**3GPP TSG-CT3 Meeting #112e C3-205038\_r4**

**E-Meeting, 04th – 13th November 2020**

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| *CR-Form-v12.1* | | | | | | | | |
| **CHANGE REQUEST** | | | | | | | | |
|  | | | | | | | | |
|  | **29.513** | **CR** | **0194** | **rev** | **1** | **Current version:** | **17.0.0** |  |
|  | | | | | | | | |
| *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:*** | Usage of PCF Group ID for PCF selection when delegated discovery is used | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Source to WG:*** | Huawei, Ericsson | | | | | | | | | |
| ***Source to TSG:*** | CT3 | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Work item code:*** | 5G\_eSBA | | | | |  | ***Date:*** | | | 2020-10-?? |
|  |  | | | |  | |  | | |  |
| ***Category:*** | **A** |  | | | | | ***Release:*** | | | Rel-17 |
|  | *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 can be 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-15 (Release 15) Rel-16 (Release 16) Rel-17 (Release 17) Rel-18 (Release 18)* | |
|  |  | | | | | | | | | |
| ***Reason for change:*** | | In case delegated discovery and selection is used for AMF/SMF interactions with the PCF, there is a need to clarify the usage of the PCF Group ID vs the PCF set ID and the PCF instance ID, as per S2-2008233.  In addition, the following issues need to be corrected:   * Clause 5.1.1 (Step 1) refers to a clause 5.1.2.1.1 of 3GPP TS 29.507 that does not exist. * Clause 5.2.2.2.1 also contains a wrong reference to clause 4.2.4 of TS 29.512, whereas it should be clause 4.2.3. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Summary of change:*** | | * Clarify the usage of the PCF group ID in the process of PCF selection, as per S2-2008233. * Additional related editorial corrections. * Replace the wrong reference in clause 5.1.1 to the inexistent clause 5.1.2.1.1 with references to clauses 4.2.2 and 5.3.2.3.1. * Correct the wrong reference in clause 5.2.2.2.1. * Additional editorial corrections. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Consequences if not approved:*** | | Current text is not correct and can create confusions to readers. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Clauses affected:*** | | 4, 5.1.1, 5.1.3.1, 5.1.3.2, 5.2.2.2.1, 8.2, 8.3 | | | | | | | | |
|  | |  | | | | | | | | |
|  | | **Y** | **N** |  | | | |  | | |
| ***Other specs*** | | **X** |  | Other core specifications | | | | TS/TR 23.501 CR 2483 | | |
| ***affected:*** | |  |  | Test specifications | | | | TS/TR ... CR ... | | |
| ***(show related CRs)*** | |  |  | O&M Specifications | | | | TS/TR ... CR ... | | |
|  | |  | | | | | | | | |
| ***Other comments:*** | |  | | | | | | | | |
|  | |  | | | | | | | | |
| ***This CR's revision history:*** | | Rev 1:   * Improve the clarity of introduced text and correct some editorial errors. * Add the changes proposed in C3-205069 (#0195) that is merged into this CR. | | | | | | | | |

\* \* \* Start of changes \* \* \* \*

# 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 Charing Function (CHF), the Unified Data Repository (UDR) and the Application Function (AF). For the roaming scenario, the Security Edge Protection Proxy (SEPP) is deployed between the V-PCF and H-PCF. 3GPP TS 23.503 [4] specifies the 5G policy framework stage 2 functionality.



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



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

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

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].

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

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



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



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

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

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

NOTE 5: For the sake of clarity, SEPPs are not depicted in the roaming reference point architecture figures.

NOTE 6: N4 and N32 are not service based interfaces.



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



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

NOTE 7: For the sake of clarity, SEPPs are not depicted in the roaming reference point architecture figures.

NOTE 8: N4 and N32 are not service based interfaces.

NOTE 9: 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.

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

\* \* \* Next changes \* \* \* \*

5.1.1 AM Policy Association Establishment

This procedure concerns the following scenarios:

1. UE initial registration with the network.

2. The AMF re-allocation with PCF change in handover procedure and registration procedure.

3. UE registers with 5GS during the UE moving from EPS to 5GS when there is no existing AM Policy Association.

****

**Figure 5.1.1-1: AM Policy Association Establishment procedure**

This procedure concerns both roaming and non-roaming scenarios.

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

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

1. The AMF receives the registration request from the AN. Based on local policy, the AMF selects to contact the (V-) PCF to create the policy association with the (V-) PCF and to retrieve Access and Mobility control policy. The AMF selects the PCF as described in subclause 8.2 and invokes the Npcf\_AMPolicyControl\_Create service operation by sending the HTTP POST request to the "AM Policy Associations" resource as defined in subclause 4.2.2 and subclause 5.3.2.3.1 of 3GPP TS 29.507 [7]. The request operation provides the SUPI and the allowed NSSAI if applicable, and if received from the UDM, the Service Area Restrictions, RFSP index, GPSI and a list of Internal Group Identifiers, and may provide the access type, the PEI if received in the AMF, the User Location Information if available, the UE Time Zone if available, Serving Network, RAT type, GUAMI of AMF, alternative or backup address(es) of AMF and trace control and configuration parameters information. The request includes a Notification URI to indicate to the PCF where to send a notification when the policy is updated.

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

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

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

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

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

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

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

- Policy Control Request Triggers and related policy information;

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

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.

\* \* \* Next changes \* \* \* \*

#### 5.1.3.1 AM Policy Association Termination initiated by the AMF

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

****

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

This procedure concerns both roaming and non-roaming scenarios.

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

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

1. The AMF invokes the Npcf\_AMPolicyControl\_Delete service operation to delete the policy context in the (V-) PCF by sending the HTTP DELETE request to the "Individual AM Policy Association" resource.

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

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

4. The PCF invokes the Nudr\_DataRepository\_Unsubscribe service operation to unsubscribe the notification of subscriber policy data modification from the UDR by sending the HTTP DELETE request to the "IndividualPolicyDataSubscription" resource if it has subscribed such notification.

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

\* \* \* Next changes \* \* \* \*

5.1.3.2 AM Policy Association Termination initiated by the PCF

This procedure is performed when the UDR notifies the PCF that the policy profile is removed or when the PCF decides to terminate the AM Policy Association based on the internal logic, e.g. UE movement triggers a geo-fencing rule.

****

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

This procedure concerns both roaming and non-roaming scenarios.

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

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

1. The subscriber policy control data is removed from the UDR.

2. The UDR invokes the Nudr\_DataRepository\_Notify service operation to notify the PCF that the policy profile is removed if PCF has subscribed such notification by sending the HTTP POST request to the resource URI "{notificationUri}" as specified in 3GPP TS 29.519 [12].

3. The PCF sends the response to the Nudr\_DataRepository\_Notify service operation.

4. The (V-)PCF decides to terminate the AM Policy Association based on step 2 or an internal trigger, e.g. operator policy is changed, to re-evaluate Access and Mobility control policy for a UE.

5. The (V-)PCF may, depending on operator policies, 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 subclause 4.2.4.3 of 3GPP TS 29.507 [7].

Alternatively, the (V-)PCF may decide to maintain the Policy Association if a default profile is applied, and then step 4 through 6 are not executed.

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

7. Step 1 through step 3 as specified in Figure 5.1.3.1-1 are executed with the following difference:

- the AMF removes the policy control request trigger(s) related to the AM policy association, but still keeps the provisioned AM policies and applies them to the UE.

\* \* \* Next changes \* \* \* \*

5.2.2.2.1 Interactions between SMF, PCF and CHF

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

****

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

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

- The UDR notifies the PCF about a policy subscription change (e.g. change in MPS EPS Priority, MPS Priority Level, 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 subclause 5.3.5.

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

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

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

If the feature "TimeSensitiveNetworking" is supported and the PCF receives the TSCAI input information and QoS related data or a BMIC and/or one or more PMIC(s) from the AF, the PCF provisions them to the SMF.

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

\* \* \* Next changes \* \* \* \*

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], subclause 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 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).

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], subclause 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 subclause. 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.

\* \* \* Next changes \* \* \* \*

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], subclause 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.

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 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], subclause 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.

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