**3GPP TSG-CT3 Meeting #127e *C3-231134***

**e-meeting, 17th April 2023 – 21st April 2023**

|  |
| --- |
| *CR-Form-v12.2* |
| **CHANGE REQUEST** |
|  |
|  | **29.513** | **CR** |  **0448** | **rev** | **-** | **Current version:** | **18.1.0** |  |
|  |
| *For* [***HE******LP***](http://www.3gpp.org/3G_Specs/CRs.htm#_blank)*on using this form: comprehensive instructions can be found at* [*http://www.3gpp.org/Change-Requests*](http://www.3gpp.org/Change-Requests)*.* |
|  |

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| ***Proposed change affects:*** | UICC apps |  | ME |  | Radio Access Network |  | Core Network | **X** |

|  |
| --- |
|  |
| ***Title:***  | Update the description with references. |
|  |  |
| ***Source to WG:*** | , Ericsson |
| ***Source to TSG:*** | CT3 |
|  |  |
| ***Work item code:*** | TEI18, 5GS\_Ph1-CT |  | ***Date:*** | 2023-04-07 |
|  |  |  |  |  |
| ***Category:*** | **F** |  | ***Release:*** | Rel-18 |
|  | *Use one of the following categories:****F*** *(correction)****A*** *(mirror corresponding to a change in an earlier release)****B*** *(addition of feature),* ***C*** *(functional modification of feature)****D*** *(editorial modification)*Detailed explanations of the above categories canbe found in 3GPP [TR 21.900](http://www.3gpp.org/ftp/Specs/html-info/21900.htm). | *Use one of the following releases:Rel-8 (Release 8)Rel-9 (Release 9)Rel-10 (Release 10)Rel-11 (Release 11)…Rel-16 (Release 16)Rel-17 (Release 17)Rel-18 (Release 18)Rel-19 (Release 19)* |
|  |  |
| ***Reason for change:*** | TS 21.801 - Specification drafting rules6.6.6      References6.6.6.1          GeneralAs a general rule, references to particular pieces of text shall be used instead of repetition of the original source material, since such repetition involves the risk of error or inconsistency and increases the length of the document. However, if it is considered necessary to repeat such material, its source shall be identified precisely. If it is necessary to reproduce text from a work other than a 3GPP TS or TR, appropriate copyright permission shall be obtained. |
|  |  |
| ***Summary of change:*** | cl 5.2.1, 5.2.2.2.2.1, 5.5.3.2, 5.5.3.3, 6.3, 8.4.2 are updated by providing the reference to other specifications and removing the repetitive text. |
|  |  |
| ***Consequences if not approved:*** | Non compliant with specification drafting rules. |
|  |  |
| ***Clauses affected:*** | 5.2.1, 5.2.2.2.2.1, 5.5.3.2, 5.5.3.3, 6.3, 8.4.2  |
|  |  |
|  | **Y** | **N** |  |  |
| ***Other specs*** |  | **X** |  Other core specifications  | TS/TR ... CR ...  |
| ***affected:*** |  | **X** |  Test specifications | TS/TR ... CR ...  |
| ***(show related CRs)*** |  | **X** |  O&M Specifications | TS/TR ... CR ...  |
|  |  |
| ***Other comments:*** |  |
|  |  |
| ***This CR's revision history:*** |  |

\* \* \* \* First change \* \* \* \*

### 5.2.1 SM Policy Association Establishment

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



Figure 5.2.1-1: SM Policy Association Establishment procedure

This procedure concerns both roaming and non-roaming scenarios.

In the 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 needed information within the "SmPolicyContextData" as defined in clause 4.2.2 of 3GPP TS 29.512 [9].

2-3. If "PvsSupport" feature defined in 3GPP TS 29.512 [9] is supported and the Onboarding Indication set to true is received and the combination of the received DNN and S-NSSAI corresponds to a PDU session used for User Plane Remote Provisioning, 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 or the "ExtendedSamePcf" feature is not supported and the "SamePcf" 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 when the conditions as specified in 3GPP TS 29.512 [9], clause 4.2.2.2 are met.

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.

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.

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.

\* \* \* \* Next change \* \* \* \*

###### 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 as defined in 3GPP TS 29.514 [10] by sending the HTTP POST request to the "Application Sessions" resource.

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.

\* \* \* \* Next change \* \* \* \*

#### 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 as defined in 3GPP TS 29.514 [10] 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\_TrafficInfluence\_Update request in step 1a, the NEF invokes the Npcf\_PolicyAuthorization\_Update service operation as defined in 3GPP TS 29.514 [10] 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\_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 as defined in 3GPP TS 29.514 [10] by sending the HTTP POST request to the "Application Sessions" resource as described in clause 5.2.2.2.2.1.

 To update an existing AF request, the AF invokes the Npcf\_PolicyAuthorization\_Update service operation as defined in 3GPP TS 29.514 [10] by sending the HTTP PATCH request to the "Individual Application Session Context" resource as described in clause 5.2.2.2.2.2.

 To remove an existing AF request, the AF invokes the Npcf\_PolicyAuthorization\_Delete service operation by sending the HTTP POST request to the "Individual Application Session Context" resource as described in clause 5.2.2.2.2.3.

2-3. Upon receipt of the AF request, the PCF invokes the Npcf\_SMPolicyControl\_UpdateNotify service operation as defined in 3GPP TS 29.512 [9] 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.

- 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.

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;

vii. using the FQDN range within the PCC rule if available to match the FQDN received from the EASDF via the Neasdf\_DNSContext\_Notify request and, if matched, indicating the UE the common EAS address(s) within the PCC rule; 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].

 If the "SFC" feature is supported and if the SMF received service function chaining control information in the PCC rule, the SMF takes the proper actions to control the traffic steering towards the N6-LAN as defined in clause 5.4.8 of 3GPP TS 29.244[59].

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 as defined in 3GPP TS 29.522 [24].

 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 as defined in 3GPP TS 29.508 [8] 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.

\* \* \* \* Next change \* \* \* \*

#### 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 as defined in clause 4.4.7 of 3GPP TS 29.522 [24] to the NEF by sending the HTTP POST request to the "Traffic Influence Subscription" resource.

 To update an existing AF request, the AF invokes the Nnef\_TrafficInfluence\_Update service operation defined in clause 4.4.7 of 3GPP TS 29.522 [24] by sending the HTTP PUT or PATCH request to the "Individual Traffic Influence Subscription" resource.

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

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 defined in 3GPP TS 29.519 [12] to store the AF request information in the UDR by sending the HTTP PUT request to the "Individual Influence Data" resource, and the UDR sends a "201 Created" response.

 When receiving the Nnef\_TrafficInfluence\_Update request, the NEF invokes the Nudr\_DataRepository\_Update service operation as defined in 3GPP TS 29.519 [12] to modify the AF request information in the UDR by sending the HTTP PATCH/PUT request to the resource "Individual Influence Data", and the UDR sends a "200 OK" or "204 No Content" response accordingly.

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

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 as specified in in clause 4.2.6.2.6.2 of 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.

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.

\* \* \* \* Next change \* \* \* \*

## 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 shall assign an appropriate 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. Additional information may be needed in the PCC rule based on feature support and available information as described in 3GPP TS 29.512 [9].

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.

\* \* \* \* Next change \* \* \* \*

### 8.4.2 Binding Support Function (BSF)

The BSF has the following characteristics:

a) The BSF stores internally information about the corresponding selected PCF as defined in 3GPP TS 29.521 [22].

- 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.

- If the PCFdetermines whether the same PCF shall be selected for the SM Policy associations as described in 3GPP TS 29.512 [9],the PCF registers in the BSF including the available parameter combination . The BSF applies the procedures to identify if there is a PCF handling the binding information and accepts or rejects the request accordingly(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].

\* \* \* \* End of changes \* \* \* \*