**3GPP TSG-CT3 Meeting #120-e *C3-221202***

**E-Meeting, 17th – 25th February 2022 (Revision of C3-22xxxx)**

|  |
| --- |
| *CR-Form-v12.1* |
| **CHANGE REQUEST** |
|  |
|  | **29.514** | **CR** | 0387 | **rev** | **-** | **Current version:** | **17.3.0** |  |
|  |
| *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:***  |  Support of AN-GW restoration |
|  |  |
| ***Source to WG:*** | Huawei |
| ***Source to TSG:*** | CT3 |
|  |  |
| ***Work item code:*** | en5GPccSer17 |  | ***Date:*** | 2022-02-25 |
|  |  |  |  |  |
| ***Category:*** | **B** |  | ***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 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-15 (Release 15)Rel-16 (Release 16)Rel-17 (Release 17)Rel-18 (Release 18)* |
|  |  |
| ***Reason for change:*** | When the PDN connection is established via the E-UTRAN/EPC, the S-GW failure may occur. The S-GW restoration support needs to be considered.  |
|  |  |
| ***Summary of change:*** | The PCF informs the AF of the S-GW failure. |
|  |  |
| ***Consequences if not approved:*** | The AF may make wrong decision. |
|  |  |
| ***Clauses affected:*** | 4.2.2.2, 4.2.3.2, 4.2.5.5, 5.7.3 |
|  |  |
|  | **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 the OpenAPI file. |
|  |  |
| ***This CR's revision history:*** |  |

**Additional discussion(if needed):**

**Proposed changes:**

\*\*\* 1st Change \*\*\*

#### 4.2.2.2 Initial provisioning of service information

This procedure is used to set up an AF application session context for the service as defined in 3GPP TS 23.501 [2], 3GPP TS 23.502 [3] and 3GPP TS 23.503 [4].

Figure 4.2.2.2-1 illustrates the initial provisioning of service information.



Figure 4.2.2.2-1: Initial provisioning of service information

When a new AF application session context is being established and media information for this application session context is available at the NF service consumer and the related media requires PCC control, the NF service consumer shall invoke the Npcf\_PolicyAuthorization\_Create service operation by sending the HTTP POST request to the resource URI representing the "Application Sessions" collection resource of the PCF, as shown in figure 4.2.2.2-1, step 1.

The NF service consumer shall include in the "AppSessionContext" data type in the payload body of the HTTP POST request a partial representation of the "Individual Application Session Context" resource by providing the "AppSessionContextReqData" data type. The "Individual Application Session Context" resource and the "Events Subscription" sub-resource are created as described below.

The NF service consumer shall provide in the body of the HTTP POST request:

- for IP type PDU sessions, the IP address (IPv4 or IPv6) of the UE in the "ueIpv4" or "ueIpv6" attribute; and

- for Ethernet type PDU sessions, the MAC address of the UE in the "ueMac" attribute.

For Ethernet type PDU sessions, if the "TimeSensitiveNetworking" or "TimeSensitiveCommunication" feature is supported, the "ueMac" attribute containing the MAC address of the DS-TT port as received from the PCF during the reporting of TSC user plane node information as defined in subclause 4.2.5.16.

NOTE 1: The determination of the DS-TT port MAC address is specified in subclause 5.28.2 of 3GPP TS 23.501 [2]. The DS-TT port MAC address is used as identifier of the PDU session related to the reported TSC user plane node information.

For IP type PDU sessions, if the "TimeSensitiveCommunication" feature is supported, the "ueIpv4" or "ueIpv6" attribute containing the IPv4 or IPv6 address of the UE as received from the PCF during the reporting of user plane node information as defined in subclause 4.2.5.16.

NOTE 2: The IP address of the PDU session is used as identifier of the PDU session related to the reported TSC user plane node information.

The NF service consumer shall provide the corresponding service information in the "medComponents" attribute if available. The AF shall indicate to the PCF as part of the "medComponents" attribute whether the service data flow(s) (IP or Ethernet) should be enabled or disabled with the "fStatus" attribute.

If the "AuthorizationWithRequiredQoS" feature as defined in subclause 5.8 is supported, the AF may provide within the MediaComponent data structure required QoS information as specified in subclause 4.2.2.32.

The AF may include the AF application identifier in the "afAppId" attribute into the body of the HTTP POST request in order to indicate the particular service that the AF session belongs to.

The AF application identifier may be provided at both "AppSessionContextReqData" data type level, and "MediaComponent" data type level. When provided at both levels, the AF application identifier provided at "MediaComponent" data type level shall have precedence.

The AF application identifier at the "AppSessionContextReqData" data type level may be used to trigger the PCF to indicate to the SMF/UPF to perform the application detection based on the operator's policy as defined in 3GPP TS 29.512 [8].

If the "IMS\_SBI" feature is supported, the NF service consumer may include the AF charging identifier in the "afChargId" attribute for charging correlation purposes.

If the "TimeSensitiveNetworking" or "TimeSensitiveCommunication" feature is supported the NF service consumer may provide TSC information as specified in subclauses 4.2.2.24 and 4.2.2.25.

The NF service consumer may also include the "evSubsc" attribute of "EventsSubscReqData" data type to request the notification of certain user plane events. The NF service consumer shall include the events to subscribe to in the "events" attribute, and the notification URI where to address the Npcf\_PolicyAuthorization\_Notify service operation in the "notifUri" attribute. The events subscription is provisioned in the "Events Subscription" sub-resource.

The AF shall also include the "notifUri" attribute in the "AppSessionContextReqData" data type to indicate the URI where the PCF can request to the AF the deletion of the "Individual Application Session Context" resource.

If the PCF cannot successfully fulfil the received HTTP POST request due to the internal PCF error or due to the error in the HTTP POST request, the PCF shall send the HTTP error response as specified in subclause 5.7.

Otherwise, when the PCF receives the HTTP POST request from the NF service consumer, the PCF shall apply session binding as described in 3GPP TS 29.513 [7]. To allow the PCF to identify the PDU session for which the HTTP POST request applies, the NF service consumer shall provide in the body of the HTTP POST request:

- for IP type PDU session, either the "ueIpv4" attribute or "ueIpv6" attribute containing the IPv4 or the IPv6 address applicable to an IP flow or IP flows towards the UE; and

- for Ethernet type PDU session, the "ueMac" attribute containing the UE MAC address applicable to an Ethernet flow or Ethernet flows towards the UE.

The NF service consumer may provide DNN in the "dnn" attribute, SUPI in the "supi" attribute, GPSI in the "gpsi" attribute, the S-NSSAI in the "sliceInfo" attribute if available for session binding. The NF service consumer may also provide the domain identity in the "ipDomain" attribute.

NOTE 3: The "ipDomain" attribute is helpful in the following scenario: Within a network slice, there are several separate IP address domains, with SMF/UPF(s) that allocate Ipv4 IP addresses out of the same private address range to UE PDU sessions. The same IP address can thus be allocated to UE PDU sessions served by SMF/UPF(s) in different address domains. If one PCF controls several SMF/UPF(s) in different IP address domains, the UE IP address is thus not sufficient for the session binding. A NF service consumer can serve UEs in different IP address domains, either by having direct IP interfaces to those domains, or by having interconnections via NATs in the user plane between the UPF and the NF service consumer. If a NAT is used, the NF service consumer obtains the IP address allocated to the UE PDU session via application level signalling and supplies it for the session binding to the PCF in the "ueIpv4" attribute. The NF service consumer supplies an "ipDomain" attribute denoting the IP address domain behind the NAT in addition. The NF service consumer can derive the appropriate value from the source address (allocated by the NAT) of incoming user plane packets. The value provided in the "ipDomain" attribute is operator configurable.

NOTE 4: The "sliceInfo" attribute is helpful in the scenario where multiple network slices are deployed in the same DNN, and the same IPv4 address may be allocated to UE PDU sessions in different network slices. If one PCF controls several network slices, the UE IP address is not sufficient for the session binding. The NF service consumer supplies "sliceInfo" attribute denoting the network slice that allocated the IPv4 address of the UE PDU session. How the NF service consumer derives S-NSSAI is out of the scope of this specification.

NOTE 5: When the scenario described in NOTE 3 applies and the NF service consumer is a P-CSCF it is assumed that the P-CSCF has direct IP interfaces to the different IP address domains and that no NAT is located between the UPF and P-CSCF. How a non-IMS NF service consumer obtains the UE private IP address to be provided to the PCF is out of scope of the present release; it is unspecified how to support applications that use a protocol that does not retain the original UE’s private IP address.

If the PCF fails in executing session binding, the PCF shall reject the Npcf\_PolicyAuthorization\_Create service operation with an HTTP "500 Internal Server Error" response including the "cause" attribute set to "PDU\_SESSION\_NOT\_AVAILABLE".

If the request contains the "medComponents" attribute the PCF shall store the received service information. The PCF shall process the received service information according to the operator policy and may decide whether the request is accepted or not. The PCF may take the priority information within the "resPrio" attribute into account when making this decision.

If the service information provided in the body of the HTTP POST request is rejected (e.g. the subscribed guaranteed bandwidth for a particular user is exceeded or the authorized data rate in that slice for a UE is exceeded), the PCF shall indicate in an HTTP "403 Forbidden" response message the cause for the rejection including the "cause" attribute set to "REQUESTED\_SERVICE\_NOT\_AUTHORIZED".

If the PCF detects that a temporary network failure has occurred (e.g. the SGW has failed as defined in subclause B.3.3.x or B.3.4.x of 3GPP TS 29.512 [8]) and the AF initiates an Npcf\_PolicyAuthorization\_Create service operation, the PCF shall reject the request with an HTTP "403 Forbidden" response including the "cause" attribute set to "TEMPORARY\_NETWORK\_FAILURE".

If the service information provided in the HTTP POST request is rejected due to a temporary condition in the network (e.g. the NWDAF reported the network slice selected for the PDU session is congested), the PCF may include in the "403 Forbidden" response the "cause" attribute set to "REQUESTED\_SERVICE\_TEMPORARILY\_NOT\_AUTHORIZED". The PCF may also provide a retry interval within the "Retry-After" HTTP header field. When the NF service consumer receives the retry interval within the "Retry-After" HTTP header field, the NF service consumer shall not send the same service information to the PCF again (for the same application session context) until the retry interval has elapsed. The "Retry-After" HTTP header is described in 3GPP TS 29.500 [5] subclause 5.2.2.2.

NOTE 6: When the PCF supports data rate control per network slice and/or data rate control per network slice for a UE as specified in 3GPP TS 29.512 [8] and the authorized data rate for any of those cases in a slice is exceeded due to the bandwidth demands of the new service information, it is also possible to accept the request based on operator policies. In this case the derived PCC rule(s) belonging to the authorized GBR service data flows can include a different MBR and/or have a different charging than the one applicable if the data rate is not exceeded as specified in 3GPP TS 29.512 [8].

The PCF may additionally provide the acceptable bandwidth within the attribute "acceptableServInfo" included in the "ExtendedProblemDetails" data structure returned in the rejection response message.

To allow the PCF and SMF/UPF to perform PCC rule authorization and QoS flow binding for the described service data flows, the NF service consumer shall supply:

- for IP type PDU session, both source and destination IP addresses and port numbers in the "fDescs" attribute within the "medSubComps" attribute, if such information is available; and

- for Ethernet type PDU session, the Ethernet Packet filters in the "ethfDescs" attribute within the "medSubComps" attribute, if such information is available.

The NF service consumer may specify the ToS traffic class within the "tosTrCl" attribute for the described service data flows together with the "fDescs" attribute.

The NF service consumer may include the "resPrio" attribute at the "AppSessionContextReqData" data type level to assign a priority to the AF Session as well as include the "resPrio" attribute at the "MediaComponent" data type level to assign a priority to the service data flow. The presence of the "resPrio" attribute in both levels does not constitute a conflict as they each represent different types of priority. The reservation priority at the "AppSessionContextReqData" data type level provides the relative priority for an AF session while the reservation priority at the "MediaComponent" data type level provides the relative priority for a service data flow within a session. If the "resPrio" attribute is not specified, the requested priority is PRIO\_1.

The PCF shall check whether the received service information requires PCC rules to be created and provisioned as specified in 3GPP TS 29.513 [7]. Provisioning of PCC rules to the SMF shall be carried out as specified at 3GPP TS 29.512 [8].

Based on the received subscription information from the NF service consumer, the PCF may create a subscription to event notifications for a related PDU session from the SMF, as described in 3GPP TS 29.512 [8].

If the PCF created an "Individual Application Session Context" resource, the PCF shall send to the NF service consumer a "201 Created" response to the HTTP POST request, as shown in figure 4.2.2.2-1, step 2. The PCF shall include in the "201 Created" response:

- a Location header field; and

- an "AppSessionContext" data type in the payload body.

The Location header field shall contain the URI of the created individual application session context resource i.e. "{apiRoot}/npcf-policyauthorization/v1/app-sessions/{appSessionId}".

When "Events Subscription" sub-resource is created in this procedure, the NF service consumer shall build the sub-resource URI by adding the path segment "/events-subscription" at the end of the URI path received in the Location header field.

The "AppSessionContext" data type payload body shall contain the representation of the created "Individual Application Session Context" resource and may include the "Events Subscription" sub-resource.

The PCF shall include in the "evsNotif" attribute:

- if the NF service consumer subscribed to the event "PLMN\_CHG" in the HTTP POST request, the "event" attribute set to "PLMN\_CHG" and the "plmnId" attribute including the PLMN Identifier or the SNPN Identifier if the PCF has previously requested to be updated with this information in the SMF;

NOTE 7: The SNPN Identifier consists of the PLMN Identifier and the NID.

- if the NF service consumer subscribed to the event "ACCESS\_TYPE\_CHANGE" in the HTTP POST request, the "event" attribute set to "ACCESS\_TYPE\_CHANGE" and:

i. the "accessType" attribute including the access type, and the "ratType" attribute including the RAT type when applicable for the notified access type; and

ii. if the "ATSSS" feature is supported, the "addAccessInfo" attribute with the additional access type information if available, where the access type is encoded in the "accessType" attribute, and the RAT type is encoded in the "ratType" attribute when applicable for the notified access type; and

NOTE 8: For a MA PDU session, if the "ATSSS" feature is not supported by the NF service consumer the PCF includes the "accessType" attribute and the "ratType" attribute with a currently active combination of access type and RAT type (if applicable for the notifed access type). When both 3GPP and non-3GPP accesses are available, the PCF includes the information corresponding to the 3GPP access.

iii. the "anGwAddr" attribute including access network gateway address when available,

if the PCF has previously requested to be updated with this information in the SMF; and

- if the "IMS\_SBI" feature is supported and if the NF service consumer subscribed to the "CHARGING\_CORRELATION" event in the HTTP POST request, the "event" attribute set to "CHARGING\_CORRELATION" and may include the "anChargIds" attribute containing the access network charging identifier(s) and the "anChargAddr" attribute containing the access network charging address.

The NF service consumer subscription to other specific events using the Npcf\_PolicyAuthorization\_Create request is described in the related subclauses. Notification of events when the applicable information is not available in the PCF when receiving the Npcf\_PolicyAuthorization\_Create request is described in subclause 4.2.5.

The acknowledgement towards the NF service consumer should take place before or in parallel with any required PCC rule provisioning towards the SMF.

NOTE 9: The behaviour when the NF service consumer does not receive the HTTP response message, or when it arrives after the internal timer waiting for it has expired, or when it arrives with an indication different than a success indication, are outside the scope of this specification and based on operator policy.

\*\*\* Next Change \*\*\*

#### 4.2.3.2 Modification of service information

This procedure is used to modify an existing application session context as defined in 3GPP TS 23.501 [2], 3GPP TS 23.502 [3] and 3GPP TS 23.503 [4] when the feature "PatchCorrection" is supported.

Figure 4.2.3.2-1 illustrates the modification of service information using HTTP PATCH method.



Figure 4.2.3.2-1: Modification of service information using HTTP PATCH

The NF service consumer may modify the application session context information at any time (e.g. due to an AF session modification or internal NF service consumer trigger) and invoke the Npcf\_PolicyAuthorization\_Update service operation by sending the HTTP PATCH request message to the resource URI representing the "Individual Application Session Context" resource, as shown in figure 4.2.3.2-1, step 1, with the modifications to apply.

The JSON body within the PATCH request shall include the "AppSessionContextUpdateDataPatch" data type and shall be encoded according to "JSON Merge Patch", as defined in IETF RFC 7396 [21]. The modifications to apply are encoded within the attributes of the "ascReqData" attribute, as described below and in subsequent subclauses.

The NF service consumer may include the updated service information in the "medComponents" attribute of the "ascReqData" attribute.

If the "AuthorizationWithRequiredQoS" feature as defined in subclause 5.8 is supported, the NF service consumer may provide within the MediaComponentRm data structure an update of the required QoS information as specified in subclause 4.2.3.30.

The NF service consumer may include in the "ascReqData" attribute an AF application identifier in the "afAppId" attribute to trigger the PCF to indicate to the SMF/UPF to perform the application detection based on the operator's policy as defined in 3GPP TS 29.512 [8].

If the "TimeSensitiveNetworking" or "TimeSensitiveCommunication" feature is supported, the NF service consumer may provide TSC user plane node related information as specified in subclauses 4.2.3.24 and 4.2.3.25.

The NF service consumer may also create, modify or remove events subscription information by sending the HTTP PATCH request message to the resource URI representing the "Individual Application Session Context" resource.

The NF service consumer shall create event subscription information by including in the "ascReqData" attribute the "evSubsc" attribute of "EventsSubscReqDataRm" data type with the corresponding list of events to subscribe to; and the "notifUri" attribute with the notification URI where the PCF shall send the notifications.

The NF service consumer shall update existing event subscription information by including in the "ascReqData" attribute an updated value of the "evSubsc" attribute of the "EventsSubscReqDataRm" data type as follows:

- The "events" attribute shall include the new complete list of subscribed events.

- When the NF service consumer requests to update the additional information related to an event (e.g. the NF service consumer needs to provide new thresholds to the PCF in the "usgThres" attribute related to the "USAGE\_REPORT" event) the NF service consumer shall include the additional information, which shall completely replace the previously provided one.

NOTE 1: Note that when the NF service consumer requests to remove an event, this event is not included in the "events" attribute.

NOTE 2: When an event is included in the "events" attribute and its related additional information is set to null, the PCF considers the subscription to this event is active, but the related procedures stop applying.

NOTE 3: When an event is removed from the "events" attribute but its related information is not set to null, the PCF considers the subscription to this event is terminated, the related additional information is removed, and the related procedures stop applying.

The NF service consumer shall remove existing event subscription information by setting to null the "evSubsc" attribute included in the "ascReqData" attribute.

Events with "notifMethod" set to "ONE\_TIME" shall only apply at the time the NF service consumer requests their subscription. Once the event report is performed, the subscription to this event is automatically terminated in the PCF and the related information is removed. The presence of a one-time event, together with its related additional information when applicable, during an update procedure shall represent the recreation of the subscription to this event in the PCF.

NOTE 4: The "notifUri" attribute within the EventsSubscReqData data structure can be modified to request that subsequent notifications are sent to a new NF service consumer.

If the PCF cannot successfully fulfil the received HTTP PATCH request due to the internal PCF error or due to the error in the HTTP PATCH request, the PCF shall send the HTTP error response as specified in subclause 5.7.

If the feature "ES3XX" is supported, and the PCF determines the received HTTP PATCH request needs to be redirected, the PCF shall send an HTTP redirect response as specified in subclause 6.10.9 of 3GPP TS 29.500 [5].

Otherwise, the PCF shall process the received service information according the operator policy and may decide whether the HTTP request message is accepted or not.

If the updated service information is not acceptable (e.g. the subscribed guaranteed bandwidth for a particular user is exceeded or the authorized data rate in that slice for the UE is exceeded), the PCF shall include in an HTTP "403 Forbidden" response message the "cause" attribute set to "REQUESTED\_SERVICE\_NOT\_AUTHORIZED".

If the PCF detects that a temporary network failure has occurred (e.g. the SGW has failed as defined in subclause B.3.3.x or B.3.4.x of 3GPP TS 29.512 [8]) and the AF initiates an Npcf\_PolicyAuthorization\_Update service operation, the PCF shall reject the request with an HTTP "403 Forbidden" response including the "cause" attribute set to "TEMPORARY\_NETWORK\_FAILURE".

If the service information provided in the HTTP PATCH request is rejected due to a temporary condition in the network (e.g. the NWDAF reported the network slice selected for the PDU session is congested), the PCF may include in the "403 Forbidden" response the "cause" attribute set to "REQUESTED\_SERVICE\_TEMPORARILY\_NOT\_AUTHORIZED". The PCF may also provide a retry interval within the "Retry-After" HTTP header field. When the NF service consumer receives the retry interval within the "Retry-After" HTTP header field, the NF service consumer shall not send the same service information to the PCF again (for the same application session context) until the retry interval has elapsed. The "Retry-After" HTTP header is described in 3GPP TS 29.500 [5] subclause 5.2.2.2.

NOTE 5: When the PCF supports data rate control per network slice and/or data rate control per network slice for a UE as specified in 3GPP TS 29.512 [8] and the authorized data rate in a slice is exceeded due to the bandwidth demands of the modified service information, it is also possible to accept the request based on operator policies. In this case the derived PCC rule(s) belonging to the authorized GBR service data flows can include a different MBR and/or have a different charging than the one applicable if the data rate is not exceeded as specified in 3GPP TS 29.512 [8].

The PCF may additionally provide the acceptable bandwidth within the attribute "acceptableServInfo" included in the "ExtendedProblemDetails" data structure returned in the rejection response message.

If the request is accepted, the PCF shall update the service information with the new information received. Due to the updated service information, the PCF may need to create, modify or delete the related PCC rules as specified in 3GPP TS 29.513 [7] and provide the updated information towards the SMF following the corresponding procedures specified in 3GPP TS 29.512 [8].

Based on the received subscription information from the NF service consumer, the PCF may create a subscription to event notifications or may modify the existing subscription to event notifications, for a related PDU session from the SMF, as described in 3GPP TS 29.512 [8].

The PCF shall reply with the HTTP response message to the NF service consumer and may include the "AppSessionContext" data type payload body with the representation of the modified "Individual Application Session Context" resource and may include the "Events Subscription" sub-resource.

The PCF shall include in the "evsNotif" attribute:

- if the NF service consumer subscribed to the "PLMN\_CHG" event in the HTTP PATCH request, the "event" attribute set to "PLMN\_CHG" and the "plmnId" attribute including the PLMN Identifier or the SNPN Identifier if the PCF has previously requested to be updated with this information in the SMF;

NOTE 6: The SNPN Identifier consists of the PLMN Identifier and the NID.

- if the NF service consumer subscribed to the event "ACCESS\_TYPE\_CHANGE" event in the HTTP PATCH request, the "event" attribute set to "ACCESS\_TYPE\_CHANGE" and: the attributes

i. the "accessType" attribute including the access type, and the "ratType" attribute including the RAT type when applicable for the notified access type; and

ii. if the "ATSSS" feature is supported, the "addAccessInfo" attribute with the additional access type information if available, where the access type is encoded in the "accessType" attribute, and the RAT type is encoded in the "ratType" attribute when applicable for the notified access type; and

NOTE 7: For a MA PDU session, if the "ATSSS" feature is not supported by the NF service consumer, the PCF includes the "accessType" attribute and the "ratType" attribute with a currently active combination of access type and RAT type (if applicable for the notifed access type). When both 3GPP and non-3GPP accesses are available, the PCF includes the information corresponding to the 3GPP access.

iii. the "anGwAddr" attribute including access network gateway address when available,

if the PCF has previously requested to be updated with this information in the SMF; and

- if the "IMS\_SBI" feature is supported and if the NF service consumer subscribed to the "CHARGING\_CORRELATION" event in the HTTP PATCH request, the "event" attribute set to "CHARGING\_CORRELATION" and may include the "anChargIds" attribute containing the access network charging identifier(s) and the "anChargAddr" attribute containing the access network charging address.

The NF service consumer subscription to other specific events using the Npcf\_PolicyAuthorization\_Update request is described in the related subclauses. Notification of events when the applicable information is not available in the PCF when receiving the Npcf\_PolicyAuthorization\_Update request is described in subclause 4.2.5.

The HTTP response message towards the NF service consumer should take place before or in parallel with any required PCC rule provisioning towards the SMF.

If the PCF does not have an existing application session context for the application session context being modified (such as after a PCF failure), the PCF shall reject the HTTP request message with the HTTP response message with the applicable rejection cause.

\*\*\* Next Change \*\*\*

#### 4.2.5.5 Notification about Service Data Flow Deactivation

When the PCF gets the knowledge that one or more SDFs have been deactivated, the PCF shall inform the NF service consumer accordingly if the NF service consumer has previously subscribed as described in subclauses 4.2.2.7 and 4.2.3.7.

When not all the service data flows within the AF application session context are affected, the PCF shall notify the NF service consumer by including the "EventsNotification" data type in the body of the HTTP POST request as described in subclause 4.2.5.2.

The PCF shall include within the "evNotifs" attribute an event of "AfEventNotification" data type indicating the matched event "FAILED\_RESOURCES\_ALLOCATION" in the "event" attribute and the deactivated service data flows (if not all the flows are affected) encoded in the "flows" attribute.

NOTE x1: If the PCF detects that the PCC rules related to an AF application session context cannot be installed or modified because there is a temporary network failure (e.g. SGW failed according to subclause B.3.3.x or B.3.4.x of 3GPP TS 29.512 [8]) and if requested by the AF, the PCF can notify the AF of the event "FAILED\_RESOURCES\_ALLOCATION".

If the "MediaComponentVersioning" feature is supported, and if the content version was included when the corresponding media component was provisioned as described in subclause 4.2.5.8, the PCF shall also include in the "flows" attribute the "contVers" attribute with the content version(s) of the media components.

If the "RAN-NAS-Cause" feature is supported and the PCF received the RAN-NAS release cause and access network information from the SMF, the PCF shall provide in the "EventsNotification" data type of the HTTP POST request:

- in case of 3GPP access, the user location information in the "eutraLocation" or in the "nrLocation" attribute in the "ueLoc" attribute, if available;

- in case of untrusted non-3GPP access, the user location information in the "n3gaLocation" attribute in the "ueLoc" attribute, if available, as follows:

a) the user local IP address in the "ueIpv4Addr" or "ueIpv6Addr" attribute; and

b) the UDP source port or the TCP source port in the "portNumber" and "protocol" attributes, if available;

NOTE x2: When the UE reaches the ePDG via a NAT, the combination of UE local IP address and the UE source port is needed for lawful interception purposes. The UE source port may be either a UDP or a TCP port, and it is indicated in the "protocol" attribute.

- in case of trusted non-3GPP access, the user location information in the "n3gaLocation" attribute in the "ueLoc" attribute, if available, as follows:

a) the user local IP address in the "ueIpv4Addr" or "ueIpv6Addr" attribute, if available; and

b) the UDP source port in the "portNumber" attribute if available; and

NOTE x3: The UDP protocol can be used between the UE and the TNGF to enable NAT traversal.

c) either the TNAP identifier encoded in the "tnapId" attribute or the TWAP identifier encoded in the "twapId" attribute. The TNAP identifier and the TWAP identifier shall consist of:

i. the SSID in the "ssId" attribute;

ii. the BSSID the "bssId" attribute if available; and

iii. the civic address in the "civicAddress" attribute if available;

- the serving network identity i.e. the PLMN Identifier (the PLMN network code and the country code) or the SNPN Identifier (the PLMN Identifier and the NID) in the "plmnId" attribute, if user location information is not available in any access;

- the UE timezone in the "ueTimeZone" attribute if available; and

- the RAN and/or NAS release cause in the "ranNasRelCauses" attribute, if available.

NOTE x4: The PCF forwards both 3GPP and non-3GPP access UE locations in the "ueLoc" attribute when both UE locations are provided by the SMF as defined in 3GPP TS 29.512 [8].

The PCF shall include in the "evNotifs" attribute, together with the event "FAILED\_RESOURCES\_ALLOCATION", an event of the "AfEventNotification" data type with the "event" attribute set to the value "RAN\_NAS\_CAUSE".

The PCF shall include more than one entry in the "contVers" attribute for the same media component if the PCF has received multiple content versions as described in subclause 4.2.6.2.14 in 3GPP TS 29.512 [8].

When the NF service consumer receives the HTTP POST request, it shall acknowledge the request by sending a "204 No Content" response to the PCF. The NF service consumer may also update the AF application session context information by sending an HTTP PATCH request to the PCF.

When all the service data flows within the AF session are affected, the PCF shall inform the NF service consumer by sending a notification about application session context termination as defined in subclause 4.2.5.3.

Signalling flows for Service Data Flow Deactivation cases are presented in 3GPP TS 29.513 [7].

\*\*\* Next Change \*\*\*

### 5.7.3 Application Errors

The application errors defined for the Npcf\_PolicyAuthorization API are listed in table 5.7.3-1. The PCF shall include in the HTTP status code a "ProblemDetails" data structure with the "cause" attribute indicating the application error as listed in table 5.7.3-1.

Table 5.7.3-1: Application errors

| Application Error | HTTP status code | Description |
| --- | --- | --- |
| INVALID\_SERVICE\_INFORMATION | 400 Bad Request | The HTTP request is rejected because the service information is invalid or insufficient for the PCF to perform the requested action, e.g. invalid media type or invalid QoS reference. (NOTE 1) |
| FILTER\_RESTRICTIONS | 400 Bad Request | The HTTP request is rejected because the IP flow descriptions cannot be handled by the PCF because the restrictions defined in clause 5.3.8 of 3GPP TS 29.214 [20] are not observed. (NOTE 1) |
| DUPLICATED\_AF\_SESSION | 400 Bad Request | The HTTP request is rejected because the new Individual Application Session Context relates to an AF session with another related active Individual Application Session Context, e.g. if the AF provided the same AF charging identifier for this new Individual Application Session Context that is already in use for the other ongoing Individual Application Session Context. (NOTE 2) |
| REQUESTED\_SERVICE\_NOT\_AUTHORIZED | 403 Forbidden | The service information provided in the request is rejected. (NOTE 1) |
| REQUESTED\_SERVICE\_TEMPORARILY\_NOT\_AUTHORIZED | 403 Forbidden | The service information provided in the request is temporarily rejected. (NOTE 2) |
| UNAUTHORIZED\_SPONSORED\_DATA\_CONNECTIVITY | 403 Forbidden | The request for sponsored data connectivity is not authorized. (NOTE 3) |
| UNAUTHORIZED\_NON\_EMERGENCY\_SESSION | 403 Forbidden | The PCF rejects a new AF session context setup because the session binding function associated a non-Emergency IMS session to a PDU session established to an Emergency DNN. |
| TEMPORARY\_NETWORK\_FAILURE | 403 Forbidden | The PCF rejects new or modified service information because there is a temporary failure in the access network (e.g. the SGW has failed) |
| APPLICATION\_SESSION\_CONTEXT\_NOT\_FOUND | 404 Not Found | The HTTP request is rejected because the specified Individual Application Session Context does not exist. (NOTE 4) |
| PDU\_SESSION\_NOT\_AVAILABLE | 500 Internal Server Error | The PCF failed in executing session binding. (NOTE 5) |
| NOTE 1: This application error is included in the response to the POST request (see subclauses 4.2.2.2 and 4.2.2.5) and to the PATCH request (see subclauses 4.2.3.2 and 4.2.3.5).NOTE 2: This application error is included in the response to the POST request (see subclause 4.2.2.2) and to the PATCH request (see subclause 4.2.3.2).NOTE 3: This application error is included in the response to the POST request (see subclause 4.2.2.5) and to the PATCH request (see subclause 4.2.3.5).NOTE 4: This application error is included in the responses to the GET, PATCH and delete custom operation requests to the Individual Application Session Context resource, and to the PUT and DELETE requests to the Events Subscription resource.NOTE 5: This application error is included in the response to the POST request (see subclauses 4.2.2.2, 4.2.6.3 and 4.2.2.27). |

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