**3GPP TSG-CT3 Meeting #112e C3-205042\_r1**

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

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| *CR-Form-v12.1* | | | | | | | | |
| **CHANGE REQUEST** | | | | | | | | |
|  | | | | | | | | |
|  | **29.507** | **CR** | **0136** | **rev** | **1** | **Current version:** | **16.5.0** |  |
|  | | | | | | | | |
| *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:*** | Essential corrections and alignments | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Source to WG:*** | Huawei | | | | | | | | | |
| ***Source to TSG:*** | CT3 | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Work item code:*** | SBIProtoc16 | | | | |  | ***Date:*** | | | 2020-10-?? |
|  |  | | | |  | |  | | |  |
| ***Category:*** | **F** |  | | | | | ***Release:*** | | | Rel-16 |
|  | *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:*** | | The following corrections and alignments are necessary:   * The "Resource URI" column of Table 5.3.1-1 should contain a "<relative URI below root>" instead of a full resource URI, as per the API TS skeleton provided in TS 29.501. Same for the "Custom operation URI" column of Table 5.3.3.4.1-1. * The "Notifications overview" table needs to be updated to align with the SBI TS skeleton provided in TS 29.501. * The procedure used by the AMF to retrieve the "Service Area Restrictions, RFSP index, subscribed UE-AMBR and GPSI(s) from the UDM" in 5GC is rather the Access and Mobility Subscription Data retreival procedure, as per clause 5.2.2.2.3 of TS 29.503. In clause 4.2.2.1, it is wrongly referred to as the "update location" procedure. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Summary of change:*** | | * Update the "Resource URI" column of Table 5.3.1-1 by replacing the full resource URI with the associated "<relative URI below root>", i.e. by removing the part "{apiRoot}/<apiName>/<apiVersion>". Similar update for the "Custom operation URI" column of Table 5.3.3.4.1-1. * Update the "Notifications overview" table to align with the SBI TS skeleton provided in TS 29.501. * Correct clause 4.2.2.1 with the right procedure, i.e. Access and Mobility Subscription Data retreival procedure, used to retrieve the "Service Area Restrictions, RFSP index, subscribed UE-AMBR and GPSI(s)" information from the UDM. * Some additional editorial corrections to improve the text. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Consequences if not approved:*** | | Necessary corrections are not applied. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Clauses affected:*** | | 4.2.1, 4.2.2.1, 4.2.3.1, 4.2.4.2, 4.2.4.3, 5.3.1, 5.3.3.4.1, 5.3.3.4.2.1, 5.5.1, 5.6.3.3 | | | | | | | | |
|  | |  | | | | | | | | |
|  | | **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 does not impact OpenAPI specification files. | | | | | | | | |
|  | |  | | | | | | | | |
| ***This CR's revision history:*** | | Rev 1:   * Revert the changes on "subclause" (to "clause") to keep the existing wording. * Revert some changes (use "PCF", not "it") in clauses 4.2.4.2 and 4.2.4.3. * Remove "shall" from the second bullet of clause 4.2.4.3 * Update the changes to the resource URIs in clause 5.3.3.4.1 and clause 5.3.1 by removing the solidus. | | | | | | | | |

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

4.2.1 Introduction

**Table 4.2.1-1: Operations of the Npcf\_AMPolicyControl Service**

| **Service operation name** | **Description** | **Initiated by** |
| --- | --- | --- |
| Npcf\_AMPolicyControl\_Create | Creates an AM Policy Association and provides corresponding policies to the NF consumer. | NF consumer (AMF) |
| Npcf\_AMPolicyControl\_Update | Updates an AM Policy Association and provides corresponding policies to the NF consumer when a policy control request trigger is met or the AMF is relocated due to UE mobility and the old PCF is selected. | NF consumer (AMF) |
| Npcf\_AMPolicyControl\_UpdateNotify | Provides updated policies to the NF consumer. | PCF (V-PCF in roaming case) |
| Npcf\_AMPolicyControl\_Delete | Provides means for the NF consumer to delete the AM Policy Association. | NF consumer (AMF) |

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

4.2.2.1 General

The procedure in the present subclause is applicable when the NF service consumer creates an AM policy association when the UE registers to the network, and when the AMF is relocated (between the different AMF sets) and the new AMF selects a new PCF. The procedure for the case where the AMF is relocated and the new AMF selects the old PCF is defined in subclause 4.2.3.1.

The creation of an AM policy association only applies for normally registered UEs, i.e., it does not apply for Emergency Registered UEs.

Figure 4.2.2.1-1 illustrates the creation of a policy association.



**Figure 4.2.2.1-1: Creation of a policy association**

When a UE registers and a UE context is being established, the AMF can obtain Service Area Restrictions, RFSP index, subscribed UE-AMBR and GPSI(s) from the UDM during the Access and Mobility Subscription Data retrieval procedure and the allowed NSSAI from local configuration or from the NSSF during the slice selection procedure and shall decide based on local policies whether to request policies from the PCF.

To request policies from the PCF, the NF service consumer (e.g. AMF) shall send an HTTP POST request with: "{apiRoot}/npcf-am-policy-control/v1/policies" as Resource URI and the PolicyAssociationRequest data structure as request body that shall include:

- Notification URI encoded as "notificationUri" attribute;

- SUPI encoded as "supi" attribute; and

- if the feature "SliceSupport" or the feature "DNNReplacementControl" is supported in the AMF and the UE is registered via a 3GPP access, the allowed NSSAI in the 3GPP access encoded in the "allowedSnssais" attribute;

and that shall include when available:

- GPSI encoded as "gpsi" attribute;

- if the feature "MultipleAccessTypes" is not supported, the access type encoded as "accessType" attribute;

- Permanent Equipment Identifier (PEI) encoded as "pei" attribute;

- User Location Information encoded as "userLoc" attribute;

- UE Time Zone encoded as "timeZone" attribute;

- Serving PLMN Identifier and for SNPN the NID encoded as "servingPlmn" attribute;

- if the feature "MultipleAccessTypes" is not supported, the RAT type encoded as "ratType" attribute;

- Service Area Restrictions (see subclause 4.2.2.3.1) derived from the Service Area Restrictions obtained from the UDM by mapping any service areas denoted by geographical information into Tracking Area Identities (TAIs) and encoded as "servAreaRes" attribute;

- RFSP index (see subclause 4.2.2.3.2) as obtained from the UDM encoded as "rfsp" attribute;

- A list of Internal Group Identifiers encoded as "groupIds" attribute;

- if the NF service consumer is an AMF, the GUAMI encoded as "guami" attribute;

- if the NF service consumer is an AMF, the name of a service produced by the AMF that expects to receive information within Npcf\_AMPolicyControl\_UpdateNotify service operation encoded as "serviceName" attribute;

- Alternate or backup IPv4 Address(es) where to send Notifications encoded as "altNotifIpv4Addrs" attribute;

- Alternate or backup IPv6 Address(es) where to send Notifications encoded as "altNotifIpv6Addrs" attribute;

- Alternate or backup FQDN(s) where to send Notifications encoded as "altNotifFqdns" attribute;

- trace control and configuration parameters information encoded as "traceReq" attribute;

- if the feature "UE-AMBR\_Authorization" is supported in the AMF, the subscribed UE-AMBR (see subclause 4.2.2.3.3) in the "ueAmbr" attribute; and

- if the feature"DNNReplacementControl" is supported, the mapping of each S-NSSAI of the Allowed NSSAI to the corresponding S-NSSAI of the HPLMN encoded in the "mappingSnssais" attribute.

Upon the reception of this HTTP POST request, the PCF shall:

- assign a policy association ID;

- determine the applicable policy (taking into consideration and optionally modifying the possibly received UE-AMBR, Service Area Restrictions and/or RFSP index);

- for the successful case, send a HTTP "201 Created" response with the URI for the created resource in the "Location" header field

NOTE: The assigned policy association ID is part of the URI for the created resource and is thus associated with the SUPI.

and the PolicyAssociation data type as response body including:

- conditionally AMF Access and Mobility Policy (see subclause 4.2.2.3), i.e.:

a) if the PCF received the "servAreaRes" attribute in the request, Service Area Restrictions encoded as "servAreaRes" attribute; and/or

b) if the PCF received the "rfsp" attribute in the request, RAT Frequency Selection Priority (RFSP) Index encoded as "rfsp" attribute; and/or

c) if the feature "UE-AMBR\_Authorization" is supported and the PCF received the "ueAmbr" attribute in the request, the authorized UE-AMBR encoded as "ueAmbr" attribute;

- optionally one or several of the following Policy Control Request Trigger(s) encoded as "triggers" attribute (see subclause 4.2.3.2):

a) Location change (tracking area); and

b) Change of UE presence in PRA; and

c) if the "SliceSupport" feature or the "DNNReplacementControl" feature is supported, change of allowed NSSAI; and

d) if the "DNNReplacementControl" feature is supported, change of SMF selection information; and

- if the Policy Control Request Trigger "Change of UE presence in PRA" is provided, the presence reporting areas for which reporting is required encoded as "pras" attribute;

- if the Policy Control Request Trigger "Change of SMF selection information" is provided, the SMF selection information representing the conditions upon which the AMF shall request a DNN replacement (see subclause 4.2.2.3.4) encoded as "smfSelInfo" attribute;

- if errors occur when processing the HTTP POST request, apply error handling procedures as specified in subclause 5.7 and according to the following provisions:

- if the user information received within the "supi" attribute is unknown, the PCF shall reject the request and include in an HTTP "400 Bad Request" response message the "cause" attribute of the ProblemDetails data structure set to "USER\_UNKNOWN";

- if the PCF is, due to incomplete, erroneous or missing information in the request, not able to provision an AM policy decision, the PCF may reject the request and include in an HTTP "400 Bad Request" response message the "cause" attribute of the ProblemDetails data structure set to "ERROR\_REQUEST\_PARAMETERS".

- if the PCF rejects the AM policy association establishment, the NF service consumer shall apply the policy retrieved from the UDM if available; otherwise, the NF service consumer shall apply the operator configured policy.

If the PCF received a GUAMI, the PCF may subscribe to GUAMI changes using the AMFStatusChange service operation of the Namf\_Communication service specified in 3GPP TS 29.518 [14], and it may use the Nnrf\_NFDiscovery Service specified in 3GPP TS 29.510 [13] (using the obtained GUAMI and possibly service name) to query the other AMFs within the AMF set.

If the PCF received a "traceReq" attribute, it shall perform trace procedures as defined in 3GPP TS 32.422 [18].

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

4.2.3.1 General

The procedure in the present subclause is applicable when the NF service consumer modifies an existing AM policy association (including the case where the AMF is relocated and the new AMF selects the old PCF to maintain the policy association and to update the Notification URI).

Figure 4.2.3.1-1 illustrates the update of a policy association.

****

**Figure 4.2.3.1-1: Update of a policy association**

The AMF as NF service consumer invokes this procedure when a policy control request trigger (see subclause 4.2.3.2) occurs. When the Service Area restriction change trigger and/or the RFSP index change trigger occur, and/or the feature "UE-AMBR\_Authorization" is supported and the subscribed UE-AMBR change trigger occurs, the AMF shall always invoke the procedure. When the location change trigger or the change of UE presence in PRA trigger occurs, the AMF shall only invoke the procedure if the PCF has subscribed to that event trigger.

If an AMF knows by implementation specific means that the UE context has been transferred to an AMF with another GUAMI within the AMF set, it may also invoke this procedure to update the Notification URI and the GUAMI.

NOTE 1: Either the old or the new AMF can invoke this procedure.

During the AMF relocation, if the new AMF received the resource URI of the individual AM Policy from the old AMF and selects the old PCF, the new AMF shall also invoke this procedure to update the Notification URI and the GUAMI. The new AMF may also update the alternate or backup IP addresses.

To request policies from the PCF, to update the Notification URI, to update the trace control configuration and/or to request the termination of trace, the NF Service Consumer (e.g. AMF) shall request the update of the AM Policy Association by providing the relevant parameters about the UE context by sending an HTTP POST request with "{apiRoot}/npcf-am-policy-control/v1/policies/{polAssoId}/update" as Resource URI and the PolicyAssociationUpdateRequest data structure as request body that shall include:

- at least one of the following:

1. a new Notification URI encoded in the "notificationUri" attribute;

2. observed Policy Control Request Trigger(s) (see subclause 4.2.3.2) encoded as "triggers" attribute;

3. if a Service Area restriction change occurred, the Service Area Restrictions (see subclause 4.2.2.3.1) as obtained from the UDM encoded as "servAreaRes" attribute;

4. if a RFSP index change occurred, the RFSP index (see subclause 4.2.2.3.2) as obtained from the UDM encoded as "rfsp" attribute;

5. if a UE location change occurred, the UE location encoded as "userLoc" attribute;

6. if the Policy Control Request Trigger "Change of UE presence in PRA" is provided, the current presence status of the UE for the presence reporting areas for which reporting was requested, if not previously provided, or the presence reporting areas for which reporting was requested and the status has changed encoded as "praStatuses" attribute.

7. if the trace control configuration needs to be updated, trace control and configuration parameters information encoded as "traceReq" attribute;

8. if trace needs to be terminated, the "traceReq" attribute set to the Null value;

9. if the "SliceSupport" feature or the "DNNReplacementControl" feature is supported, the UE is registered via 3GPP access, the allowed NSSAI changed, and the Policy Control Request Trigger "Change of allowed NSSAI" was provided, then the allowed NSSAI encoded in the "allowedSnssais" attribute;

10. for AMF relocation scenarios, if available, alternate or backup IPv4 Address(es) where to send Notifications encoded as "altNotifIpv4Addrs" attribute;

11. for AMF relocation scenarios, if available, alternate or backup IPv6 Address(es) where to send Notifications encoded as "altNotifIpv6Addrs" attribute;

12. for AMF relocation scenarios, if available, alternate or backup FQDN(s) where to send Notifications encoded as "altNotifFqdns" attribute;

13. for AMF relocation scenarios, if available, the GUAMI encoded as "guami" attribute;

NOTE 2: An alternate NF service consumer than the one that requested the generation of the subscription resource can send the request. For instance, an AMF as service consumer can change.

14. if the feature "UE-AMBR\_Authorization" is supported, and a subscribed UE-AMBR change occurred, the UE-AMBR (see subclause 4.2.2.3.x) as obtained from the UDM encoded as "ueAmbr" attribute;

15. if the feature "DNNReplacementControl" is supported, DNN replacement applies and the Policy Control Request Trigger "Change of SMF selection information" is provided, the "smfSelInfo" attribute including:

- the UE requested DNN in the "dnn" attribute; and

- the UE requested S-NSSAI in the "snssai" attribute and, if available, the corresponding mapped home S-NSSAI in the "mappingSnssai" attribute;

when:

- the UE requested an unsupported DNN and the "unsuppDnn" attribute is set to "true"; or

- the UE requested DNN and S-NSSAI matched one of the S-NSSAI and DNN provided in the "candidates" attribute; and

16. if feature "DNNReplacementControl" is supported, the UE is registered via 3GPP access, the Allowed NSSAI changed and/or the mapping of a S-NSSAI of the Allowed NSSAI to the corresponding S-NSSAI of the HPLMN changed, and the Policy Control Request Trigger" Change of allowed NSSAI" was provided, then the mapping of each S-NSSAI of the Allowed NSSAI to the corresponding S-NSSAI of the HPLMN encoded in the "mappingSnssais" attribute.

NOTE 3: When the feature "DNNReplacementControl" is supported, the AMF applies DNN replacement for non-roaming scenarios and LBO. For a PDU session with home routed roaming, whether to perform DNN replacement is based on operator agreement.

Upon the reception of the HTTP POST request, the PCF shall:

- update the corresponding individual AM Policy resource based on the information provided by the AMF;

- determine the applicable policy based on local policy;

- for the succesfull case, send a HTTP "200 OK" response with the PolicyUpdate data type as body with possible updates for that applicable policy and Policy Control Request Trigger(s) encoded as described in subclause 4.2.3.3 and according to the following provisions:

a) if the PCF received the "servAreaRes" attribute in the request, Service Area Restrictions encoded as "servAreaRes" attribute;

b) if the PCF received the "rfsp" attribute in the request, RAT Frequency Selection Priority (RFSP) Index encoded as "rfsp" attribute;

c) if the feature "UE-AMBR\_Authorization" is supported and the PCF received the "ueAmbr" attribute in the request, UE-AMBR encoded as "ueAmbr" attribute; and/or

d) if the PCF received the "smfSelInfo" attribute in the request, the "smfSelInfo" attribute encoding the PCF selected DNN in the "dnn" attribute corresponding to the S-NSSAI received in the "snssai" attribute;

NOTE 4: A PolicyUpdate data structure with only mandatory attribute(s) is included in the "200 OK" response when the PCF decides not to update the policies.

- if errors occur when processing the HTTP POST request, apply error handling procedures as specified in subclause 5.7 and according to the following provisions:

- if the PCF is, due to incomplete, erroneous or missing information in the request, not able to provision an AM policy decision, the PCF may reject the request and include in an HTTP "400 Bad Request" response message the "cause" attribute of the ProblemDetails data structure set to "ERROR\_REQUEST\_PARAMETERS".

If the PCF received a "traceReq" attribute, it shall perform trace procedures as defined in 3GPP TS 32.422 [18].

If the AMF received the request of removal of Service Area Restrictions and/or RFSP and/or UE-AMBR from the UDM, the AMF shall remove the authorized Service Area Restrictions and/or RFSP and/or UE-AMBR provisioned by the PCF and apply the configured Service Area Restrictions and/or RFSP and/or UE-AMBR at the AMF without interacting with the PCF.

If feature "DNNReplacementControl" is supported and the AMF received the update of the SMF selection information within the "smfSelInfo" attribute in the response, the AMF shall apply the updated SMF selection information to the new PDU Sessions only, i.e. already established PDU Sessions are not affected.

If the PCF received a new GUAMI, the PCF may subscribe to GUAMI changes using the AMFStatusChange service operation of the Namf\_Communication service specified in 3GPP TS 29.518 [14], and it may use the Nnrf\_NFDiscovery Service specified in 3GPP TS 29.510 [13] (using the obtained GUAMI and possibly service name) to query the other AMFs within the AMF set.

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

#### 4.2.4.2 Policy update notification

Figure 4.2.4.2-1 illustrates the policy update notification.



Figure 4.2.4.2-1: policy update notification

The PCF may decide to update Access and Mobility policies and shall then send an HTTP POST request with "{notificationUri}/update" as URI (where the Notification URI was previously supplied by the NF service consumer) and the PolicyUpdate data structure as request body encoded as described in subclause 4.2.3.3.

Upon the reception of the HTTP POST request, the NF service consumer shall:

- enforce the received updated policy;

- either send a HTTP "204 No Content" response indicating the success of the enforcement or an appropriate failure response; and

- if errors occur when processing the HTTP POST request, apply error handling procedures as specified in subclause 5.7.

If the AMF as NF service consumer is not able to handle the notification but knows by implementation specific means that another AMF is able to handle the notification, it shall reply with an HTTP "307 temporary redirect" error response pointing to the URI of the new AMF. If the AMF is not able to handle the notification but another unknown AMF could possibly handle the notification, it shall reply with an HTTP "404 Not found" error response.

If the PCF receives a "307 temporary redirect" response, the PCF shall resend the failed policy update notification request using the received URI in the Location header field as Notification URI. Subsequent policy update notifications, triggered after the failed one, shall be sent to the Notification URI provided by the NF service consumer during the corresponding policy association creation/update.

If the PCF becomes aware that a new AMF is requiring notifications (e.g. via the "404 Not found" response, via Namf\_Communication service AMFStatusChange Notifications, see 3GPP TS 29.518 [14], or via link level failures), and the PCF knows alternate or backup IPv4, IPv6 Addess(es) or FQDN(s) where to send Notifications (e.g. via "altNotifIpv4Addrs", "altNotifIpv6Addrs" or "altNotifFqdns" attributes received when the policy association was created, via AMFStatusChange Notifications or via the Nnrf\_NFDiscovery Service specified in 3GPP TS 29.510 [13] (using the service name and GUAMI obtained during the creation of the subscription) to discover the other AMFs within the AMF set), the PCF shall exchange the authority part of the corresponding Notification URI with one of those addresses and shall use that URI in any subsequent communication.

If the PCF received a "404 Not found" response, the PCF should resend the failed policy update notification request to that URI.

If the feature "DNNReplacementControl" is supported and the AMF received the update of the SMF selection information within the "smfSelInfo" attribute in the request, the AMF shall apply the updated SMF selection information to the new PDU Sessions only, i.e. already established PDU Sessions are not affected.

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

#### 4.2.4.3 Request for termination of the policy association

Figure 4.2.4.3-1 illustrates the request for a termination of the policy association.



Figure 4.2.4.3-1: request for a termination of the policy association

The PCF may request the termination of the policy association and shall then send an HTTP POST request with "{notificationUri}/terminate" as URI (where the Notification URI was previously supplied by the NF service consumer) and the TerminationNotification data structure as request body that shall include:

- the policy association ID encoded as "polAssoId" attribute; and

- the cause why the PCF requests the termination of the policy association encoded as "cause" attribute.

Upon the reception of the HTTP POST request, the NF service consumer shall:

- either send a HTTP "204 No Content" response for the succesfull processing of the HTTP POST request or an appropriate failure response; and

- if errors occur when processing the HTTP POST request, apply error handling procedures as specified in subclause 5.7.

After the succesfull processing of the HTTP POST request, the NF service consumer shall remove the context related to the policy association but still apply the provisioned AM policies to the UE and invoke the Npcf\_AMPolicyControl\_Delete Service Operation defined in subclause 4.2.5 to terminate the policy association.

If the AMF as NF service consumer is not able to handle the notification but knows by implementation specific means that another AMF is able to handle the notification, it shall reply with an HTTP "307 temporary redirect" error response pointing to the URI of the new AMF. If the AMF is not able to handle the notification but another unknown AMF could possibly handle the notification, it shall reply with an HTTP "404 Not found" error response.

If the PCF receives a "307 temporary redirect" response, the PCF shall resend the failed request for termination of the policy association using the received URI in the Location header field as Notification URI.

If the PCF becomes aware that a new AMF is requiring notifications (e.g. via the "404 Not found" response, via Namf\_Communication service AMFStatusChange Notifications, see 3GPP TS TS 29.518 [14], or via link level failures), and the PCF knows alternate or backup IPv4, IPv6 Addess(es) or FQDN(s) where to send Notifications (e.g. via "altNotifIpv4Addrs", "altNotifIpv6Addrs" or "altNotifFqdns" attributes received when the policy association was created, via AMFStatusChange Notifications or via the Nnrf\_NFDiscovery Service specified in 3GPP TS 29.510 [13] (using the service name and GUAMI obtained during the creation of the subscription) to discover the other AMFs within the AMF set), the PCF shall exchange the authority part of the corresponding Notification URI with one of those addresses and shall resend the failed request for termination of the policy association to that URI.

If the PCF received a "404 Not found" response, the PCF should resend the failed request for termination of the policy association to that URI.

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

5.3.1 Resource Structure

****

**Figure 5.3.1-1: Resource URI structure of the Npcf\_AMPolicyControl API**

Table 5.3.1-1 provides an overview of the resources and applicable HTTP methods.

**Table 5.3.1-1: Resources and methods overview**

|  |  |  |  |
| --- | --- | --- | --- |
| **Resource name** | **Resource URI** | **HTTP method or custom operation** | **Description** |
| AM Policy Associations | /policies/ | POST | Create a new Individual AM Policy Association resource. |
| Individual AM Policy Association | /policies/{polAssoId} | GET | Read the Individual AM Policy Association resource. |
| DELETE | Delete the Individual AM Policy Association resource. |
| /policies/{polAssoId}/update | update (POST) | Report observed event trigger and obtain updated policies. |

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

##### 5.3.3.4.1 Overview

Table 5.3.3.4.1-1: Custom operations

|  |  |  |  |
| --- | --- | --- | --- |
| Operation Name | Custom operation URI | Mapped HTTP method | Description |
| Update | /policies/{polAssoId}/update | POST | Report observed event trigger and obtain updated policies. |

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

###### 5.3.3.4.2.1 Description

The update custom operation allows an NF service consumer to report the occurrence of a policy control request trigger and to obtain related updated policies.

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

5.5.1 General

**Table 5.5.1-1: Notifications overview**

|  |  |  |  |
| --- | --- | --- | --- |
| **Notification** | **Callback URI** | **HTTP method or custom operation** | **Description (service operation)** |
| Policy Update Notification | {notificationUri}/update | update (POST) | Policy Update Notification. |
| Request for termination of the policy association | {notificationUri}/terminate | terminate(POST) | Request for termination of the policy association. |

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

5.6.3.3 Enumeration: RequestTrigger

The enumeration RequestTrigger represents the possible Policy Control Request Triggers. It shall comply with the provisions defined in table 5.6.3.3-1.

**Table 5.6.3.3-1: Enumeration RequestTrigger**

|  |  |  |
| --- | --- | --- |
| **Enumeration value** | **Description** | **Applicability** |
| LOC\_CH | Location change (tracking area): the tracking area of the UE has changed. |  |
| PRA\_CH | Change of UE presence in PRA: the UE is entering/leaving a Presence Reporting Area. |  |
| SERV\_AREA\_CH | Service Area Restriction change: the UDM notifies the AMF that the subscribed service area restriction information has changed. |  |
| RFSP\_CH | RFSP index change: the UDM notifies the AMF that the subscribed RFSP index has changed. |  |
| ALLOWED\_NSSAI\_CH | Allowed NSSAI change: the AMF notifies that the set of UE allowed S-NSSAIs has changed. | SliceSupport, DNNReplacementControl |
| UE\_AMBR\_CH | UE-AMBR change: the UDM notifies the AMF that the subscribed UE-AMBR has changed. | UE-AMBR\_Authorization |
| SMF\_SELECT\_CH | SMF selection information change: UE request for an unsupported DNN or UE request for a DNN within the list of DNN candidates for replacement per S-NSSAI. | DNNReplacementControl |
| ACCESS\_TYPE\_CH | Access Type change: the AMF notifies that the access type and the RAT type combinations available in the AMF for a UE with simultaneous 3GPP and non-3GPP connectivity have changed. | MultipleAccessTypes |

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