5 interface, or the AAR command from the Rx interface, the PCF finds the corresponding PDU session according to the received information from the P-CSCF, and invokes the Npcf_SMPolicyControl_UpdateNotify to indicate the SMF the request of P-CSCF restoration for the corresponding PDU session by sending an HTTP POST request to the SMF notification URI and including in body the SmPolicyDecision data type the "pcscfRestIndication" attribute set to true.

4. When receiving the HTTP POST request indicating P-CSCF Restoration, the SMF acknowledges the request by sending an HTTP "204 No Content" response to the PCF and performs the subsequent P-CSCF Restoration procedure as specified in 3GPP TS 23.380 [45].

NOTE: If the PDU session is terminated as result of P-CSCF Restoration, the SMF invokes the Npcf_SMPolicyControl_Delete service operation to terminate the SM Policy Association and delete the corresponding "Individual SM Policy" resource in the PCF.

B.10 IMS Restricted Local Operator Services

RLOS may be supported as described in clause B.1 with the following differences:

- Only RLOS requests over E-UTRAN are supported in this release of the specification
- emergency service is replaced by RLOS;
- emergency indication is replaced by RLOS indication;
- emergency session is replaced by RLOS session;
- emergency DNN is replaced by RLOS DNN; and
- the call back functionality is not applicable to RLOS.

NOTE: Clause B.2.2 is not supported for RLOS, because only UE originated RLOS requests over E-UTRAN are supported and there is no support for mobile terminated services as specified in 3GPP TS 23.221 [46].

B.11 Retrieval of Network Provided Location Information for SMS over IP at Originating side

This clause covers the optional request of access network information for SMS over IP.

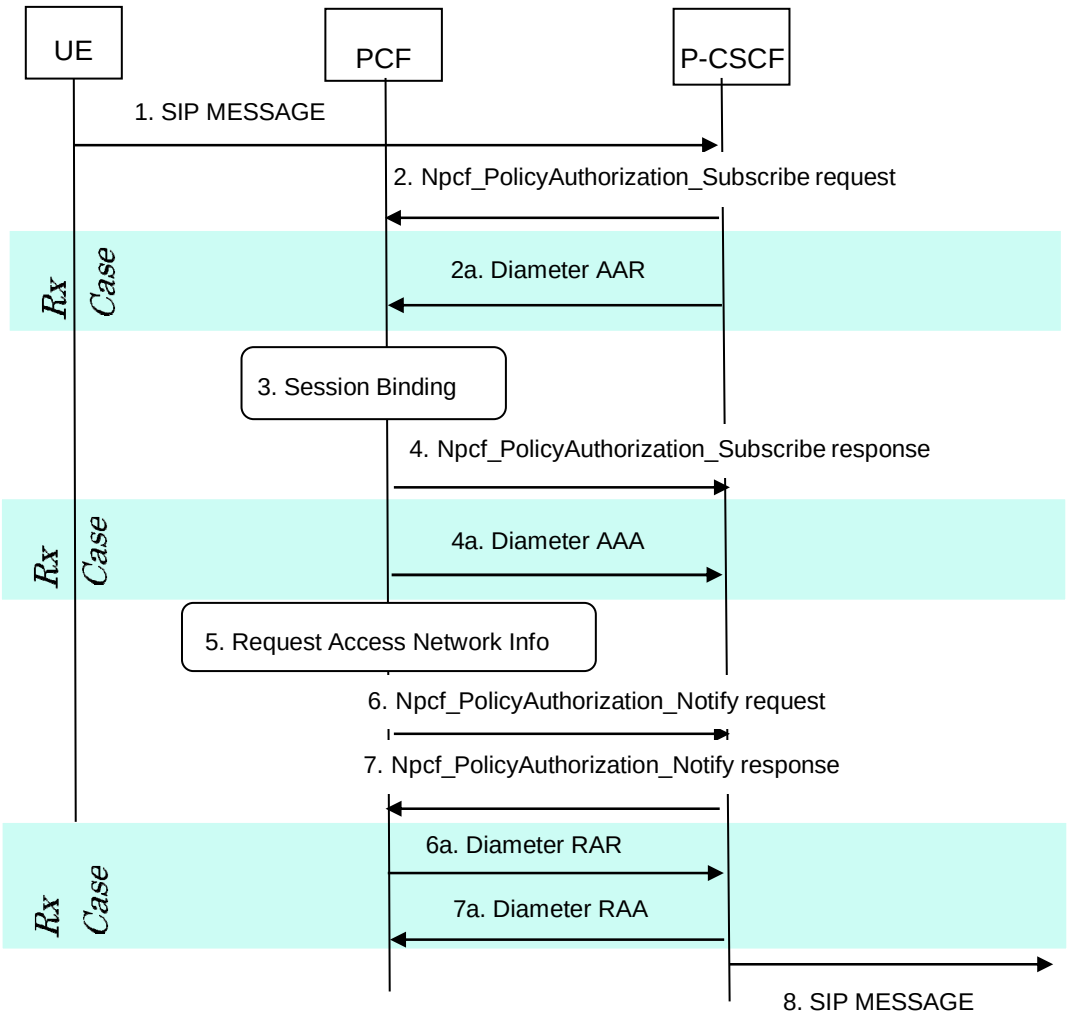


Figure B.11.1: Retrieval of Access Network Information for SMS over IP at originating side

1.- The UE sends a SIP MESSAGE request to IMS.

2. The P-CSCF requests the creation of a new "Individual Application Session Context" resource with the intention of retrieval the access network information. The P-CSCF sends an HTTP POST request message to the PCF.

   2a. The P-CSCF requests the establishment of a new Diameter Rx session with the intention of retrieval the access network information. The P-CSCF sends a Diameter AAR command to the PCF.

3. The PCF performs session binding.

4. The PCF replies with an HTTP "201 Created" message back to the P-CSCF.

   4a. The PCF replies with a Diameter AAA command back to the P-CSCF.

5. The PCF requires access network information according to figure 5.2.2.2.1-1.

6. The PCF invokes the Npcf_PolicyAuthorization_Notify service operation to forward the access network information received in step 5 in an HTTP POST request sent to the Notification URI received in step 4.

   6a. The PCF forwards the access network information received in step 5 in a Diameter RAR.

7. The P-CSCF acknowledges the receipt of the notification request with an HTTP "204 No Content" response to the PCF.

   7a. The P-CSCF acknowledges the receipt of Diameter RAR.

8. IMS sends a SIP MESSAGE to the terminating side including the network provided location information.

After, the P-CSCF terminates the AF session as described in clause 5.2.2.2.2.3.

B.12 Retrieval of Network Provided Location Information for SMS over IP at Terminating side

This clause covers the optional request of access network information for SMS over IP.

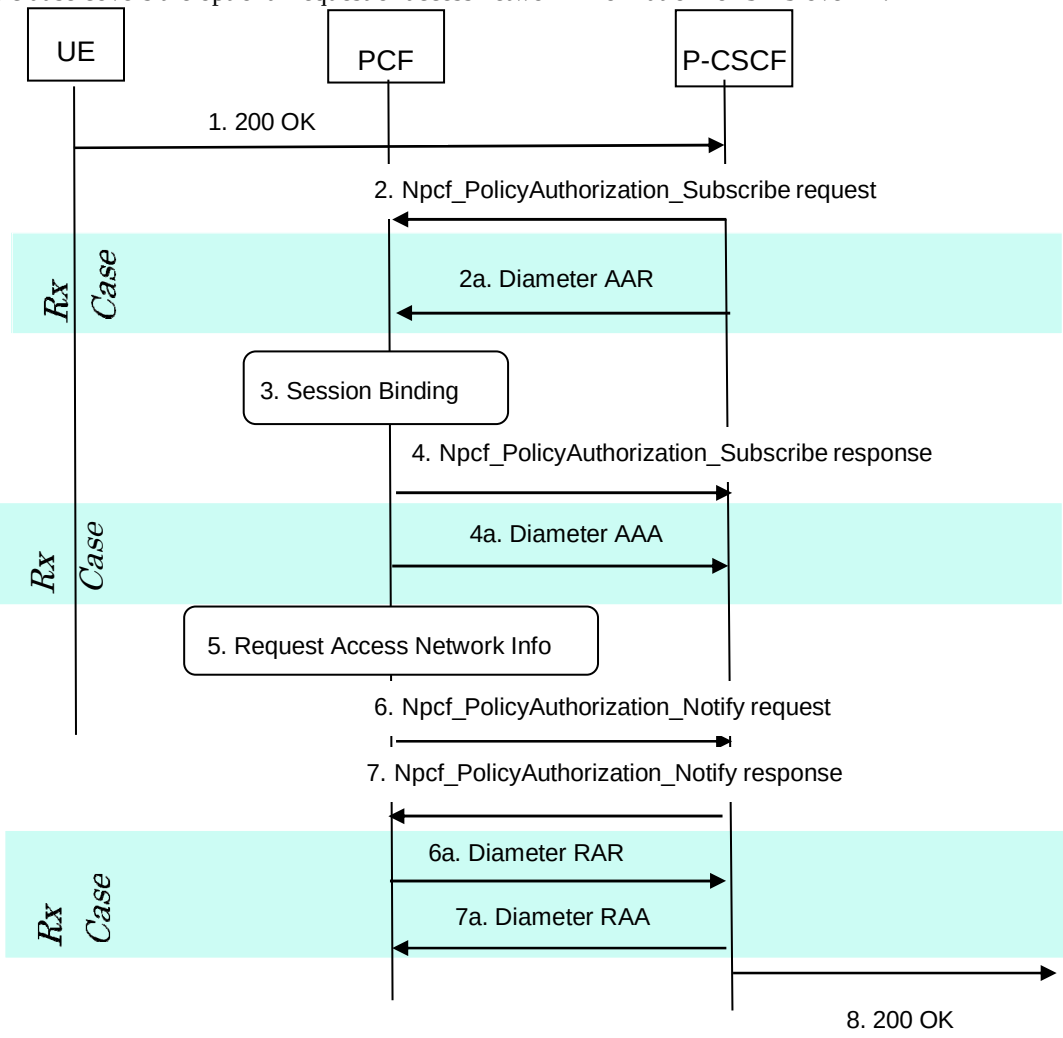


Figure B.12.1: Retrieval of Access Network Information for SMS over IP at terminating side

1.- The P-CSCF receives the 200 OK message on SIP MESSAGE request.

2. The P-CSCF requests the creation of a new "Individual Application Session Context" resource with the intention of retrieval the access network information. The P-CSCF sends an HTTP POST request message to the PCF.

   2a. The P-CSCF requests the establishment of a new Diameter Rx session with the intention of retrieval the access network information. The P-CSCF sends a Diameter AAR command to the PCF.

3. The PCF performs session binding.

4. The PCF replies with an HTTP "201 Created" message back to the P-CSCF.

   4a. The PCF replies with a Diameter AAA command back to the P-CSCF.

5. The PCF requires access network information according to figure 5.2.2.2.1-1.

6. The PCF invokes the Npcf_PolicyAuthorization_Notify service operation to forward the access network information received in step 5 in an HTTP POST request sent to the Notification URI received in step 4.

6a. The PCF forwards the access network information received in step 5 in a Diameter RAR.

7. The P-CSCF acknowledges the receipt of the notification request with an HTTP "204 No Content" response to the PCF.

   7a. The P-CSCF acknowledges the receipt of Diameter RAR.

8. The P-CSCF forwards the 200 OK including the network provided location information.

After, the P-CSCF terminates the AF session as described in clause 5.2.2.2.2.3

Annex C (informative): Guidance for underlay network to support QoS differentiation for User Plane IPsec Child SA

C.1 Access to PLMN services via SNPN and access to SNPN services via PLMN

To access PLMN services, a UE in SNPN access mode that has successfully registered with a SNPN may perform another registration via the SNPN User Plane with the PLMN, discovering and establishing connectivity to an N3IWF in the PLMN.

In these scenarios, the PLMN is the overlay network and the SNPN is the underlay network.

Equivalently, to access SNPN services, a UE that has successfully registered with a PLMN over 3GPP access may perform another registration via the PLMN User Plane with a SNPN, discovering and establishing connectivity to an N3IWF in the SNPN.

In these scenarios, the SNPN is the overlay network and the PLMN is the underlay network.

C.2 QoS differentiation support in the underlay network for overlay services

When an overlay network service has specific QoS requirements that need to be fulfilled by the underlay network, an SLA needs to be determined between the two networks.

The SLA covers the selective services of the overlay network that require QoS support in the underlay network. The rest of the overlay network traffic could be handled in best effort basis by the underlay network.

The SLA includes a mapping between the DSCP value(s) of the User Plane IPsec Child SA(s) and the QoS requirement of the overlay network service(s). The QoS requirement includes the QoS parameters (defined in 3GPP TS 23.501 [2], clause 5.7.2) that are necessary (e.g. 5QI, ARP, etc.). The SLA also includes the N3IWF IP address of the overlay network.

Based on the SLA, the N3IWF in the overlay network derives DSCP value(s) of the User Plane IPsec Child SA(s) from the QoS requirements of the service(s), and the SMF/PCF in the underlay network derives the QoS requirements for the User Plane IPsec Child SA(s) from the DSCP value(s) of the traffic. The description of the PCC procedures for the underlay network support of QoS differentiation for User Plane IPsec Child SA(s) for network initiated QoS and UE initiated QoS modification are described in clauses C.4 and C.5 respectively.

In order to facilitate the SLA, the clause C.3 below provides a guidance for details of the possible mapping table between DSCP value(s) of the User Plane IPsec Child SA(s) and the QoS parameters of the overlay network service(s). The QoS parameters that the underlay network may need to determine based on the DSCP value (e.g. ARP, 5QI, GBR, MBR, …) should be described in the SLA, and configured in the underlay network SMF and/or PCF and in the N3IWF in the overlay network.

C.3 Guidelines for QoS requirements to/from DSCP mapping

The mapping guidelines in this clause represent an example of how the DSCP values can be used to reference a combination of QoS parameters.

In these scenarios, where it is pursued to determine the applicable QoS in the underlay network based on the QoS handling of the service in the overlay network, the DSCP values represent a tool for the underlay network to reproduce the combination of QoS parameters determined by the overlay network.

To achieve this goal, it is assumed that the DSCP marking(s) done by the N3IWF remain unaltered in the underlay network. The non-alteration of the DSCP values on NWu interface should be governed and ensured by the SLA and by transport level agreements.

The mapping guidelines in the tables below are only examples and are not expected to fit every possible deployment. E.g., a deployment may use DSCP 44 and DSCP EF for conversational voice, 5QI 1, indicating the different DSCP values different GBR UL/DL values while another one may use only DSCP 44 and estimate the GBR/MBR parameters that would best fit with a set of possible different GBR/MBR requirements. The DSCP to/from QoS parameter mapping is determined by network administrators, as needed.

Table C.3-1: Example of QoS parameters to/from DSCP mapping for conversational voice

DSCP	QoS parameter					
	5QI	ARP PL	ARP PC	ARP PV	GBR UL/DL	MBR UL/DL
46	1	10	NO	YES	31 kbps UL/DL (IPv4 case) 39 kbps UL/DL (IPv6 case)	31 kbps UL/DL (IPv4 case) 39 kbps UL/DL (IPv6 case)
44	1	10	NO	YES	25 kbps UL/DL (IPv4 case) 33 kbps UL/DL (IPv6 case)	31 kbps UL/DL (IPv4 case) 39 kbps UL/DL (IPv6 case)
45	1	10	NO	YES	32 kbps UL/DL (IPv4 case) 40 kbps UL/DL (IPv6 case)	32 kbps UL/DL (IPv4 case) 40 kbps UL/DL (IPv6 case)

Table C.3-2: Example of QoS parameters to/from DSCP mapping for conversational video

DSCP	QoS parameter					
	5QI	ARP PL	ARP PC	ARP PV	GBR UL/DL	MBR UL/DL
34	2	11	NO	YES	64 kbps UL/DL (IPv6 case)	704 kbps UL/DL (IPv6 case)

C.4 Network initiated QoS modification

The mapping agreed in SLA is configured at N3IWF of the overlay network (QoS parameters to DSCP mapping) and at the SMF/PCF of the underlay network (DSCP to QoS parameters). If a dedicated DNN/S-NSSAI is used in the underlay network for providing access to the N3IWF in the overlay network, the SMF/PCF in the underlay network can be configured to enable packet detection (based on N3IWF IP address and DSCP value) for PDU sessions associated with the dedicated DNN/S-NSSAI.

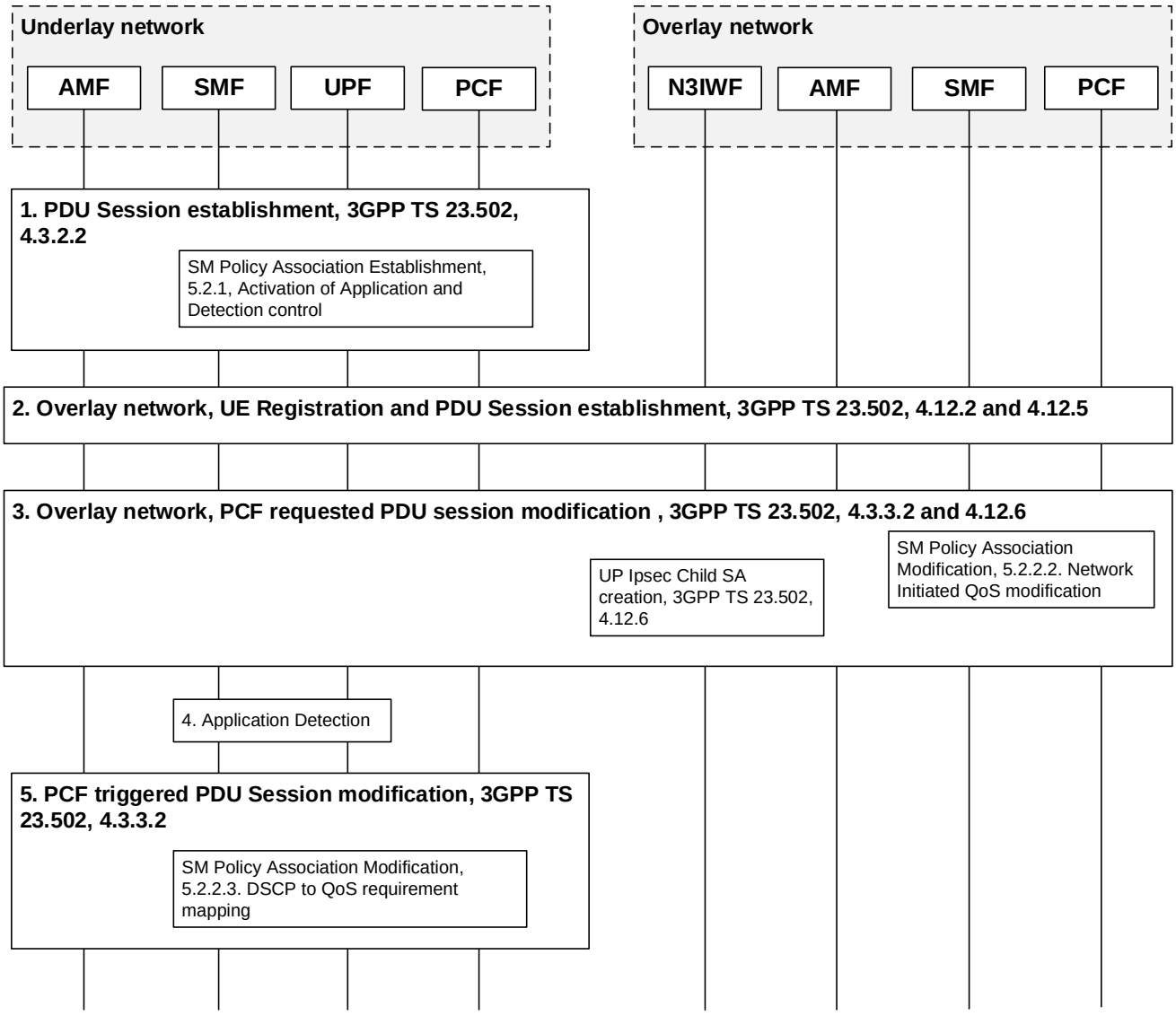


Figure C.4-1: Example of network initiated QoS procedure

1. When the UE establishes a PDU Session in underlay network, the SMF creates a SM Policy Association with the PCF (clause 5.2.1), which determines the PCC rules to install based on UE subscription information and local configuration (which takes into account the SLA). The PCF in the underlay network installs in the SMF PCC rule(s) that contain an application identifier (see 3GPP TS 29.512 [9], clause 4.2.2.7) that refer to the N3IWF IP address and the DSCP value(s) of the User Plane IPsec Child SA(s) of the overlay network that require QoS differentiation by the underlay network.

2. The UE registers (see 3GPP TS 23.502 [3], clause 4.12.2) and establishes PDU Session (3GPP TS 23.502 [3], clause 4.12.5) in the overlay network via the User Plane connectivity established in the underlay network.

3. When the UE is accessing a specific service of the overlay network, the service can e.g. request via the PCF a specific QoS treatment to the overlay network. The PCF then invokes the SM Policy Association Modification procedure (see clause 5.2.2.2), which triggers the creation of the corresponding QoS Flow in the overlay network. The N3IWF is configured to allocate different dedicated User Plane IPsec Child SA(s) for each overlay network QoS Flow(s) (3GPP TS 23.502 [3], clause 4.12.6).

   The N3IWF uses the QoS Flow level QoS parameters it receives from SMF in overlay network along with the mapping agreed in the SLA to derive a specific DSCP value for the User Plane IPsec Child SA (e.g. QoS parameters to DSCP mapping table described in clause C.3). The N3IWF can provide to the UE the DSCP value for the User Plane IPsec Child SA (clause 4.12.5, step 4a and 4c of TS 23.502 [3]) mapped to QoS Flow for the specific network service.

   The UE receives the QoS Flow level QoS parameters (e.g. 5QI, GFBR, MFBR, as specified in TS 24.501 [33]) from SMF/PCF in overlay network for the QoS Flow which is created for the specific overlay network service.

   The N3IWF (for DL) and the UE (for UL) will set the DSCP marking in the outer IP header of the User Plane IPsec Child SA.

   When the service requests the termination of the specific QoS treatment to the overlay network, the PCF invokes the SM Policy Association Modification procedure (see clause 5.2.2.2), which triggers the termination of the corresponding QoS Flow(s) in the overlay network. The N3IWF terminates the dedicated User Plane IPsec Child SA(s) for each terminated overlay network QoS Flow(s).

4. The overlay network traffic between UE and N3IWF using the specific DSCP marking will be detected by the UPF/SMF in the underlay network based on the previously installed PCC rules.

   When the N3IWF terminates the dedicated User Plane IPsec Child SA(s), the termination of the traffic with the specific DSCP marking will be detected by the UPF/SMF in the underlay network based on the previously installed PCC rules.

5. The UE and N3IWF detected traffic are reported by the SMF to the PCF as described in 3GPP TS 29.512 [9], clause 4.2.4.6, using the SM Policy Association Modification procedure described in clause 5.2.2.3. The PCF, based on the DSCP value of the detected traffic, derives the QoS requirements for the related service and installs new PCC rules on the SMF including the QoS parameters (5QI, ARP, GBR, etc., as described in the DSCP to QoS parameters mapping of the SLA) for handling the packets corresponding to the specific User Plane IPsec Child SA. The SMF in the underlay network may generate a separate QoS Flow, as described in clause 4.3.3 of TS 23.502 [3], for the traffic of the User Plane IPsec Child SA, which will receive the same QoS treatment as the QoS treatment of the overlay network for the service traffic.

   The detection of the termination of the UE and N3IWF traffic is reported by the SMF to the PCF as described in 3GPP TS 29.512 [9], clause 4.2.4.6, using the SM Policy Association Modification procedure described in clause 5.2.2.3. The PCF, based on the identification of the traffic, removes the previously provided PCC rules that handle the packets corresponding to the specific User Plane IPsec Child SA. The SMF in the underlay network may terminate the corresponding QoS Flow.

C.5 UE initiated QoS modification

To support QoS differentiation in the underlay network with UE-requested QoS modification, the UE can request for an IPsec SA the same QoS parameters from the underlay network as the QoS parameters provided by the overlay network for the related service. It is assumed that UE-requested QoS modification is used only when the 5QIs used by the overlay network are from the range of standardized 5QIs. The packet filter in the UE-requested QoS rule can be based on the N3IWF address and the SPI associated with the IPsec SA.

The mapping (DSCP to QoS requirements) agreed in SLA is configured at the SMF/PCF of the underlay network and in the N3IWF of the overlay network.

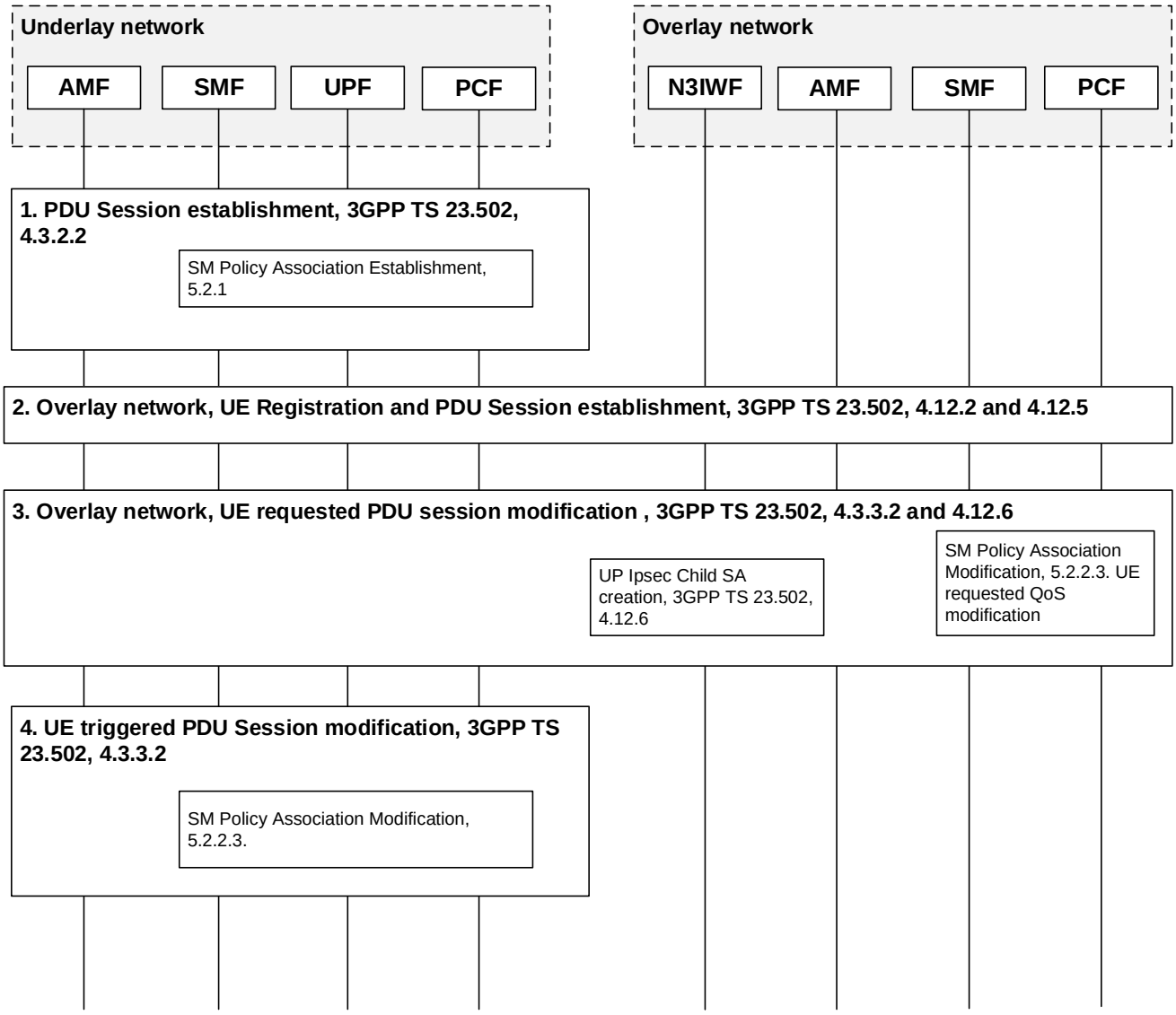


Figure C.5-1: Example of UE initiated QoS procedure

1. When the UE establishes a PDU Session in underlay network, the SMF creates a SM Policy Association with the PCF (clause 5.2.1).

2. UE registers (3GPP TS 23.502 [3], clause 4.12.2) and establishes PDU Session (3GPP TS 23.502 [3], clause 4.12.5) in the overlay network via the User Plane connectivity established in the underlay network.

3. When UE is accessing a specific service of the overlay network, the UE e.g. can request to the overlay network a specific QoS treatment for this service. The SMF in the overlay network invokes the SM Policy Association Modification procedure (see clause 5.2.2.3) and includes the UE-requested QoS as described in 3GPP TS 29.512 [9], clause 4.2.4.17. The PCF in the overlay network responds to the SMF with the PCC rule(s) with the QoS requirements as per the UE-requested QoS. The SMF creates the corresponding QoS Flow in the overlay network (see clause 4.3.3 of TS 23.502 [3]).

   The N3IWF is configured to allocate different dedicated User Plane IPsec Child SA(s) for each overlay network QoS Flow(s) (3GPP TS 23.502 [3], clause 4.12.6) that requires underlay network QoS support. The UE receives the QoS Flow level QoS parameters (e.g. 5QI, GFBR, MFBR, as specified in TS 24.501 [33]) from SMF/PCF in overlay network for the QoS Flow which is created for the specific overlay network service.

   If an SLA exists, the SLA is configured in the N3IWF in the overlay network, and the N3IWF can provide to the UE the DSCP value for the User Plane IPsec Child SA (clause 4.12.5, step 4a and 4c of TS 23.502 [3]).

When the UE requests the termination of the UE-requested QoS in the overlay network as described in 3GPP TS 29.512 [9], clause 4.2.4.17, the PCF in the overlay network responds to the SMF with the removal of the corresponding PCC rule(s). The SMF terminates the corresponding QoS Flow in the overlay network

4 In order to ensure the underlay network handles the traffic of the overlay network service with the desired QoS, the UE can request a new QoS Flow for the PDU session in the underlay network for the concerned User Plane IPsec Child SA(s). The UE triggers a PDU session modification procedure and derives the UE-requested QoS for the underlay network from the QoS Flow level QoS parameters the UE received from the overlay network. The Packet Filter in the QoS rule of the request includes the overlay network N3IWF IP address and SPI associated with the User Plane IPsec Child SA.

The SMF in the underlay network, after receiving the PDU Session Modification Request, invokes the SM Policy Association Modification procedure (see clause 5.2.2.3) to notify to the PCF that the UE has initiated a resource modification (see 3GPP TS 29.512 [9], clause 4.2.4.17). The PCF in the underlay network determines if the request can be authorized based on UE subscription and local policy which can take into account the SLA between overlay network and underlay network. If the request is authorized, the PCF generates a new PCC rule with the UE-requested QoS, and includes it in the response to the SMF in order to create new QoS Flow in underlay network using the QoS Flow level QoS parameters from the overlay network. The generated SDF refers to the N3IWF IP address and the SPI (provided by the UE in Traffic filter in PDU Session Modification request) to enable filtering and mapping of DL traffic towards the right PDU Session/QoS Flow within the underlay network.

- If the SLA exists, and the N3IWF in overlay network provides to the UE the DSCP value for the User Plane IPsec Child SA as described in step 3, the UE can include the DSCP value in the Packet Filter of the PDU Session Modification procedure including the UE requested QoS in the underlay network. The PCF in the underlay network performs QoS authorization of the UE QoS request considering the UE subscription and local configuration which takes into account the mapping of DSCP to QoS requirements in the SLA.

  In order to ensure the underlay network terminates the QoS handling of the traffic of the overlay network when the UE requested the termination of the UE-requested QoS in the overlay network, the UE triggers the termination of the UE requested QoS in the underlay network. The SMF in the underlay network, notifies to the PCF that the UE has initiated a resource modification to terminate the requested QoS (see 3GPP TS 29.512 [9], clause 4.2.4.17), and the PCF removes the concerned PCC rule(s). The SMF terminates the corresponding QoS Flow in the underlay network.

Annex D (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
2019-06	CT#84	CP-191089	0060	1	F	DN Authorization data for Policy Control	16.0.0
2019-06	CT#84	CP-191089	0061	1	B	Npcf_AMPolicyControl support of Allowed NSSAI	16.0.0
2019-06	CT#84	CP-191089	0062	2	B	Race condition handling	16.0.0

2019-06	CT#84	CP-191089	0065	2	B	BSF binding update	16.0.0
2019-06	CT#84	CP-191109	0066	1	B	PCF selection for ATSSS	16.0.0
2019-06	CT#84	CP-191085	0068	1	B	Session binding of 5WWC	16.0.0
2019-06	CT#84	CP-191089	0069	2	F	Clarifications to UE Policy Delivery, Roaming	16.0.0
2019-09	CT#85	CP-192143	0072	1	A	Session binding for IPv6 addresses	16.1.0
2019-09	CT#85	CP-192143	0076	1	A	Alignment of notification URI name and HTTP reponse code	16.1.0
2019-09	CT#85	CP-192143	0078	1	A	Corrections on NWDA procedures	16.1.0
2019-09	CT#85	CP-192143	0080		A	Corrections on PFD procedure and SM policy procedure	16.1.0
2019-09	CT#85	CP-192157	0081	1	B	BDT notification procedure	16.1.0
2019-09	CT#85	CP-192157	0082	2	B	Update NWDA procedures for more Analytics	16.1.0
2019-09	CT#85	CP-192171	0083	2	B	xBDT procedure	16.1.0
2019-12	CT#86	CP-193185	0085	1	A	Correct AMF behaviour during PCF-initiated AM Policy Association Termination procedure	16.2.0
2019-12	CT#86	CP-193223	0086	1	B	Retrieval of BDT policy data for a set of BDT reference identifiers	16.2.0
2019-12	CT#86	CP-193185	0088	1	A	Correction to PCF selection	16.2.0
2019-12	CT#86	CP-193185	0090	1	A	Correction to QoS Mapping	16.2.0
2019-12	CT#86	CP-193202	0091	2	B	QoS Handling for V2X Communication	16.2.0
2019-12	CT#86	CP-193202	0092	2	B	QoS mapping for QoS Handling for V2X Communication	16.2.0
2019-12	CT#86	CP-193180	0093	1	B	Architecture clarification for eSBA	16.2.0
2019-12	CT#86	CP-193180	0094	2	B	PCF selection for eSBA	16.2.0
2019-12	CT#86	CP-193181	0097	1	B	Include AF relocation acknowledgement into Traffic influence procedures	16.2.0
2019-12	CT#86	CP-193215	0098	2	B	Coverage and Handover Enhancements for Media (CHEM)	16.2.0
2019-12	CT#86	CP-193197	0099	1	B	MCS Priority Level	16.2.0
2019-12	CT#86	CP-193223	0101		F	Remove EN related to BDT reference ID storage in SMPolicyData	16.2.0
2019-12	CT#86	CP-193217	0102	2	B	QoS Parameter mapping at AF, N5 interface	16.2.0
2019-12	CT#86	CP-193196	0103	4	B	Skeleton for Annex B, Signalling Flows for IMS	16.2.0
2020-03	CT#87e	CP-200208	0100	2	B	BDT renegotiation upon the network conditions change	16.3.0
2020-03	CT#87e	CP-200215	0105	1	F	Incorrect figure 5.2.3.1-1: SMF-initiated SM Policy Association Termination procedure	16.3.0
2020-03	CT#87e	CP-200215	0106		B	Impacts on QoS mapping to support FLUS functionality	16.3.0
2020-03	CT#87e	CP-200200	0108	1	B	PCF selection performed by the SMF	16.3.0
2020-03	CT#87e	CP-200225	0109	1	B	Binding mechanism update for V2X	16.3.0
2020-03	CT#87e	CP-200212	0110	1	B	QoS parameter mapping at PCF update for V2X	16.3.0
2020-03	CT#87e	CP-200225	0111	1	B	QoS parameter mapping at SMF update for V2X	16.3.0
2020-03	CT#87e	CP-200222	0112	1	B	Annex B, IMS Session Establishment	16.3.0
2020-03	CT#87e	CP-200222	0113	1	B	Annex B, IMS Session Modification, provisioning of service information	16.3.0
2020-03	CT#87e	CP-200206	0114	1	B	Annex B, IMS Session Modification, gate control	16.3.0
2020-03	CT#87e	CP-200206	0115	1	B	Annex B, IMS Session Modification, media component removal	16.3.0
2020-03	CT#87e	CP-200206	0116	1	B	Annex B, IMS Session Termination	16.3.0
2020-03	CT#87e	CP-200206	0117	1	B	Annex B, Provisioning of SIP signalling flow information at IMS Registration	16.3.0
2020-03	CT#87e	CP-200206	0118	1	B	Annex B, Subscription to Notification of Change of Access Type	16.3.0
2020-03	CT#87e	CP-200206	0121		B	Annex B, P-CSCF Restoration	16.3.0
2020-03	CT#87e	CP-200207	0122	1	B	DNN Replacement as PCF discovery factor for the AMF	16.3.0
2020-03	CT#87e	CP-200218	0123		B	AF session binding to PDU session for TSN networks	16.3.0
2020-03	CT#87e	CP-200201	0124		B	SRVCC impacts on QoS mapping	16.3.0
2020-03	CT#87e	CP-200219	0125		F	Applying UE Policy Association Modification to all affected UEs	16.3.0
2020-03	CT#87e	CP-200206	0130	1	B	Subscription to Notification of Signalling Path Status at IMS Registration	16.3.0
2020-03	CT#87e	CP-200206	0133	1	B	Subscription to Notification of change of PLMN Identifier at initial IMS Registration	16.3.0
2020-03	CT#87e	CP-200206	0136		B	Annex B, IMS Restricted Local Operator Services	16.3.0
2020-06	CT#88e	CP-201233	0137		B	Clarifiction of PCF selection by the AMF and SMF	16.4.0
2020-06	CT#88e	CP-201268	0138	2	B	Correction on QoS Flow Binding for QoS Flow Behaviour	16.4.0
2020-06	CT#88e	CP-201233	0139		B	Correction to PCC rule Authorization	16.4.0
2020-06	CT#88e	CP-201233	0140	1	B	Correction to binding information procedures	16.4.0
2020-06	CT#88e	CP-201233	0141	3	B	Same PCF selection support	16.4.0
2020-06	CT#88e	CP-201259	0142	3	B	Update of PCF discovery by the AF for eSBA	16.4.0
2020-06	CT#88e	CP-201229	0143	3	B	QoS Flow Binding about ATSSS	16.4.0
2020-06	CT#88e	CP-201252	0144	1	B	Correction to session binding for TSN	16.4.0
2020-06	CT#88e	CP-201232	0146		B	Update for eIMS5G_SBA	16.4.0
2020-06	CT#88e	CP-201234	0147		F	Corrections on Network data analyticis subscribe procedure	16.4.0
2020-06	CT#88e	CP-201212	0148	3	B	Binding information: PCF set ID and PCF instance ID	16.4.0
2020-06	CT#88e	CP-201234	0149	1	F	Removal of not valid BDT policy from UDR	16.4.0
2020-06	CT#88e	CP-201252	0150	1	B	Binding of PCC rules to a QoS flow considering TSCAI information	16.4.0
2020-06	CT#88e	CP-201246	0151		B	Support of applications with specific QoS hints	16.4.0
2020-06	CT#88e	CP-201260	0154	1	F	Correction on QoS Flow Binding for CN PDB	16.4.0
2020-06	CT#88e	CP-201256	0155	1	F	URI correction on Npcf_SMPolicyControl	16.4.0
2020-06	CT#88e	CP-201228	0157	1	B	Framed Routing Support	16.4.0
2020-06	CT#88e	CP-201266	0158	1	B	Support of ATSSS	16.4.0

2020-06	CT#88e	CP-201218	0176	1	A	Correction to PCC call flows	16.4.0
2020-06	CT#88e	CP-201238	0179	1	B	Procedure of N2 PC5 Policy	16.4.0
2020-09	CT#89e	CP-202053	0181		A	Application data change triggers PCF-initiated SM Policy Association Modification	16.5.0
2020-09	CT#89e	CP-202059	0182	1	F	Procedure for IPTV configuration	16.5.0
2020-09	CT#89e	CP-202069	0183	1	F	Procedure of AF-based service parameter provisioning for V2X	16.5.0
2020-09	CT#89e	CP-202209	0184	1	F	GPSI used for PCF selection	16.5.0
2020-09	CT#89e	CP-202081	0185		F	Correction to QoS flow binding	16.5.0
2020-09	CT#89e	CP-202053	0189	1	A	Corrections on AF-initiated PFD management procedure	16.5.0
2020-09	CT#89e	CP-202049	0190	1	F	Correction to PCF discovery and selection	16.5.0
2020-09	CT#89e	CP-202049	0191	1	F	Correction to selection of the same PCF	16.5.0
2020-09	CT#89e	CP-202081	0192		F	Update the call flows to support TSN	16.5.0
2020-09	CT#89e	CP-202079	0186	1	F	Correction to the SM policy association procedure	17.0.0
2020-12	CT#90e	CP-203157	0194	1	A	Usage of PCF Group ID for PCF selection when delegated discovery is used	17.1.0
2020-12	CT#90e	CP-203146	0199		F	Correction to Notification response receiver	17.1.0
2020-12	CT#90e	CP-203148	0200		F	Correction to pending transactions	17.1.0
2020-12	CT#90e	CP-203147	0201	1	F	Correction to SM policy association modification procedure	17.1.0
2020-12	CT#90e	CP-203115	0204		A	Correction to PFD retrieval in PULL mode	17.1.0
2020-12	CT#90e	CP-203135	0205	1	B	Procedure of PUSH notification	17.1.0
2020-12	CT#90e	CP-203115	0208		A	Correction to traffic influence procedures	17.1.0
2020-12	CT#90e	CP-203156	0212	1	A	Correction to Alternative QoS as binding parameter	17.1.0
2020-12	CT#90e	CP-203132	0210		A	Correction to Alternative QoS parameter mapping	17.1.0
2020-12	CT#90e	CP-203150	0214	1	A	Modification of UE Policy related clauses to support URSP rules for 5G VN Group	17.1.0
2021-03	CT#91e	CP-210215	0219	4	B	Procedure of notification push update	17.2.0
2021-03	CT#91e	CP-210215	0220	3	B	Procedure of partial pull	17.2.0
2021-03	CT#91e	CP-210202	0222	1	A	Correction to AM Policy Control for Wireline and Wireless Convergence feature	17.2.0
2021-03	CT#91e	CP-210210	0226	1	A	Correction to N2 PC5 policy provision procedure	17.2.0
2021-03	CT#91e	CP-210193	0228	3	A	QoS monitoring procedure	17.2.0
2021-03	CT#91e	CP-210226	0229	1	F	Clean up TS references	17.2.0
2021-03	CT#91e	CP-210206	0231		A	Alignment of BDT policy re-negotiation	17.2.0
2021-03	CT#91e	CP-210237	0233	1	A	Correction to TSN scenarios.	17.2.0
2021-03	CT#91e	CP-210219	0234	1	F	Removal of resource URI from Notify service operations	17.2.0
2021-03	CT#91e	CP-210196	0239	1	A	Determination of the default QoS flow	17.2.0
2021-03	CT#91e	CP-210229	0242	1	F	Correction to table 7.4.1	17.2.0
2021-03	CT#91e	CP-210196	0245		A	Correction to Notification URI	17.2.0
2021-03	CT#91e	CP-210227	0250	1	F	Correction to Network data analytics Unsubscribe procedure	17.2.0
2021-03	CT#91e	CP-210222	0252		A	PFD change subscription modification procedure	17.2.0
2021-03	CT#91e	CP-210205	0254	1	A	Correction to SamePcf Feature	17.2.0
2021-06	CT#92e	CP-211226	0257	1	B	PCF control of MPS for DTS	17.3.0
2021-06	CT#92e	CP-211201	0258	3	B	5G ProSe related updates to PCC procedures	17.3.0
2021-06	CT#92e	CP-211268	0262	1	A	QoS flow binding for QoS monitoring	17.3.0
2021-06	CT#92e	CP-211259	0263	1	B	Selecting the same PCF for AMF and SMF	17.3.0
2021-06	CT#92e	CP-211221	0264	1	F	Clean up of Network Data Analytics procedures	17.3.0
2021-06	CT#92e	CP-211273	0265	1	B	Support Time Sensitive Communication other than TSN	17.3.0
2021-06	CT#92e	CP-211276	0266	1	B	Support of Network Exposure to EAS via Local NEF	17.3.0
2021-06	CT#92e	CP-211211	0269	1	F	Correction of missing interaction for updating UDR data based on usage report	17.3.0
2021-06	CT#92e	CP-211218	0270	1	B	Updates of PCC procedures related to AF influence on URSP	17.3.0
2021-09	CT#93e	CP-212212	0272	1	B	29.513 MPS for DTS note fix	17.4.0
2021-09	CT#93e	CP-212225	0273	1	B	AM Influence procedure for DCAMP	17.4.0
2021-09	CT#93e	CP-212225	0274	1	B	AM Policy Authorization procedure for DCAMP	17.4.0
2021-09	CT#93e	CP-212225	0275	1	B	AM Policy association procedure updates to support DCAMP	17.4.0
2021-09	CT#93e	CP-212225	0276	1	B	DCAMP impact on PCC architecture	17.4.0
2021-09	CT#93e	CP-212205	0277	-	B	DCAMP impact on PCC architecture	17.4.0
2021-09	CT#93e	CP-212225	0278	1	F	BSF enhancement on PCF Discovery and Selection for DCAMP	17.4.0
2021-09	CT#93e	CP-212206	0279	1	B	Npcf_AMPolicyControl support of UE-Slice-MBR	17.4.0
2021-09	CT#93e	CP-212211	0280	1	F	Correction to abbreviations for TSC	17.4.0
2021-09	CT#93e	CP-212224	0281	-	F	Correction of resource name used in xBDT	17.4.0
2021-09	CT#93e	CP-212193	0284	1	B	5QI value for services carried over satellite access/backhaul	17.4.0
2021-09	CT#93e	CP-212208	0286	1	A	Correction to V2X Policy Provisioning Request	17.4.0
2021-09	CT#93e	CP-212188	0287	1	F	Correction to ProSe Policy Provisioning Request	17.4.0
2021-09	CT#93e	CP-212188	0288	-	B	Architecture updates to support ProSe	17.4.0
2021-09	CT#93e	CP-212188	0289	-	B	BSF support for the PCF notification of PDUID changes	17.4.0
2021-12	CT#94-e	CP-213234	0291	1	B	Updates for TSC networks other than TSN	17.5.0
2021-12	CT#94-e	CP-213229	0292		B	PCC Support of restricted PDU Session for remote provisioning of UE using User Plane	17.5.0
2021-12	CT#94-e	CP-213225	0294	1	B	Handling of Session Management Policy Data per PLMN	17.5.0
2021-12	CT#94-e	CP-213222	0295	1	B	Notification on the outcome of UE Policies delivery due to service specific parameter provisioning	17.5.0

2021-12	CT#94-e	CP-213194	0296	1	F	Updates on DCAMP related BSF services	17.5.0
2021-12	CT#94-e	CP-213227	0297	1	B	NWDAF discovery by the PCF	17.5.0
2021-12	CT#94-e	CP-213237	0298		F	Correction to PFD procedures	17.5.0
2021-12	CT#94-e	CP-213243	0299	1	F	Correction to SM Policy Association Establishment procedure	17.5.0
2021-12	CT#94-e	CP-213194	0300	1	B	Completion of PCF discovery mechanisms	17.5.0
2021-12	CT#94-e	CP-213194	0301	1	B	Alternative mechanism for PCF for a UE discovery	17.5.0
2021-12	CT#94-e	CP-213213	0302		B	Completion of the PCF for a UE registration in the BSF	17.5.0
2021-12	CT#94-e	CP-213230	0293	2	B	Support of monitoring the data rate per Network Slice	17.5.0
2021-12	CT#94-e	CP-213223	0303	1	B	Update the procedure to support AF preference for the user plane latency	17.5.0
2021-12	CT#94-e	CP-213225	0304	1	B	Architectures for interworking with EPS	17.5.0
2021-12	CT#94-e	CP-213200	0305	1	F	Updates on DCAMP related BSF procedures	17.5.0
2021-12	CT#94-e	CP-213200	0306		F	Corrections to DCAMP	17.5.0
2021-12	CT#94-e	CP-213213	0307	1	F	Correction of PCF registration in the BSF at UE policy association creation	17.5.0
2021-12	CT#94-e	CP-213225	0308	1	F	cancel subscription to UDR at SM policy assocaition termination	17.5.0
2021-12	CT#94-e	CP-213244	0309		F	cancel subscription to UDR at UE policy assocaition termination	17.5.0
2021-12	CT#94-e	CP-213244	0312	1	F	Correction to PFD retrieval procedure	17.5.0
2021-12	CT#94-e	CP-213228	0313	2	B	Policy decisions based on Network Analytics	17.5.0
2021-12	CT#94-e	CP-213230	0314	1	B	Same PCF discovery for the control of data rate per network slice	17.5.0
2021-12	CT#94-e	CP-213200	0315	1	B	Management of AM Policies depending on the application in use	17.5.0
2021-12	CT#94-e	CP-213223	0316	1	B	AF Request for Simultaneous Connectivity over Source and Target PSA at Edge Relocation	17.5.0
2022-03	CT#95e	CP-220198	0317	2	B	Resolution of DCAMP open issues such as applicable filters and immediate reporting	17.6.0
2022-03	CT#95e	CP-220197	0318	2	F	Correction to the BSF procedure	17.6.0
2022-03	CT#95e	CP-220197	0319	1	F	PCF for a PDU session discovery by PCF a UE	17.6.0
2022-03	CT#95e	CP-220183	0320	1	B	TSCTSF discovery	17.6.0
2022-03	CT#95e	CP-220196	0322	1	F	Handling of VN Group data during UE Policy Association Termination procedure	17.6.0
2022-03	CT#95e	CP-220187	0323	2	F	Correction on the UE-Slice-MBR sent to PCF	17.6.0
2022-03	CT#95e	CP-220197	0324	2	B	Reporting requested service area coverage change, clarification	17.6.0
2022-03	CT#95e	CP-220182	0325	1	B	Informative guideline for mapping between QoS parameters and DSCP marking	17.6.0
2022-03	CT#95e	CP-220182	0326	1	B	Clarification to PCC Support of restricted PDU Session for remote provisioning of UE using User Plane	17.6.0
2022-03	CT#95e	CP-220186	0327	1	B	Adding service specific authorization in the service parameter provisioning procedure	17.6.0
2022-03	CT#95e	CP-220195	0328	1	F	Collision in SMF during UpdateNotify procedure	17.6.0
2022-03	CT#95e	CP-220186	0329	1	B	Support of AF triggered EAS rediscovery	17.6.0
2022-03	CT#95e	CP-220186	0330	1	B	Support of EAS IP replacement	17.6.0
2022-03	CT#95e	CP-220186	0331	1	B	Support of uplink buffering indication for Application Relocation	17.6.0
2022-03	CT#95e	CP-220202	0332	1	B	QoS Mapping at SMF+PGW-C for interworking scenario	17.6.0
2022-03	CT#95e	CP-220202	0333	1	B	Signalling flows for interworking scenario	17.6.0
2022-03	CT#95e	CP-220195	0335	1	F	Correction to enable retrieval of Network Provided Location information in a MESSAGE request	17.6.0
2022-03	CT#95e	CP-220183	0336	1	B	Deferred invocation of Npcf_PolicyAuthorization_Create service operation	17.6.0
2022-06	CT#96	CP-221116	0337		F	Incorrect step number referenced in UE Policy Association Modification procedures	17.7.0
2022-06	CT#96	CP-221129	0338		F	Correction to PCF subscription on USER_DATA_CONGESTION	17.7.0
2022-06	CT#96	CP-221126	0339		F	Correction of wrong features in the flow procedures for Edge Computing	17.7.0
2022-06	CT#96	CP-221129	0340		F	PCF behaviour for Data Dispersion and WLAN performance	17.7.0
2022-06	CT#96	CP-221129	0341		B	PCF behaviour for Service Experience analytics	17.7.0
2022-06	CT#96	CP-221138	0342	1	F	Completion of User Plane Remote Provisioning	17.7.0
2022-06	CT#96	CP-221159	0343	1	F	Correction to AM Policy Association Modification procedure	17.7.0
2022-06	CT#96	CP-221159	0344	1	F	Correction to AM Policy Association Termination procedure	17.7.0
2022-06	CT#96	CP-221159	0345	1	B	Notification of PDU session establishment or PDU session termination	17.7.0
2022-06	CT#96	CP-221159	0346	1	B	Update of AF requests to influence AM policies procedure	17.7.0
2022-06	CT#96	CP-221159	0347	1	B	Update of binding information subscription procedure	17.7.0
2022-06	CT#96	CP-221159	0348	1	B	Update of PCF for a PDU session discovery and selection by the PCF for a UE	17.7.0
2022-06	CT#96	CP-221145	0350	1	F	Session binding for TSC	17.7.0
2022-06	CT#96	CP-221144	0351		F	Correction to SM policy association establishment	17.7.0
2022-06	CT#96	CP-221145	0352	1	F	Correction to SM policy association modification by the PCF	17.7.0
2022-06	CT#96	CP-221145	0353	1	F	Correction to SM policy association modifiction initiated by the SMF	17.7.0
2022-06	CT#96	CP-221145	0354	1	F	BSF storage information for TSC	17.7.0
2022-06	CT#96	CP-221126	0355	1	F	Correction to the procedure of maximum allowed user plane latency	17.7.0
2022-06	CT#96	CP-221126	0356	1	F	Correction to the SMF behaviour of IP replacement	17.7.0

2022-06	CT#96	CP-221120	0359	1	B	Introduction of 5MBS in PCC architecture	17.7.0
2022-06	CT#96	CP-221120	0360	1	B	Structure to introduce MBS flows	17.7.0
2022-06	CT#96	CP-221120	0361	1	B	PCF Discovery in MBS PCC deployments	17.7.0
2022-06	CT#96	CP-221120	0362	1	B	QoS mapping in MBS PCC deployments	17.7.0
2022-06	CT#96	CP-221120	0363	2	B	Redefining the scope of TS 29.513	17.7.0
2022-06	CT#96	CP-221120	0364	1	B	Specification of PCC MBS Session Creation	17.7.0
2022-06	CT#96	CP-221120	0365	1	B	Specification of PCC MBS Session Modification	17.7.0
2022-06	CT#96	CP-221120	0366	1	B	Specification of PCC MBS Session Termination	17.7.0
2022-06	CT#96	CP-221126	0367		F	Handling of UE Policy delivery notifications	17.7.0
2022-06	CT#96	CP-221157	0368		F	Corrections in AF session procedures	17.7.0
2022-06	CT#96	CP-221157	0369	1	F	VPLMN QoS constraints in QoS mapping procedures	17.7.0
2022-06	CT#96	CP-221126	0370	1	F	Correction to QoS monitoring report	17.7.0
2022-06	CT#96	CP-221141	0371	1	A	Request of V2XP/ProSeP during NAS Transport procedure	17.7.0
2022-06	CT#96	CP-221157	0374		F	PCF selection for V2XP and ProSe	17.7.0
2022-06	CT#96	CP-221145	0375	1	F	Handling of individual alternative QoS	17.7.0
2022-06	CT#96	CP-221145	0376	1	F	Discovery of TSCTSF notification URI	17.7.0
2022-06	CT#96	CP-221159	0377	1	F	Wrong reference allocation	17.7.0
2022-09	CT#97e	CP-222091	0382	1	A	Attribute name correction for QoS monitoring	17.8.0
2022-09	CT#97e	CP-222127	0383	1	F	Correction to SMF-initiated SM Policy Association Modification procedure	17.8.0
2022-09	CT#97e	CP-222099	0384	1	F	User plane latency requirement support	17.8.0
2022-09	CT#97e	CP-222099	0385	1	F	Incorrect attribute names used in QoS monitoring procedure	17.8.0
2022-09	CT#97e	CP-222125	0386	1	F	Correction to ANDSP/URSP rules Determination	17.8.0
2022-09	CT#97e	CP-222123	0388	1	F	PCF selection based on Same PCF indication	17.8.0
2022-09	CT#97e	CP-222099	0390		F	Service parameter data retrieval	17.8.0
2022-12	CT#98e	CP-223166	0396		F	Handling of QoS mapping procedures in PCF and MB-SMF.	17.9.0
2022-12	CT#98e	CP-223166	0397		F	Removal of EN related to the impacts in 5MBS PCC architecture.	17.9.0
2022-12	CT#98e	CP-223166	0398		F	Introduction of MBS Discovery procedures	17.9.0
2022-12	CT#98e	CP-223167	0399	1	F	Completion of MBS Policy Session Modification procedure	17.9.0
2022-12	CT#98e	CP-223166	0403		F	Binding mechanism for MBS	17.9.0
2022-12	CT#98e	CP-223166	0404		F	Resolves the editor’s note in the create service operation	17.9.0
2022-12	CT#98e	CP-223166	0405		F	Resolves the editor’s note in the delete service operation	17.9.0
2022-12	CT#98e	CP-223162	0409		F	Session binding to support 5G ProSe Layer-3 UE-to-Network Relay without N3IWF	17.9.0
2023-03	CT#99	CP-230127	0424	1	F	Removal of V2XP/ProSeP during registration	17.10.0
2023-03	CT#99	CP-230140	0427		F	Correction on the feature support for implicit subscriptions	17.10.0
2023-03	CT#99	CP-230140	0428	1	F	Correction in the handling of QoS monitoring report	17.10.0

History

Document history		
V17.6.0	May 2022	Publication
V17.7.0	June 2022	Publication
V17.8.0	September 2022	Publication
V17.9.0	January 2023	Publication
V17.10.0	April 2023	Publication