**3GPP TSG-CT3 Meeting #134C3-242xxx**

**Changsha, China, 15th – 19st April 2024 was C3-242339**

|  |
| --- |
| *CR-Form-v12.2* |
| **CHANGE REQUEST** |
|  |
|  | **29.512** | **CR** | **1227** | **rev** | **1** | **Current version:** | **18.5.0** |  |
|  |
| *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:***  | Various GMEC related corrections |
|  |  |
| ***Source to WG:*** | Huawei |
| ***Source to TSG:*** | CT3 |
|  |  |
| ***Work item code:*** | GMEC |  | ***Date:*** | 2024-04-18 |
|  |  |  |  |  |
| ***Category:*** | **F** |  | ***Release:*** | Rel-18 |
|  | *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-16 (Release 16)Rel-17 (Release 17)Rel-18 (Release 18)Rel-19 (Release 19)* |
|  |  |
| ***Reason for change:*** | The following issues have been identified:* The provisions of clauses 4.2.6.9.1 and 4.2.3.2 need further clarifications and corrections to avoid confusion.
* Various terminology alignments are needed to align the provisions related to GMEC with the other impacted specifications.
 |
|  |  |
| ***Summary of change:*** | This CR proposes to:* Address the above mentioned issues.
* Apply additional editorial corrections.
 |
|  |  |
| ***Consequences if not approved:*** | * The provisions related to the GMEC functionality continue to contain provisions that may generate confusion and are misaligned with the other specifications defining this functionality.
 |
|  |  |
| ***Clauses affected:*** | 4.2.2.23, 4.2.3.2, 4.2.3.28, 4.2.4.29, 4.2.5.7, 4.2.6.2.23, 4.2.6.9.1, 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 descriptions of the APIs defined in this specification. |
|  |  |
| ***This CR's revision history:*** |  |

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

#### 4.2.2.23 Group related data rate policy control

When a Npcf\_SMPolicyControl\_Create request is received, the PCF may apply group data rate policy control as defined in clause 4.2.6.9.

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

#### 4.2.3.2 SM Policy Association Update request



Figure 4.2.3.2-1: SM Policy Association Update request

The PCF may decide to provision policies related to an Individual SM Policy resource without obtaining a request from the NF service consumer, e.g. in response to information provided to the PCF via the Rx or N5 reference points, or in response to an internal trigger within the PCF, e.g., the activation of a pending policy counter provided via the Nchf\_SpendingLimitControl Service (see 3GPP TS 29.594 [63]). The PCF shall send for this purpose a POST request to the NF service consumer (e.g. SMF) using the URI"{notificationUri}/update". The content of the message shall contain a SmPolicyNotification data structure that contains:

- the representation of the updated policies within the "smPolicyDecision" attribute; and

- the resource URI of the Individual SM Policy resource related to the notification within the "resourceUri" attribute.

Detailed procedures related to the provisioning and enforcement of the policy decisions contained within the SmPolicyDecision data structure are provided in clause 4.2.6.

When the PCF received from an NF service consumer (e.g., an AF) temporal invalidity conditions information as part of AF requested QoS for a UE or group of UE(s), the PCF shall evaluate the temporal invalidity conditions of the AF request and may inform the SMF to install, modify or remove the corresponding policy decision(s) (e.g., PCC rule(s)) according to the evaluation result for the concerned PDU Session(s).

In case of a successful update of SM policies:

- if the PCF provisioned policy control request triggers (applicable triggers are as defined in Table 5.6.2.26-1), a "200 OK" response code and a response body with the corresponding available information in the "UeCampingRep" data structure shall be returned in the response;

- otherwise, a "204 No Content" response code shall be returned in the response.

NOTE: When there is an ongoing procedure that collisions with the update of SM policies (e.g. during handover from 5GS to EPS) the SMF, based on operator policies, can delay the update of SM policies and return a "204 No Content" response code. In this case the SMF will process the request when the procedure is finished.

If errors occur when processing the HTTP POST request, the NF service consumer shall send an HTTP error response as specified in clause 5.7.

If the feature "ES3XX" is supported, and the NF service consumer determines the received HTTP POST request needs to be redirected, the NF service consumer shall send an HTTP redirect response as specified in clause 6.10.9 of 3GPP TS 29.500 [4].

If the "SessionRuleErrorHandling" feature is not supported and the NF service consumer received one or more PCC rules from the PCF, but the validation of all these PCC Rules was unsuccessful, the NF service consumer shall reject the request and include in an HTTP "400 Bad Request" response message the ErrorReport data structure. Within the ErrorReport data structure, the NF service consumer shall include the "error" attribute containing the "cause" attribute of the ProblemDetails data structure set to "PCC\_RULE\_EVENT" or "PCC\_QOS\_FLOW\_EVENT" and the "ruleReports" attribute to report the PCC rule status of the affected PCC rules as defined in clause 4.2.3.16.

If the "SessionRuleErrorHandling" feature is supported and the NF service consumer received one or more PCC rules and/or session rules from the PCF but the validation of all these PCC Rules and/or session rules was unsuccessful, the NF service consumer shall reject the request and include in an HTTP "400 Bad Request" response message the ErrorReport data structure. Within the ErrorReport data structure, the NF service consumer shall include the "error" attribute containing the "cause" attribute of the ProblemDetails data structure set to "RULE\_PERMANENT\_ERROR" or "RULE\_TEMPORARY\_ERROR" and the "ruleReports" attribute to report the PCC rule status of the affected PCC rules as defined in clause 4.2.3.16 and/or the "sessRuleReports" attribute to report the session rule status of the affected session rules as defined in clause 4.2.3.20.

If in the cases above, if the "PolicyDecisionErrorHandling" feature is supported, the PCF provisioned policy decisions and/or condition data which are not referred by any PCC rules or session rules and, in addition of the report of the faulty PCC rule(s) and/or session rule(s), the NF service consumer needs to report the failed policy decisions and/or condition data, the "policyDecFailureReports" attribute shall also be provided as described in clause 4.2.3.26. Additionally, if the "ExtPolicyDecisionErrorHandling" feature is supported the NF service consumer may also provide the "invalidPolicyDecs" as described in clause 4.2.3.26.2.

If the "Ext2PolicyDecisionErrorHandling" feature is supported, the NF service consumer did not receive neither PCC rules nor session rules and received policy decision types and/or condition types which are not referred by any PCC rules or session rules, and the storage of all the policy decision types and/or condition data was unsuccessful (e.g. the policy decision could not be successfully stored due to a limitation of resources at the SMF) or there were semantical inconsistencies in the provided data, the NF service consumer shall include in an HTTP "400 Bad Request" response message the ErrorReport data structure including the "error" attribute containing the "cause" attribute of the ProblemDetails data structure set to "POL\_DEC\_ERROR" and shall behave as defined in clause 4.2.3.26.

If the "SessionRuleErrorHandling" feature is not supported and if the NF service consumer received one or more PCC rules from the PCF but the validation of some of them was unsuccessful, the NF service consumer shall include an HTTP "200 OK" status code together with one or more RuleReport data structure(s) to report the PCC rule status of the affected PCC rules as defined in clause 4.2.3.16 in the "PartialSuccessReport" data structure included in the response message. The "failureCause" attribute of the "PartialSuccessReport" shall be set to "PCC\_RULE\_EVENT" or "PCC\_QOS\_FLOW\_EVENT".

If the "SessionRuleErrorHandling" feature is supported and the NF service consumer received one or more PCC rule and/or session rules from the PCF but the validation of some of them was unsuccessful, the NF service consumer shall include an HTTP "200 OK" status code together with the "ruleReports" attribute to report the PCC rule status of the affected PCC rules as defined in clause 4.2.3.16 and/or the "sessRuleReports" attribute to report the session rule status of the affected session rules as defined in clause 4.2.3.20 in the "PartialSuccessReport" data structure included in the response message. The "failureCause" attribute of the "PartialSuccessReport" shall be set to "RULE\_PERMANENT\_ERROR" or "RULE\_TEMPORARY\_ERROR".

If the "PolicyDecisionErrorHandling" feature is supported, the NF service consumer received policy decision types and/or condition types which are not referred by any PCC rules or session rules, and the storage or validation of not all the policy decision types and/or condition data was unsuccessful, the NF service consumer shall reply with an HTTP "200 OK" response message and behave as described in clause 4.2.3.26.

If the PCF provisioned policy control request triggers and the NF service consumer needs to report partial success information, the NF service consumer may include in the "PartialSuccessReport" data structure the "ueCampingRep" attribute with the corresponding available information. When it is required to report multiple instances of the "PartialSuccessReport" data structure due to different "failureCause" values, the NF service consumer shall use only one instance of the "PartialSuccessReport" data structure to include the "ueCampingRep" attribute with the corresponding available information.

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

#### 4.2.3.28 Group related data rate policy control

At the time a PCF-initiated change of the authorized Session-AMBR occurs or PCC Rule(s) for GBR service data flow(s) need to be provisioned at the SMF, the PCF may apply group data rate policy control as defined in clause 4.2.6.9.

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

#### 4.2.4.29 Group related data rate policy control

When a Npcf\_SMPolicyControl\_Update request that requires a change of the authorized Session-AMBR and/or MBR update(s) for PCC Rule(s) corresponding to GBR service data flow(s) is received, the PCF may apply group data rate policy control as defined in clause 4.2.6.9.

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

#### 4.2.5.7 Group related data rate policy control

When a Npcf\_SMPolicyControl\_Delete request is received, the PCF may apply group data rate policy control as defined in clause 4.2.6.9.

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

##### 4.2.6.2.23 Policy Decision for AF requested QoS for a target UE or group of UE(s) not identified by UE address(es)

When the AF requested QoS for a UE or group UE(s), the requested QoS data may be either provisioned by the AF/NEF to the TSCTSCF, and later to the PCF for the related active PDU session(s), as specified in 3GPP TS 29.565 [53] and 3GPP TS 29.514 [17], or stored by the AF/NEF at the UDR and later retrieved by the PCF for the related active PDU session(s), as defined in 3GPP TS 29.519 [15].

When the PCF needs to make Policy Decision(s) and derive PCC Rule(s) for a PDU session corresponding to the concerned UE or group of UE(s), the PCF shall take into consideration the received AF requested QoS data, if applicable, and may provide to the SMF the policy control trigger(s) corresponding to the AF subscribed event(s) as defined in clause 4.2.6.4, or activate/modify/remove PCC rule(s) as defined in clause 4.2.3.2.

When the SMF notifies the PCF about the met policy control request trigger(s) corresponding to the AF subscribed event(s), the PCF may notify either the TSCTSF or the AF/NEF, as defined in 3GPP TS 29.514 [17], based on whether the requested QoS data was provisioned via the TSCTSF or the UDR.

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

##### 4.2.6.9.1 General

A PCF that supports group related data rate policy control for 5G VN groups shall be able to control and manage the group data rate for the PDU session(s) of the UE(s) belonging to the 5G VN groups. In order to do so, the PCF shall perform the same procedures as the ones defined for network slice related data rate policy control defined in clauses 4.2.6.8 for the PDU session(s) of the UE(s) belonging to a 5G VN group, with the following differences:

- Only the PCF-based method shall be applicable for group related data rate policy control, i.e., the provisions of clause 4.2.6.8.3 shall not apply for group related data rate policy control for a 5G VN group.

- The provisions related to slice related data rate policy control for an S-NSSAI shall apply for group related data rate policy control for a 5G VN group.

- Instead of the operator configuring the Maximum Slice Date Rate per S-NSSAI at the UDR, the Maximum Group Data Rate per 5G VN group is either:

- provisioned by the AF to the UDR (for "Subscription Data") via the NEF/UDM as part of the 5G VN group subscription data, using the procedures defined in 3GPP TS 29.522 [59] and 3GPP TS 29.503 [34]);

- configured by the operator at the UDR (for "Policy Data") as part of the 5G VN group specific policy control data; or

- based on both.

- When the Maximum Group Data Rate is provisioned by the AF, the PCF shall receive the Maximum Group Data Rate either:

- by retrieving it directly from the UDR (for "Subscription Data"); or

- by receiving a notification from the UDR (for "Subscription Data") on the update of the 5G VN group subscription data, if the PCF subscribed for such notifications.

- In all of the above cases, if the value(s) of the Maximum Group Data Rate information within the 5G VN group subscription data received from the UDR (for "Subscription Data") and the value(s) of the Maximum Group Data Rate information within the 5G VN group specific policy control data received from the UDR (for "Policy Data") are different, the PCF shall update in the UDR (for "Policy Data") the value(s) of the Maximum Group Data Rate information and adjust accordingly the value(s) of the Remaining Maximum Group Data Rate information for the 5G VN group as specified in 3GPP TS 29.519[15].

- Instead of handling the Remaining Maximum Slice Data Rate per S-NSSAI, the UDR and PCF shall handle the Remaining Maximum Group Data Rate per 5G VN group.

- Instead of calculating the utilized data rate based on the value(s) of the authorized Session-AMBR and the MBR of the GBR service data flow(s) for each PDU Session of a network slice identified by an S-NSSAI, the PCF shall calculate the utilized data rate based on the value(s) of the authorized Session-AMBR and the MBR of the GBR service data flow(s) for each PDU Session of the 5G VN group.

- Instead of returning the "EXCEEDED\_SLICE\_DATA\_RATE" application error within the "403 Forbidden" error response (i.e., in case the Remaining Maximum Group Data Rate is not sufficient), the PCF shall return the "EXCEEDED\_GROUP\_DATA\_RATE" application error within the "403 Forbidden" error response.

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

### 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.

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) |
| 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 clause 9.2 of 3GPP TS 29.513 [7]. (NOTE 2) |
| 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) |
| 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) |
| EXCEEDED\_UE\_SLICE\_DATA\_RATE | 403 Forbidden | The HTTP request is rejected because the PCF does not accept the NF service consumer request because the authorized data rate exceeds the consumed data rate for that UE and network slice. (NOTE 1) (NOTE 2) |
| EXCEEDED\_SLICE\_DATA\_RATE | 403 Forbidden | The HTTP request is rejected because the PCF does not accept the NF service consumer request because the authorized data rate exceeds the consumed data rate for that slice. (NOTE 1) (NOTE 2) |
| EXCEEDED\_GROUP\_DATA\_RATE | 403 Forbidden | The HTTP request is rejected because the PCF does not accept the NF service consumer request because the authorized group data rate exceeds the consumed data rate for the concerned group. (NOTE 1) (NOTE 2) |
| POLICY\_ASSOCIATION\_NOT\_FOUND | 404 Not Found | The HTTP request is rejected because no policy association corresponding to the request exists in the PCF. (NOTE 2) |
| NOTE 1: These application errors are used by the create service operation (see clause 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 clause 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 clause 5.2.2.2 of 3GPP TS 29.524 [40].NOTE 4: Including a "ProblemDetails" data structure with the "cause" attribute in the HTTP response is optional unless explicitly mandated in the service operation clauses. |

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 1) |
| 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 1) |
| 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 clause 5.8. (NOTE 1) |
| 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 clause 5.8. (NOTE 1) |
| 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 clause 5.8. (NOTE 1) |
| 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 clause 9.2 of 3GPP TS 29.513 [7]. (NOTE 1) |
| AN\_GW\_FAILED | 400 Bad Request | This error shall be used when SGWRest feature is supported and the received policy decisions (i.e. installation/modification of PCC rules or session rules) cannot be enforced by the SMF because the AN-Gateway has failed. (NOTE 1) |
| POL\_DEC\_ERROR | 400 Bad Request | This error shall be used when Ext2PolicyDecisionErrorHandling feature is supported, the PCF provides only SM policy decisions and/or condition data and all the policy decisions and/or conditions in the request cannot be stored in the NF service consumer. |
| NOTE 1: These application errors are used by the UpdateNotify service operation (see clause 4.2.3.2) and included in the responses to the POST request.NOTE 2: Including a "ProblemDetails" data structure with the "cause" attribute in the HTTP response is optional unless explicitly mandated in the service operation clauses. |

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