**TSG-CT WG3 Meeting #117-e *C3-214082***

**E-Meeting, 18th – 27th August 2021 (Revision of C3-214xyz)**

|  |
| --- |
| *CR-Form-v12.1* |
| **CHANGE REQUEST** |
|  |
|  | **29.512** | **CR** | 0808 | **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:***  | Authorization of UE initiates a resource modification |
|  |  |
| ***Source to WG:*** | Huawei |
| ***Source to TSG:*** | CT3 |
|  |  |
| ***Work item code:*** | en5GPccSer17 |  | ***Date:*** | 2021-08-18 |
|  |  |  |  |  |
| ***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:*** | As defined in clause 4.5.2.0 of TS 29.212, if the PCRF receives a request for PCC rules for an IP-CAN session from the PCEF, or a request for QoS rules for a gateway control session from the BBERF, while no suitable authorized PCC rules are configured in the PCRF or can be derived from service information provisioned by an AF, the PCRF shall check the set of services the user is allowed to access.If the user is not allowed to access AF session based services, the PCRF shall check whether the user is allowed to request resources for services not known to the PCRF and whether the requested QoS and/or packet filters can be authorized. If this is the case, the PCRF shall provide a PCC rule to authorize the UE requested QoS and packet filters that were received as part of the request for PCC/QoS rules. The service data flow description shall be derived from the packet filter information. If the user is not allowed to request resources for services not known to the PCRF, the PCRF shall reject the request.The same scenario shall be also applied to the PCF. |
|  |  |
| ***Summary of change:*** | Define the authorization of UE initiates a resource modification |
|  |  |
| ***Consequences if not approved:*** | How to authorize the UE initiates a resource modification is not defined. |
|  |  |
| ***Clauses affected:*** | 4.2.4.17, 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 \*\*\*

#### 4.2.4.17 UE initiates a resource modification support

In the case that the UE initiates a resource modification procedure as defined in subclause 6.4.2.2 of 3GPP 3GPP TS 24.501 [20], the SMF shall within the SmPolicyUpdateContextData data structure include the "RES\_MO\_RE" within the "repPolicyCtrlReqTriggers" attribute and shall include the UE request of specific QoS handling for selected SDF within the "ueInitResReq" attribute. Within the UeInitiatedResourceRequest data structure, the SMF shall include the "ruleOp" attribute, "packFiltInfo" attribute and "reqQos" attribute if applicable as follows:

- When the UE requests to "Create new QoS rule", the SMF shall include the "ruleOp" attribute set to "CREATE\_PCC\_RULE", the "packFiltInfo" attribute and "reqQos" attribute containing the requested QoS for the new PCC rule. Each PacketFilterInfo instance shall contain one packet filters requested for creating the new QoS rule. If the PCF authorizes the request, the PCF shall create a new PCC rule by including the new packet filters within the service data flow template of the PCC rule. When the SMF received the PCC rule, the SMF shall derive the QoS rule based on the PCC rule, assign a new QoS rule identifier within the PDU session for the QoS rule. The SMF shall keep the mapping between the PCC rule identifier and the QoS rule identifier.

- When the UE requests to "Modify existing QoS rule and add packet filters" for the QoS rule created as a result of the UE-initiated resource modification, SMF shall include the "ruleOp" attribute set to "MODIFY\_PCC\_RULE\_AND\_ADD\_PACKET\_FILTERS", the "pccRuleId" attribute including the PCC rule identifier corresponding the QoS rule identifier and the "packFiltInfo" attribute. Each PacketFilterInfo instance shall contain one packet filters requested for addition to this QoS Rule. If the UE request includes the modified QoS information the SMF shall also include the "reqQos" attribute to indicate the updated QoS for the affected PCC rule(s). If the PCF authorizes the request, the PCF shall update the PCC rule by adding the new packet filters to the service data flow template of the PCC rule.

- When the UE requests to "Modify existing QoS rule and replace all packet filters" for the QoS rule created as a result of the UE-initiated resource modification, SMF shall include the "ruleOp" attribute set to "MODIFY\_PCC\_RULE\_AND\_REPLACE\_PACKET\_FILTERS", the "pccRuleId" attribute including the PCC rule identifier corresponding the QoS rule identifier and the "packFiltInfo" attribute. Each PacketFilterInfo instance shall contain one packet filters requested for addition to this QoS Rule. If the UE request includes the modified QoS information the SMF shall also include the "reqQos" attribute to indicate the updated QoS for the affected PCC rule. If the PCF authorizes the request, the PCF shall update PCC rule by replacing the all existing packet filters within the service data flow template of the PCC rule with the new packet filter(s).

- When the UE requests to "Modify existing QoS rule and delete packet filters" for the QoS rule created as a result of the UE-initiated resource modification, SMF shall include the "ruleOp" attribute set to "MODIFY\_PCC\_RULE\_AND\_DELETE\_PACKET\_FILTERS", the "pccRuleId" attribute including the PCC rule identifier corresponding the QoS rule identifier and the "packFiltInfo" attribute. Each PacketFilterInfo instance shall within the "packFiltId" attribute include the removed packet filter identifier assigned by the PCF corresponding to the packet filter identifier received from the UE. If the UE request includes modified QoS information the SMF shall also include the "reqQos" attribute to indicate the updated QoS for the affected PCC rule(s). If the PCF authorizes the request, the PCF shall update PCC rule by removing the corresponding packet filters from the service data flow template of the PCC rule.

- When the UE requests to "Modify existing QoS rule without modifying packet filters" for the QoS rule created as a result of the UE-initiated resource modification, SMF shall include the "ruleOp" attribute set to "MODIFY\_PCC\_RULE\_WITHOUT\_MODIFY\_PACKET\_FILTERS", the "pccRuleId" attribute including the PCC rule identifier corresponding the QoS rule identifier, the "packFiltInfo" attribute and the modified QoS information within the "reqQos" attribute. The "packFiltInfo" attribute shall include one PacketFilterInfo instance which includes any packet filter identifier assigned by the PCF for the PCC rule within the "packFiltId" attribute.

- When the UE requests to "Delete existing QoS rule" the SMF shall include the "ruleOp" attribute set to "DELETE\_PCC\_RULE" for the QoS rule created as a result of the UE-initiated resource modification, the "pccRuleId" attribute including the PCC rule identifier corresponding the QoS rule identifier and the "packFiltInfo" attribute. The "packFiltInfo" attribute shall include one PacketFilterInfo instance which includes any packet filter identifier assigned by the PCF for the PCC rule within the "packFiltId" attribute. The PCF shall remove the PCC rule when the PCF receives the request according to the PCC rule identifier.

NOTE 1: The UE can only modify packet filters that the UE has introduced and associated resources. The packet filter identifiers contained in the FlowInformation data structure are only used for packet filters created by the UE.

The SMF shall calculate the requested GBR, for a GBR 5QI, as the sum of the previously authorized GBR for the affected PCC rule, corresponding to the QoS rule, adjusted with the difference between the requested GBR for the QoS flow and previously negotiated GBR for the QoS flow. For the UE request to create a new QoS Rule, the GBR as requested by the UE for the QoS rule shall be used.

If the request covers all the PCC rules with a QoS flow binding to the same QoS flow, then the SMF may request a change to the 5QI for existing PCC rules.

For the purpose of creating or modifying a QoS rule with adding, replacing and modifying packet filter, within the UeInitiatedResourceRequest instance, the SMF shall include the precedence information of the QoS rule within the "precedence" attribute, and within each PacketFilterInfo instance, the SMF shall include the "packFiltCont" attribute, "tosTrafficClass" attribute, "spi" attribute, "flowLabel" attribute and "flowDirection" attribute set to the value(s) describing the packet filter provided by the UE.

NOTE 2: The UE signalling with the network is governed by the applicable NAS signalling TS. The NAS 3GPP TS for a specific access may restrict the UE possibilities to make requests compared to what is stated above.

Upon receipt of the request from the SMF, the PCF shall check the set of services the user is allowed to access. If the user is not allowed to access AF session based services, the PCF shall check whether the user is allowed to request resources for services not known to the PCF and whether the requested QoS and/or packet filters can be authorized. If the user is not allowed to request resources for services not known to the PCF, the PCF shall reject the request with in an HTTP "403 Forbidden" response message including the "cause" attribute of the ProblemDetails data structure set to "POLICY\_CONTEXT\_DENIED".

If the PCF authorizes the request from the UE, the PCF shall construct a PCC rule(s) based on the UeInitiatedResourceRequest data structure. For the request to add the filter(s), the PCF shall within the FlowInformation data structure include the assigned packet filter identifier within the "packFiltId" attribute. When the SMF derives the QoS based on the PCC rule, the SMF shall assign a new packet filter identifier for each added packet filter within the QoS rule and keep the mapping between the packet filter identifier for the packet filter within the PCC rule and QoS rule.

The PCF shall perform the QoS authorization for the new created or modified PCC rules if requested by the UE as defined in subclause 4.2.6.6.2.

If the PCF detects that the packet filters in the request for new PCC rules received from the SMF is covered by the packet filters of outstanding PCC rules that the PCF is provisioning to the SMF, the PCF may reject the request and indicate the cause for the rejection including the "cause" attribute of the ProblemDetails data structure set to "ERROR\_CONFLICTING\_REQUEST" in an HTTP "403 Forbidden" response message. If the SMF receives a response message with this code, the SMF shall ignore the PDU session modification that initiated the HTTP request as specified in 3GPP TS 24.501[20] subclause 6.3.2.5.

If the PCF does not accept one or more of the traffic mapping filters provided by the SMF in an HTTP Request (e.g. because the PCF does not allow the UE to request enhanced QoS for services not known to the PCF), the PCF shall reject the request and indicate the cause for the rejection including the "cause" attribute of the ProblemDetails data structure set to "ERROR\_TRAFFIC\_MAPPING\_INFO\_REJECTED" in an HTTP "403 Forbidden" response message. If the SMF receives an HTTP response with this code, the SMF shall reject the PDU session modification that initiated the HTTP request.

The PCF shall not combine a rejection with provisioning of PCC rule operations in the same HTTP response.

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

### 5.7.3 Application Errors

The application errors defined for the Npcf\_SMPolicyControl API are listed in table 5.7.3-1 and 5.7.3-2. 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 when PCF acts as a server. The NF service consumer shall include in the HTTP status code a "ProblemDetails" data structure with the "cause" attribute indicating the application error as listed in table 5.7.3-2 when NF service consumer acts as a server.

Table 5.7.3-1: Application errors when PCF acts as a server

|  |  |  |
| --- | --- | --- |
| Application Error | HTTP status code | Description |
| USER\_UNKNOWN | 400 Bad Request | The HTTP request is rejected because the end user specified in the request is unknown to the PCF. (NOTE 1) (NOTE 3) |
| ERROR\_INITIAL\_PARAMETERS | 400 Bad Request | The HTTP request is rejected because the set of session or subscriber information needed by the PCF for rule selection is incomplete or erroneous or not available for the decision to be made. (E.g. QoS, , RAT type, subscriber information) (NOTE 1) (NOTE 2) (NOTE 3) |
| ERROR\_TRIGGER\_EVENT | 400 Bad Request | The HTTP request is rejected because the set of session information sent the message originated due to a trigger been met is incoherent with the previous set of session information for the same session. (E.g. trigger met was RAT changed, and the RAT notified is the same as before) (NOTE 2) (NOTE 3) |
| ERROR\_TRAFFIC\_MAPPING\_INFO\_REJECTED | 403 Forbidden | The HTTP request is rejected because the PCF does not accept one or more of the traffic mapping filters provided by the NF service consumer in a PCC Request. (NOTE 2) (NOTE 3) |
| ERROR\_CONFLICTING\_REQUEST | 403 Forbidden | The HTTP request is rejected because the PCF cannot accept the UE-initiated resource request as a network-initiated resource allocation is already in progress that has packet filters that cover the packet filters in the received UE-initiated resource request. The NF service consumer shall reject the attempt for UE-initiated resource request. (NOTE 2) (NOTE 3) |
| LATE\_OVERLAPPING\_REQUEST | 403 Forbidden | The request is rejected because it collides with and exiting Policy Association with a more recent originating timestamp. (NOTE 1) |
| POLICY\_CONTEXT\_DENIED | 403 Forbidden | The HTTP request is rejected because the PCF does not accept the NF service consumer request due to operator policies and/or local configuration. (NOTE 1) (NOTE 2) (NOTE 3) |
| VALIDATION\_CONDITION\_NOT\_MET | 403 Forbidden | The HTTP request is rejected because the PCF does not accept the NF service consumer request because the validation condition of background data transfer policy is not met. (NOTE 1) (NOTE 3) |
| PENDING\_TRANSACTION | 400 Bad Request | This error shall be used when the PendingTransaction feature is supported and the PCF receives an incoming request on a policy association while it has an ongoing transaction on the same policy association and cannot handle the request as described in subclause 9.2 of 3GPP TS 29.513 [7]. (NOTE 2) |
| INVALID\_BDT\_POLICY | 403 Forbidden | The HTTP request is rejected because the PCF does not accept the NF service consumer request because the background data transfer policy is invalid. (NOTE 1) |
| NOTE 1: These application errors are used by the create service operation (see subclause 4.2.2.2) and included in the responses to the POST request.NOTE 2: These application errors are used by the update service operation (see subclause 4.2.4.2) and included in the responses to the POST request.NOTE 3: The Cause codes mapping performed by NF service consumer between this Application Error and the 5GSM related value is specified in subclause 5.2.2.2 of 3GPP TS 29.524 [40]. |

Table 5.7.3-2: Application errors when NF service consumer acts as a server to receive a notification

|  |  |  |
| --- | --- | --- |
| Application Error | HTTP status code | Description |
| PCC\_RULE\_EVENT | 400 Bad Request | The HTTP request is rejected because all the PCC rules provisioned by the PCF in the request cannot be installed/activated. It is used to inform the PCF that the request failed, and should not be attempted again. (NOTE) |
| PCC\_QOS\_FLOW\_EVENT | 400 Bad Request | The HTTP request is rejected because for some reason all the PCC rules provisioned by the PCF in the request cannot be enforced or modified successfully in a network initiated procedure. It is used to inform the PCF that the request could not be satisfied at the time it was received, but may be able to satisfy the request in the future. (NOTE) |
| UE\_STATUS\_SUSPEND | 400 Bad Request | The HTTP request is rejected because the UE’s status is suspended and the policy decisions received from the PCF cannot be enforced by the NF service consumer. Applicable only to functionality introduced with the PolicyUpdateWhenUESuspends feature as described in subclause 5.8. (NOTE) |
| RULE\_PERMANENT\_ERROR | 400 Bad Request | The HTTP request is rejected because all the PCC rules and/or session rules provisioned by the PCF in the request cannot be installed/activated. It is used to inform the PCF that the request failed, and should not be attempted again. Applicable only to functionality introduced with the SessionRuleErrorHandling feature as described in subclause 5.8. (NOTE) |
| RULE\_TEMPORARY\_ERROR | 400 Bad Request | The HTTP request is rejected because for some reason all the PCC rules and/or session rules provisioned by the PCF in the request cannot be enforced or modified successfully in a network initiated procedure. It is used to inform the PCF that the request could not be satisfied at the time it was received, but may be able to satisfy the request in the future. Applicable only to functionality introduced with the SessionRuleErrorHandling feature as described in subclause 5.8. (NOTE) |
| PENDING\_TRANSACTION | 400 Bad Request | This error shall be used when the PendingTransaction feature is supported and the NF service consumer receives an incoming request on a policy association while it has an ongoing transaction on the same policy association and cannot handle the request as described in subclause 9.2 of 3GPP TS 29.513 [7]. (NOTE) |
| NOTE: These application errors are used by the UpdateNotify service operation (see subclause 4.2.3.2) and included in the responses to the POST request. |

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