**3GPP TSG-CT WG3 Meeting #137 *C3-245216***

**Hefei, CN, 14 – 18 October, 2024**

|  |
| --- |
| *CR-Form-v12.3* |
| **CHANGE REQUEST** |
|  |
|  | **29.507** | **CR** | **0319** | **rev** | **-** | **Current version:** | **19.0.0** |  |
|  |
| *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:***  | AMF behaviour when the AM Policy Association is deleted or does not exist. |
|  |  |
| ***Source to WG:*** | Ericsson |
| ***Source to TSG:*** | CT3 |
|  |  |
| ***Work item code:*** | TEI19\_MINPA |  | ***Date:*** | 2024-09-22 |
|  |  |  |  |  |
| ***Category:*** | **B** |  | ***Release:*** | Rel-19 |
|  | *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-17 (Release 17)Rel-18 (Release 18)Rel-19 (Release 19)Rel-20 (Release 20)* |
|  |  |
| ***Reason for change:*** | The trigger to initiate the AM policy association can be initiated when the indicator is received set to enabled.The AMF needs to subscribe to changes of the AM policy association indicator to get updated of the changes of the indicator.According to the current specification, one of the reasons why the AM Policy Association is established is when the indicator is set to enabled. However, there are cases where the PCF does not want the AM Policy Association to be created or terminates the existing one. For those cases the AMF should not reattempt the establishment of a new AM Policy Association regardless of the value of the indicator. |
| ***d*** |  |
| ***Summary of change:*** | It is clarified that the indicator is only considered in the existing cases when the AM Policy Association is created plus the change of the indicator from disabled to enabled. The AM Policy Association indicator should not be considered when the PCF terminates the AM Policy Association nor when the PCF rejects its creation. Othewise, a loop situation could be generated. |
|  |  |
| ***Consequences if not approved:*** | Undefined behaviour when the AM Policy Association creation is rejected and when the AM Policy Association is terminated by the PCF. |
|  |  |
| ***Clauses affected:*** | 4.2.2.1; 4.2.4.3. |
|  |  |
|  | **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 have any impact in the Open API specification. |
|  |  |
| ***This CR's revision history:*** |  |

**Additional discussion(if needed):**

**Proposed changes:**

\*\*\* First Change \*\*\*

#### 4.2.2.1 General

The procedure in the present clause is applicable in the following cases:

- when the UE registers to the network;

- 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 performed using the Npcf\_AMPolicyControl\_Update service operation and it is thus defined in clause 4.2.3.1; and

- when the AM Policy Association establishment is controlled by the AM Policy Association Indicator provided by the UDM, when the indicator is set to enabled.

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 may obtain Service Area Restrictions, RFSP index, subscribed UE-AMBR, subscribed UE-Slice-MBR(s) and GPSI(s) from the UDM during the Access and Mobility Subscription Data retrieval procedure, and the list of NWDAF instance IDs used for the UE and their associated Analytic ID(s) consumed by the AMF, the Allowed NSSAI and the Target NSSAI from local configuration or from the NSSF during the slice selection procedure and:

i. if the AMF received from the UDM the AM Policy Association Indicator set to enabled, the AMF shall establish an AM Policy Association with the PCF in case there is no existing AM Policy Association for the UE;

ii. if the AMF received from UDM the AM Policy Association Indicator set to disabled, the AMF shall not establish the AM policy Association with the PCF;

iii. if the AMF does not receive from the UDM the AM Policy Association Indicator, the AMF may decide based on local policies whether to request policies from the PCF.

If the AM Policy Association Indicator changes from disabled to enabled, the AMF shall immediately establish the AM Policy Association in case there is no existing AM Policy Association for the UE. The PCF provides to the AMF all the applicable AM policies.

NOTE 1: The AMF can decide not to initiate the immediate establishment of the AM Policy Association if the AM Policy Association Establishment was previously rejected by the PCF or the PCF previously initiated the termination of the AM Policy Association.

NOTE 2: The indication of whether the AM Policy Association is allowed by UDM subscription is delivered by the UDM to the NF service consumer within the Access and Mobility Subscription Data Retrieval service operation as described in 3GPP TS 29.503 [34]. In roaming, the AMF does not consider the value of the AM Policy Association Indicator, if received.

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;

- if the "SliceSupport" feature, the "DNNReplacementControl" feature and/or the "NetSliceRepl" feature is/are supported in the NF service consumer and the UE is registered via a 3GPP access, the Allowed NSSAI in the 3GPP access within the "allowedSnssais" attribute; and

- if the "PartNetSliceSupport" feature and/or the "NetSliceRepl" feature is/are supported in the NF service consumer and the UE is registered via a 3GPP access, the Partially Allowed NSSAI in the 3GPP access within the "partAllowedNssai" 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;

- the identifier of the serving network (the PLMN Identifier or the SNPN Identifier)encoded as "servingPlmn" attribute;

NOTE 3: The SNPN Identifier consists of the PLMN Identifier and the NID.

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

- Service Area Restrictions (see clause 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 clause 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 NF service consumer, the subscribed UE-AMBR (see clause 4.2.2.3.3) in the "ueAmbr" attribute;

- if the "DNNReplacementControl" feature is supported, the mapping of each S-NSSAI of the Allowed NSSAI, and if the "PartNetSliceSupport" feature is supported, the mapping of each S-NSSAI of the Partially Allowed NSSAI to the corresponding S-NSSAI of the HPLMN within the "mappingSnssais" attribute;

- if the "PartNetSliceSupport" feature is supported in the NF service consumer and the UE is registered via a 3GPP access:

- the list of the S-NSSAI(s) rejected partially in the RA, if available, within the "snssaisPartRejected" attribute;

- the list of the Rejected S-NSSAI(s) in the RA, if available, within the "rejectedSnssais" attribute; and/or

- the Pending NSSAI encoded, if available, within the "pendingNssai" attribute;

- if the feature "UE-Slice-MBR\_Authorization" is supported in the NF service consumer, the subscribed UE-Slice-MBR for each subscribed S-NSSAI of the home PLMN mapping to a S-NSSAI of the serving PLMN if available (see clause 4.2.2.3.5) encoded in the "ueSliceMbrs" attribute;

- when the "EneNA" feature is supported, the list of NWDAF instance IDs used for the UE and their associated Analytic IDs consumed by the NF service consumer, included within the "nwdafDatas" attribute; and

- if the feature "TargetNSSAI" is supported in the NF service consumer, the Target NSSAI generated by the NF service consumer or received from the NSSF encoded in the "targetSnssais" 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, UE-Slice-MBR(s) for the Allowed NSSAI and the Partially Allowed NSSAI, Service Area Restrictions, RFSP index, Allowed NSSAI, Partially Allowed NSSAI, list of the S-NSSAI(s) rejected partially in the RA, list of the Rejected S-NSSAI(s) in the RA and/or Pending NSSAI);

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

NOTE 4: 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 clause 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. If the feature "RFSPValidityTime" is supported and the PCF determines to provide an RFSP index value that indicates EPC/E-UTRAN access is prioritized over 5GS access, the PCF may provide, based on operator policies, a validity time for the RFSP index value within the "rfspValTime" 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;

d) if the feature "UE-Slice-MBR\_Authorization" is supported and the PCF received the "ueSliceMbrs" attribute in the request, the corresponding authorized UE-Slice-MBR(s) encoded as "ueSliceMbrs" attribute;

e) if the feature "AMInfluence" is supported, the PCF for the UE determines that the access and mobility policies may be influenced by the traffic of PDU session(s) and local operator policies indicate that the PCF for the UE shall subscribe with the PCF for the PDU session for established/terminated PDU session(s) event notifications via the AMF and the SMF, the PCF for the UE information within the "pcfUeInfo" attribute, and the DNN and S-NSSAI of the concerned PDU session(s) within the "matchPdus" attribute. The "pcfUeInfo" attribute shall include the PCF for the UE callback URI via which the PCF(s) for the PDU session shall send notifications about the related PDU session(s) established/terminated events within the "callbackUri" attribute, and if available, the associated PCF for the UE instance ID, PCF set ID, and the level of SBA binding within the "bindingInfo" attribute;

f) if the feature "5GAccessStratumTime" is supported and the PCF receives the access stratum time distribution parameters from the TSCTSF as defined in 3GPP TS 29.534 [26], the 5G access stratum time distribution parameters encoded as "asTimeDisParam" attribute as defined in clause 4.2.2.3.6; and/or

g) if the "NetSliceUsageCtrl" feature is supported and the PCF determines that one or more S-NSSAI(s) of the UE's Allowed NSSAI is/are on-demand S-NSSAI(s) and subject to network slice usage control, the network slice usage control information (e.g., slice deregistration inactivity timer) within the "sliceUsgCtrlInfoSets" attribute as specified in clause 4.2.2.3.7;

NOTE 5: In this release of the specification, network slice usage control information provisioning by the PCF is not supported in roaming scenarios.

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

a) Location change (tracking area);

b) Change of UE presence in PRA;

c) if the "SliceSupport" feature, the "DNNReplacementControl" feature and/or the "NetSliceRepl" feature is/are supported, Change of Allowed NSSAI;

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

e) if the "EneNA" feature is supported, change of NWDAF data;

f) if the "TargetNSSAI" feature is supported, Generation of Target NSSAI;

g) if the "NetSliceRepl" feature is supported, S-NSSAI Replacement;

h) if the "PartNetSliceSupport" feature and/or the "NetSliceRepl" feature is/are supported, Change of the Partially Allowed NSSAI;

i) if the "PartNetSliceSupport" feature is supported, Change of the S-NSSAI(s) rejected partially in the RA, Change of the rejected S-NSSAI(s) in the RA and/or Change of the Pending NSSAI;

- 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;

NOTE 6: If the PCF uses a Presence Reporting Area identifier referring to a Set of Core Network predefined Presence Reporting Areas as defined in 3GPP TS 23.501 [2], the PCF includes the identifier of this Presence Reporting Area set within the "praId" 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 clause 4.2.2.3.4) encoded as "smfSelInfo" attribute;

- if the Policy Control Request Trigger "Generation of Target NSSAI" is provided, the RFSP Index associated with the Target NSSAI encoded as "targetRfsp" attribute; and

- if the "SLAMUP" feature is supported, and operator policies indicate the AMF should select same CHF that is selected by the PCF for a UE, the PCF may provide the CHF address and if available, the associated CHF instance ID(s) and/or CHF set ID(s) encoded as "chfInfo" attribute;

and

- if errors occur when processing the HTTP POST request, apply error handling procedures as specified in clause 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"; and

- 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].

If the PCF received the list of NWDAF instance IDs used for the UE and their associated Analytic IDs within the "nwdafDatas" attribute, the PCF may select those NWDAF instances as described in 3GPP TS 29.513 [7].

The PCF may retrieve AF requirements on Access and Mobility policies from the UDR as specified in 3GPP TS 29.519 [17] and consider them for determining the Access and Mobility policies to be provisioned.

\*\*\* Second Change \*\*\*

#### 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 successful processing of the HTTP POST request or an appropriate failure response; and

- if errors occur when processing the HTTP POST request, send an HTTP error response as specified in clause 5.7; or

- if the feature "ES3XX" is supported, and the NF service consumer determines the received HTTP POST request needs to be redirected, send an HTTP redirect response as specified in clause 6.10.9 of 3GPP TS 29.500 [5].

After the successful 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 clause 4.2.5 to terminate the policy association.NOTE: If the PCF requests the termination of an AM policy association and the AM Policy Indicator was provided by the UDM set to enabled, it will not mean that the NF Service Consumer has to initiate a new AM policy association establishment based on this indicator.

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" 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 Address(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.

\*\*\* End of Changes \*\*\*