**TSG-CT WG3 Meeting #112-e *C3-205xyz***

**E-Meeting, 4th – 13th November 2020 (Revision of C3-205261)**

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| *CR-Form-v12.1* | | | | | | | | |
| **CHANGE REQUEST** | | | | | | | | |
|  | | | | | | | | |
|  | **29.122** | **CR** | **0307** | **rev** | **1** | **Current version:** | **16.7.0** |  |
|  | | | | | | | | |
| *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:*** | Failure response for SCEF northbound APIs | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Source to WG:*** | Huawei, Ericsson | | | | | | | | | |
| ***Source to TSG:*** | CT3 | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Work item code:*** | NAPS-CT | | | | |  | ***Date:*** | | | 2020-10-28 |
|  |  | | | |  | |  | | |  |
| ***Category:*** | **A** |  | | | | | ***Release:*** | | | Rel-16 |
|  | *Use one of the following categories:* ***F*** *(correction)* ***A*** *(mirror corresponding to a change in an earlier release)* ***B*** *(addition of feature),* ***C*** *(functional modification of feature)* ***D*** *(editorial modification)*  Detailed explanations of the above categories can be found in 3GPP [TR 21.900](http://www.3gpp.org/ftp/Specs/html-info/21900.htm). | | | | | | | | *Use one of the following releases: Rel-8 (Release 8) Rel-9 (Release 9) Rel-10 (Release 10) Rel-11 (Release 11) … Rel-15 (Release 15) Rel-16 (Release 16) Rel-17 (Release 17) Rel-18 (Release 18)* | |
|  |  | | | | | | | | | |
| ***Reason for change:*** | | When SCEF receiving error status code from the southbound NF (e.g. PCRF, HSS). Not always correct to send 500 internal server error status code to SCS/AS, Since the southbound NF as service provider can respond with not only server error code 5xx(500 or 503), but also support to respond with specific Client error code 4xx, or other available error status codes have been specified in the OpenAPI files. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Summary of change:*** | | Proper error status code shall be sent from the SCEF to the SCS/AS upon evaluating the error status code received from the southbound NF, or SCS/AS concluded error status code. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Consequences if not approved:*** | | Sending wrong error code which is not reflecting the client error, impacting the correct procedure fulfilment and SCS/AS judgement of user status. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Clauses affected:*** | | 4.4.2.2.2.2; 4.4.2.2.2.3; 4.4.2.2.3; 4.4.3; 4.4.4; 4.4.5.3.1; 4.4.7.2.2.1; 4.4.7.2.2.3; 4.4.7.2.2.4; 4.4.7.2.3.1; 4.4.7.2.3.3; 4.4.7.2.3.4; 4.4.9; 4.4.10; 4.4.11; 4.4.12.2; 4.4.12.3; 4.4.13 | | | | | | | | |
|  | |  | | | | | | | | |
|  | | **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 doesn’t impact the OpenAPI file. | | | | | | | | |
|  | |  | | | | | | | | |
| ***This CR's revision history:*** | |  | | | | | | | | |

**Additional discussion(if needed):**

**Proposed changes:**

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

###### 4.4.2.2.2.2 Configuration Request for an individual UE

Upon receipt of the request from the SCS/AS, if the configuration request from the SCS/AS is for an individual UE, the SCEF shall interact with the HSS via S6t as specified in 3GPP TS 29.336 [11].

Upon receipt of the successful response from the HSS,

- if it is a one-time monitoring request and the monitoring event report is received, the SCEF shall delete the associated configuration, send the HTTP POST response message to the SCS/AS with a "200 OK" status code and including the received monitoring event report.

- otherwise, the SCEF shall,

- for HTTP POST request, create a resource "Individual Monitoring Event Subscription" addressed by the URI that contains the SCS/AS identifier and an SCEF-created subscription identifier, and send an HTTP POST response to the SCS/AS with a "201 Created" status code, the final suggested configuration parameter(s) (if modified), the indication(s) for the discarded parameter(s) (if discarded), the monitoring event report if received and a location header field containing the URI for the created resource.

- for HTTP PUT request, update the active resource "Individual Monitoring Event Subscription" addressed by the URI and send an HTTP response to the SCS/AS with a "200 OK" status code, the final suggested configuration parameter(s) (if modified), the indication(s) for the discarded parameter(s) (if discarded) and the monitoring event report if received.

- for HTTP DELETE request, delete the active resource "Individual Monitoring Event Subscription" addressed by the URI and send an HTTP response to the SCS/AS with a "204 No Content" status code, or a "200 OK" status code and including the monitoring event report if received.

If the SCEF receives a response with an error code from the HSS, the SCEF shall not create, update or delete the resource and shall respond to the SCS/AS with a corresponding failure code as described in subclause 5.2.6.

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

###### 4.4.2.2.2.3 Configuration Request for a group of UEs

Upon receipt of the request from the SCS/AS, if the External Group Identifier is included in the configuration request from the SCS/AS, then the monitoring configuration is for a group of UEs. The SCEF shall interact with the HSS via S6t as specified in 3GPP TS 29.336 [11].

Upon receipt of the successful response indicating that group processing is in progress from the HSS before beginning the processing of individual UEs, the SCEF shall,

- for HTTP POST request, create a resource "Individual Monitoring Event Subscription" addressed by a URI that contains the SCS/AS identity and an SCEF-created subscription identifier, store the number of UEs received in the response message from the HSS within the resource and send an HTTP POST response to the SCS/AS including a location header field containing the URI for the created resource and "201 Created" status code to acknowledge the SCS/AS of the successful group processing request.

- for HTTP PUT request, update the active resource "Individual Monitoring Event Subscription" addressed by the requested URL, and send "200 OK" status code to acknowledge the SCS/AS of the successful group processing request.

- for HTTP DELETE request, delete the active resource "Individual Monitoring Event Subscription" addressed by the requested URI and send an HTTP response to the SCS/AS with "204 No Content" status code.

If the SCEF receives a response with an error code from the HSS, the SCEF shall not create, update or delete the resource and shall respond to the SCS/AS with a corresponding failure code as described in subclause 5.2.6.

Upon receipt of the processing result of the individual UEs from the HSS, the SCEF shall perform as follows:

- if no Group Reporting Guard Time is received, the SCEF shall send an HTTP POST request message to the SCS/AS including a reference to the related monitoring subscription, a list of configuration failure result if received for the group members, and the "monitoringEventReports" attribute including a list of monitoring event reports if received for the group members;

- otherwise, the SCEF shall accumulate all of the configuration results and/or monitoring event reports received from the HSS for the group members until the Group Reporting Guard Time expires. Then the SCEF shall send an HTTP POST request message to the SCS/AS including a reference to the related monitoring subscription, and a list of configuration failure result if received for the group members, and the "monitoringEventReports" attribute including a list of monitoring event reports at the Group Reporting Guard Time.

The SCS/AS shall send an HTTP POST response to acknowledge the SCEF about the handling result of the received HTTP POST request.

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

##### 4.4.2.2.3 Monitoring Events Configuration directly via MME/SGSN

The monitoring event Number of UEs in a geographic area is applicable for the monitoring event configuration via MME/SGSN. Only one-time reporting is supported for this event with the value of Maximum Number of Reports indicated by "maximumNumberOfReports" sets to 1.

Upon receipt of the HTTP POST request from the SCS/AS, the SCEF shall

- resolve the location area to the involved SGSN(s)/MME(s) by local configuration;

- interact with the HSS via the S6t interface as specified in 3GPP TS 29.336 [11] if the External Group ID(s) is included; and

- interact with the SGSN(s)/MME(s) via the T6a/b inteface as specified in 3GPP TS 29.128 [12].

NOTE: The SCEF uses local configuration to resolve the involved SGSN(s)/MME(s) if the location area is not received.

After collecting responses from the SGSN(s)/MME(s), if the SCEF does not receive any successful response from the involved SGSN(s)/MME(s), the SCEF shall respond to the SCS/AS with a corresponding failure code as described in subclause 5.2.6; otherwise the SCEF should send 200 OK status code to acknowledge the SCS/AS with one aggregated report in the requested area by including the total count of number of UEs in the "ueCount" attribute and the External Identifier(s) (if available) or the MSISDN(s) (if available) associated with External Group ID.

NOTE: It is possible that the number of UEs does not reflect the actual number of UEs in the designated area (e.g. some SGSN(s)/MME(s) do not respond successfully). The SCEF still provides the result to the SCS/AS if at least one SGSN/MME returns successful response.

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

### 4.4.3 Procedures for resource management of Background Data Transfer

These procedures are used by an SCS/AS to perform the resource management of background data transfer (BDT) to a set of UEs, i.e. the SCS/AS requests a time window and related conditions from the SCEF via the T8 interface.

In order to create a resource for the background data transfer policy, the SCS/AS shall send an HTTP POST message to the SCEF for the "BDT Subscription" resource to negotiate the transfer policy. The body of the HTTP POST message shall include SCS/AS Identifier, Volume per UE (total volume for both DL and UL or separate volume for DL and/or UL), Number of UEs, Desired Time Window and optionally a location area information.

After receiving the HTTP POST message, if the SCS/AS is authorized, the SCEF shall map the SCS/AS Identifier to ASP Identifier and negotiate the transfer policy with the PCRF as defined in 3GPP TS 29.154 [9]. After receiving the response including the determined transfer policies from the PCRF, the SCEF shall create a resource "Individual BDT Subscription" which represents the BDT subscription, addressed by a URI that contains the SCS/AS identifier and an SCEF-created subscription identifier, and shall respond to the SCS/AS with a 201 Created message, including a Location header field containing the URI for the created resource and a message body, which may also include Reference ID and a set of transfer policies. The SCS/AS shall use the URI received in the Location header in subsequent requests to the SCEF to refer to this background data transfer subscription. If the SCEF receives a response with an error code from the PCRF, the SCEF shall not create the resource and shall respond to the SCS/AS with a corresponding failure code as described in subclause 5.2.6.

The SCS/AS may also send an HTTP PUT message to the SCEF for the "Individual BDT Subscription" resource to request starting an update for negotiation of background data transfer policy. The body of the HTTP PUT message shall include data as described in the POST message. The external group identifier shall remain unchanged from previously provided value. After receiving such request, if the SCS/AS is authorized, the SCEF shall negotiate the transfer policy with the PCRF as defined in 3GPP TS 29.154 [9]. After receiving the response including the determined transfer policies from the PCRF, the SCEF shall send an HTTP response to the SCS/AS with a corresponding status code and may include Reference ID and a set of transfer policies. If the SCEF receives a response with an error code from the PCRF, the SCEF shall not update the resource and shall respond to the SCS/AS with a corresponding failure code as described in subclause 5.2.6.

NOTE 1: The SCEF starts a new BDT policy negotiation in the Nt interface by sending the request to the PCRF without the previously associated BDT Reference ID.

If more than one policy is included in the HTTP response, the SCS/AS shall send an HTTP PATCH message to inform the SCEF for the "Individual BDT Subscription" resource of the transfer policy selected by the SCS/AS. After receiving the HTTP PATCH message, the SCEF shall send an HTTP response to the SCS/AS with a corresponding status code and interact with the PCRF as defined in 3GPP TS 29.154 [9]. If the SCEF identifies any error (e.g. selected policy is not within the set of transfer policies), the SCEF shall not update the resource and shall respond to the SCS/AS with a corresponding failure code as described in subclause 5.2.6.

The SCS/AS may also send an HTTP DELETE message to the SCEF for the "Individual BDT Subscription" resource requesting to remove an individual resource identified by the URI received in the response to the request that has created resource a URI. After receiving such request, the SCEF shall delete the resource and send an HTTP response to the SCS/AS with a corresponding status code.

NOTE 2: The SCEF can also remove the resource when the last window end time in transfer policies expires.

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

### 4.4.4 Procedures for changing the chargeable party at session set up or during the session

This procedure is used by an SCS/AS to either request to sponsor the traffic from the beginning or to request becoming the chargeable party at a later point in time via the T8 interface.

When setting up the connection between the AS and UE via the SCEF, the SCS/AS shall send an HTTP POST request to the SCEF for the "Chargeable Party Transactions" resource requesting to become the chargeable party for the session to be set up. The body of the HTTP POST message shall include SCS/AS Identifier, UE IP address, IP Flow description, Sponsor ID, ASP ID, Sponsoring Status, notification destination URI identifying the recipient of notification within the "notificationDestination" attribute and may include time period and/or traffic volume used for sponsoring. The SCS/AS may also request to activate a previously selected policy of background data transfer by including Reference ID in the body of the HTTP POST message.

After receiving the HTTP POST message, if the authorization performed by the SCEF is successful, the SCEF shall act as an AF to interact with the PCRF via the Rx interface as defined in 3GPP TS 29.214 [10] or 3GPP TS 29.201 [13] to trigger a PCRF initiated IP-CAN Session Modification. The SCEF may map the SCS/AS Identifier to AF Application Identifier and may request to be notified about the traffic plane status. If the time period and/or traffic volume are received from the AF, the SCEF should subscribe to the PCRF on the USAGE\_REPORT event.

After receiving a successful response from the PCRF, the SCEF shall create a resource "Individual Chargeable Party Transaction", which represents the chargeable party transaction, addressed by a URI that contains the SCS/AS identity and an SCEF-created transaction identifier, and shall respond to the SCS/AS with a 201 Created message, including a Location header field containing the URI for the created resource. The SCS/AS shall use the URI received in the Location header in subsequent requests to the SCEF to refer to this chargeable party transaction. If the SCEF receives a response with an error code from the PCRF, the SCEF shall not create the resource and respond to the SCS/AS with a corresponding failure code as described in subclause 5.2.6.

In order to update the sponsoring status of an established AS session, the SCS/AS shall send an HTTP PATCH message to the SCEF for the "Individual Chargeable Party Transaction" resource requesting to change Sponsoring Status. When receiving the HTTP PATCH message, the SCEF shall make the change and interact with the PCRF to modify the Rx session as defined in 3GPP TS 29.214 [10] or 3GPP TS 29.201 [13]. After receiving the response with successful result code from the PCRF, the SCEF shall send an HTTP response to the SCS/AS with a 200 OKstatus code and the result in the body of the HTTP response. The accumulated usage received from the PCRF shall be included if the SCS/AS requested to disable the sponsoring. If the SCEF receives a response with an error code from the PCRF, the SCEF shall not update the resource and respond to the SCS/AS with a corresponding failure code as described in subclause 5.2.6.

If the SCEF receives a traffic plane notification (e.g. the usage threshold is reached or transmission resource lost), or if the SCEF gets informed that the Rx session is terminated (e.g. due to a release of PDN connection), the SCEF shall send an HTTP POST message including the notified event (e.g. session terminated) and the accumulated usage to the SCS/AS identified by the notification destination URI received during session setting up. The SCS/AS shall respond with an HTTP response to confirm the received notification.

In order to remove the established AS session, the SCS/AS shall send an HTTP DELETE message to the SCEF for the "Individual Chargeable Party Transaction" resource. After receiving the HTTP DELETE message, the SCEF shall remove all properties of the resource and interact with the PCRF to terminate the Rx session (as defined in 3GPP TS 29.214 [10] or 3GPP TS 29.201 [13]). After receiving the response from the PCRF, the SCEF shall send an HTTP response to the SCS/AS with a corresponding status code and the accumulated usage (if received from the PCRF).

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

##### 4.4.5.3.1 Mobile Terminated NIDD for a single UE

If the SCS/AS needs to perform a downlink non-IP data delivery for a single UE, the SCS/AS shall send an HTTP POST message to the SCEF for the "NIDD downlink data deliveries" resource, identifying an existing NIDD configuration resource as parent resource. The body of the HTTP POST message shall include External Identifier or MSISDN and non-IP data and may include PDN Connection Establishment Option, Reliable Data Service Configuration, Maximum Latency and Priority. The Reliable Data Service Configuration includes port numbers on UE and SCEF that are used to identify a specific application for data transfer between UE and SCS/AS and an indication if reliable data service acknowledgement is enabled or not.

Upon receipt of a HTTP POST request from the SCS/AS for a downlink data delivery for a single UE, the SCEF shall:

- verify the NIDD configuration resource already exists based on the URI passed, if the configuration resource does not exist, the SCEF shall respond a 404 Not Found response to reject the downlink data delivery, and

- check whether the SCS/AS is authorised to send NIDD requests, if not authorized, the SCEF shall respond a 401 Unauthorized response to reject the downlink data delivery, and

- check whether the non-IP packet size is larger than the Maximum Packet Size that was provided to the SCS/AS during NIDD Configuration. If the packet is oversized, the SCEF shall respond a 403 Forbidden response with a cause value "DATA\_TOO\_LARGE" in the "cause" attribute of the "ProblemDetails" structure indicating received non-IP packet size is larger than "maximumPacketSize" of the NIDD configuration.

- if the Rds\_port\_verification feature is supported, check whether the RDS port numbers are within the configured RDS port list. If the RDS port numbers are unknown in the SCEF, the SCEF shall respond a 403 Forbidden response with a cause value "RDS\_PORT\_UNKNOWN" in the "cause" attribute of the "ProblemDetails" structure.

If all above checks are successful, the SCEF shall determine the EPS Bearer Context based on the APN associated with the NIDD configuration and the User Identity. If the SCEF EPS bearer context is not found in the SCEF, depending on PDN Connection Establishment Option received in the POST request or from NIDD configuration, the SCEF may:

- reject the request with an error message to the SCS/AS;

- send a Device Trigger to the UE as described in subclause 4.4.6 without buffering the non-IP data and respond the SCS/AS with a 500 Internal Server Error response; or

- buffer the non-IP data and create the "Individual NIDD downlink data delivery" sub-resource, then send a 201 Created response to the SCS/AS. The response message also includes an indication of whether the Device Trigger procedure (as described in subclause 4.4.6) was performed by the SCEF. A Location header shall be included in the response message that provides the URI of the resource identifying this individual downlink data delivery. The SCS/AS shall use the URI received in the Location header in subsequent requests to the SCEF to refer to this individual downlink data delivery for possible replacement or cancellation. The non-IP data shall be delivered when the non-IP PDN connection is established.

If the SCEF EPS bearer context is found in the SCEF, the SCEF shall check if the SCS/AS has exceeded the quota or rate of data submission considering the number of existing buffered non-IP data and restriction in APN and serving PLMN rate control. If quota is reached, the SCEF shall respond the SCS/AS with a 403 Forbidden response and a cause value "QUOTA\_EXCEEDED" in the "cause" attribute of the "ProblemDetails" structure indicating the reason for the failure condition. If rate limit is reached, the SCEF shall respond the SCS/AS with 429 Too Many Requests.

If the check is passed, the SCEF shall continue the downlink non-IP data delivery procedure as the defined 3GPP TS 29.128 [12].

If the non-IP data delivery was successful, the SCEF shall send a 200 OK response to the HTTP POST request indicating the downlink non-IP data delivery is successful along with the acknowledge information; otherwise the SCEF may:

- send a 500 Internal Server Error and a cause value indicating the reason for the delivery failure; or

- if the MME/SGSN indicates UE is temporary not reachable, either:

1. buffer the non-IP data and and create the "Individual NIDD downlink data delivery" sub-resource, then send a 201 Created response to the SCS/AS. The response may include a Requested Re-Transmission time to indicate the SCS/AS when the UE is expected to be reachable so that the SCEF re-transmits the buffered non-IP data; or

2. send a 500 Internal Server Error response without buffering the non-IP data, and include a cause value "TEMPORARILY\_NOT\_REACHABLE" in the "cause" attribute of the "ProblemDetails" structure indicating the downlink non-IP data delivery is perfomed but stopped since UE is temporarily unreachable. The response may include a Requested Re-Transmission time to indicate the SCS/AS when the UE is expected to be reachable so that the SCS/AS may prepare any re-transmission;

If the MT\_NIDD\_modification\_cancellation feature is supported and the SCS/AS decides to replace the pending downlink data delivery in the SCEF, the SCS/AS shall send an HTTP PUT message to the SCEF, using the URI received in the response to the request that has created the individual downlink data delivery resource. The External Identifier or MSISDN shall remain unchanged from previous values. Upon receipt of the HTTP PUT request from the SCS/AS, the SCEF shall check whether a pending non-IP data exists with the same URI (i.e. resource exists). If it is found, the SCEF shall replace it with the new non-IP data and continue waiting for any message from the MME/SGSN for the UE indicating either the non-IP PDN connection is being established or the UE is reachable (such message may be an MO NIDD); otherwise the SCEF shall respond 409 Conflict with a cause value "SENDING" in the "cause" attribute of the "ProblemDetails" structure indicating replacement failure. If the buffered data is already delivered, the SCEF shall respond with 404 Not Found and include a cause value a cause value "ALREADY\_DELIVERED" in the "cause" attribute of the "ProblemDetails" structure indicating replacement failure.

If the MT\_NIDD\_modification\_cancellation feature is supported and the SCS/AS decides to cancel the pending downlink data delivery in the SCEF, the SCS/AS shall send an HTTP DELETE message to the SCEF, using the URI received in the response to the request that has created the individual downlink data delivery resource. Upon receipt of the HTTP DELETE request from the SCS/AS, the SCEF shall check whether a pending request exists with the same URI. If such non-IP data has not been delivered, the SCEF shall remove the individual downlink data delivery resource and respond with an HTTP 204 No Content response; otherwise the SCEF shall respond with 404 Not Found (i.e. data already delivered) with a cause value "ALREADY\_DELIVERED" in the "cause" attribute of the "ProblemDetails" structure or 409 Conflict (i.e. data delivery ongoing) response with a cause value "SENDING" in the "cause" attribute of the "ProblemDetails" structure, and include a cause value indicating cancellation failure.

If a pending non-IP data is delivered by the SCEF (e.g. due to non-IP PDN connection establishment), and the SCEF gets the delivery result from the MME/SGSN, the SCEF shall remove the "Individual NIDD downlink data delivery" sub-resource and send an HTTP POST message to the SCS/AS, identified by the notification destination URI received during the NIDD configuration, to notify the delivery result for the pending non-IP data. Upon receipt of the request, the SCS/AS shall acknowledge the notification with an HTTP 200 OK or 204 No Content response.

During MT NIDD delivery, if the UE indicates no support for RDS and the SCEF previously indicated RDS is enabled to the SCS/AS, the SCEF shall stop sending the non-IP data and send MT NIDD delivery notification with "FAILURE\_RDS\_DISABLED" delivery status.

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

###### 4.4.7.2.2.1 TMGI Allocation

If the SCS/AS acts as a GCS AS in the application level and if there is no assigned TMGI for an External Group Identifier, the SCS/AS shall send an HTTP message to the SCEF to the resource "TMGI Allocation". The body of the HTTP POST request message shall include the External Group Identifier. The SCS/AS may also include the location information in the body.

Upon receipt of the HTTP POST request from the SCS/AS to allocate a TMGI, the SCEF shall check whether the SCS/AS is authorized to request TMGI allocation. If authorization is successful, the SCEF shall initiate TMGI allocation by the BM-SC as defined in subclause 5.2.1 of 3GPP TS 29.468 [36]. Upon successful allocation of a TMGI, the SCEF shall create the resource which represents the TMGI allocation, addressed by a URI that contains the SCS identity and TMGI, and shall respond to the SCS/AS with a 201 Created message including the TMGI and the TMGI expiration time.

In order to renew the TMGI expiration time, the SCS/AS shall send an HTTP PUT or PATCH message to the SCEF to the resource "Individual TMGI Allocation". Upon receipt of the HTTP PUT or PATCH request from the SCS/AS to renew TMGI expiration time, the SCEF shall initiate TMGI expiration time renewal to the BM-SC as defined in subclause 5.2.1 of 3GPP TS 29.468 [36]. Upon successful result, the SCEF shall update the resource and respond to the SCS/AS by sending an HTTP response with 200 OK including the new TMGI expiration time.

If the SCEF receives the response with an error code from the BM-SC for the allocation of TMGI or renewal of expiration time for the existing TMGI, the SCEF shall not create or update the resource and shall respond to the SCS/AS with a corresponding failure code as described in subclause 5.2.6.

Upon the TMGI expiration, the SCEF may delete the resource of the TMGI locally.

Upon receipt of the notification of TMGI expiration by the BM-SC as defined in subclause 5.2.3 of 3GPP TS 29.468 [36], the SCEF shall delete the resource if not yet deleted.

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

###### 4.4.7.2.2.3 Creation of group message delivery

If the SCS/AS acts as a GCS AS in the application level and if the SCS/AS has an assigned TMGI for the External Group Identifier, in order to perform the group message delivery, the SCS/AS shall sends an HTTP POST request message to the SCEF to the resource "GMD via MBMS by MB2". The body of the HTTP POST request message shall include the External Group Identifier and notification destination URI identifying the recipient of notification within the "notificationDestination" attribute. The SCS/AS may also include the Group Message Payload, the location information and a Message Delivery Start Time in the body.

The SCS/AS may also send an HTTP POST message to the SCEF directly to the resource "TMGI Allocation" without previously requesting TMGI allocation as defined in subclause 4.4.7.2.2. The SCEF shall create the resource "Individual TMGI Allocation" and perform the procedure as define in subclause 4.4.7.2.2, and shall also create resource "GMD via MBMS by MB2" and perform the procedure as mentioned in this subcaluse for MBMS bearer creation.

Upon receipt of the HTTP POST request from the SCS/AS to deliver the group message, the SCEF shall check whether the SCS/AS is authorized to send a group message request. It also checks to see if the Message Delivery Start Time does not start after the TMGI expiration. If authorization is successful, the SCEF shall initiate the Active MBMS Bearer procedure as defined in subclause 5.3.2 of 3GPP TS 29.468 [36] with the difference that the SCEF acts as a GCS AS. The SCEF shall include the location information based on the local configuration if the location information is not provided in the HTTP POST request message.

Upon successful activation of MBMS bearer, the SCEF shall create resource which represents "Individual GMD via MBMS by MB2", addressed by a URI that contains Transaction Id allocated by the SCEF and respond to the SCS/AS by sending an HTTP response with a 201 Created status code, including a Location header field containing the URI for the created resource. When the SCS/AS receives the URI in the Location header, it shall use this URI in subsequent requests to the SCEF to refer to this active MBMS bearer. If the Group Message Payload was not include in the HTTP POST above, the HTTP response sent from the SCEF shall also include the SCEF message delivery Ipv4 address or Ipv6 address and port number.

If the SCEF receives the response with an error code from the BM-SC for the activation of MBMS bearer, the SCEF shall not create the resource and shall respond to the SCS/AS with a corresponding failure code as described in subclause 5.2.6.

If the Group Message Payload was included the HTTP POST above, the SCEF shall deliver to BM-SC the Group Message Payload(s) as defined in 3GPP TS 29.468 [36] at Message Delivery Start Time.

If the Group Message Payload was not include in the HTTP POST above, the SCEF shall transfer the contents received from the SCS/AS to the BM-CS at or after the requested Group Message Start Time, but before the TMGI Expiration time. In this case, when the SCEF detects the group message delivery was triggered successful, the SCEF shall send an HTTP POST request message to the SCS/AS.

NOTE: If Group Message Payload was included, then at Message Delivery Start Time, the SCEF delivers to BM-SC the Group Message Payload(s) to corresponding to MB2-U IP address and port number associated with respective TMGI.

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

###### 4.4.7.2.2.4 Modification of previous submitted group message delivery

If the SCS/AS determines that modification of previous accepted Group Message Delivery Request is required, the SCS/AS shall send an HTTP PATCH or HTTP PUT request message to the SCEF to the resource "Individual GMD via MBMS by MB2". The body of the HTTP PATCH request message shall include the Message Delivery Start Time. The SCS/AS may also include the External Group Identifier, the Group Message Payload and the location information in the body. The body of the HTTP PUT request message shall include the information as the information provided in the HTTP POST in subclause 4.4.7.2.2.2.3. The body of the HTTP PATCH request message shall include the information defined in the data type of GMDViaMBMSByMb2Patch as defined in subclause 5.8.2.1.1.6.

Upon receipt of the HTTP PATCH or HTTP PUT request from the SCS/AS to modify the previous group message delivery subscription, the SCEF shall check whether the SCS/AS is authenticated and authorized to modify the submitted group message delivery. If the authorization is successful, the SCEF shall initiate the Modify MBMS Bearer procedure as defined in subclause 5.3.4 of 3GPP TS 29.468 [36] with the difference that the SCEF acts as a GCS AS. The SCEF shall include the location information based on the local configuration if the location information is not provided in the HTTP PATCH or HTTP PUT request message.

Upon successful modification of MBMS bearer, the SCEF shall update the resource and respond to the SCS/AS with a 200 OK success message indicating that previous group message delivery subscription is successfully updated.

If the SCEF receives the response with an error code from the BM-SC for the modification of MBMS bearer, the SCEF shall not update the resource and shall respond to the SCS/AS with a corresponding failure code as described in subclause 5.2.6.

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

###### 4.4.7.2.3.1 Service Creation

If the SCS/AS acts as a content provider in the application level and if there is no assigned Service ID for an External Group Identifier, the SCS/AS shall send an HTTP POST message to the SCEF to the resource "xMB Services". The body of the HTTP POST request message shall include the External Group Identifier.

Upon receipt of the HTTP POST request from the SCS/AS to create a service, the SCEF shall check whether the SCS/AS is authorized to request service creation. If authorization is successful, the SCEF shall initiate service creation by the BM-SC as defined in subclause 5.2.1.2.2 of 3GPP TS 29.116 [37]. Upon successful service creation, the SCEF shall create the resource which represents the service creation, addressed by a URI that contains the SCS identity and Service Id, and shall respond to the SCS/AS with a 201 Created message which may include the service announcement information.

If the SCEF receives the response with an error status code from the BM-SC for the service creation, the SCEF shall not create or update the resource and shall respond to the SCS/AS with a corresponding failure code as described in subclause 5.2.6.

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

###### 4.4.7.2.3.3 Creation of group message delivery

If the SCS/AS acts as a content provider in the application level, the SCS/AS may sends an HTTP POST request message to the SCEF to the resource "GMD via MBMS by xMB". The body of the HTTP POST request message shall include the External Group Identifier and notification destination URI identifying the recipient of notification within the "notificationDestination" attribute. The SCS/AS may also include the Group Message Payload, the location information, a Message Delivery Start Time and Message Delivery Stop Time in the body.

Upon receipt of the HTTP POST request from the SCS/AS to deliver the group message, the SCEF shall check whether the SCS/AS is authorized to send a group message request. It also checks to see if the Message Delivery Start Time doesn't start after the Message Delivery Stop Time. If authorization is successful, the SCEF shall initiate the Create Session procedure as defined in subclause 4.4.5.2 of 3GPP TS 29.116 [37] and the Update Session procedure as defined in subclause 4.4.5.3 of 3GPP TS 29.116 [37] with the difference that the SCEF acts as a Content Provider, Session Start is set accordiong to the Message Delivery Start Time and the Session Stop is set according to the Message Delivery Stop Time. The SCEF shall include the location information based on the local configuration if the location information is not provided and include the session type set to "Files" in the HTTP POST request message.

Upon successful activation of MBMS bearer, the SCEF shall create resource which represents "Individual GMD via MBMS by xMB ", addressed by a URI that contains Transaction Id allocated by the SCEF and respond to the SCS/AS by sending an HTTP response with a 201 Created status code, including a Location header field containing the URI for the created resource. When the SCS/AS receives the URI in the Location header, it shall use this URI in subsequent requests to the SCEF to refer to this active MBMS bearer. If the Group Message Payload was not included in the HTTP POST above, the HTTP response sent from the SCEF shall also include the SCEF message delivery Ipv4 address or Ipv6 address and port number.

If the SCEF receives the response with an error code from the BM-SC for the activation of MBMS bearer, the SCEF shall not create the resource and shall respond to the SCS/AS with a corresponding failure code as described in subclause 5.2.6.

If the Group Message Payload was included the HTTP POST above, the SCEF shall deliver to BM-SC the Group Message Payload(s) as defined in 3GPP TS 29.468 [36] at Message Delivery Start Time.

If the Group Message Payload was not included in the HTTP POST above, the SCEF shall transfer the contents received from the SCS/AS to the BM-CS at or after the requested Message Delivery Start Time, but before the Message Delivery Stop Time. In this case, when the SCEF detects the group message delivery was triggered successful, the SCEF shall send an HTTP POST request message to the SCS/AS.

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

###### 4.4.7.2.3.4 Modification of previous submitted group message delivery

If the SCS/AS determines that modification of previous accepted Group Message Delivery Request is required, the SCS/AS shall send an HTTP PATCH or HTTP PUT request message to the SCEF to the resource "Individual GMD via MBMS by xMB ". The body of the HTTP PATCH request message shall include the Message Delivery Start Time and Message Delivery Stop Time. The SCS/AS may also include the External Group Identifier, the Group Message Payload and the location information in the body. The body of the HTTP PUT request message shall include the information as the information provided in the HTTP POST in subclause 4.4.7.2.3.3. The body of the HTTP PATCH request message shall include the information defined in the data type of GMDViaMBMSByxMBPatch as defined in subclause 5.8.3.1.1.4.

Upon receipt of the HTTP PATCH or HTTP PUT request from the SCS/AS to modify the previous group message delivery subscription, the SCEF shall check whether the SCS/AS is authenticated and authorized to modify the submitted group message delivery. If the authorization is successful, the SCEF shall initiate the Update Session procedure as defined in subclause 4.4.5.3 of 3GPP TS 29.116 [37] with the difference that the SCEF acts as a Content Provider, Session Start is set accordiong to the Message Delivery Start Time and the Session Stop is set according to the Message Delivery Stop Time. The SCEF shall include the location information based on the local configuration if the location information is not provided in the HTTP PATCH or HTTP PUT request message.

Upon successful modification of MBMS bearer, the SCEF shall respond to the SCS/AS with a 200 OK success message indicating that previous group message delivery subscription is successfully updated.

If the SCEF receives the response with an error code from the BM-SC for the modification of MBMS bearer, the SCEF shall not update the resource and shall respond to the SCS/AS with a corresponding failure code as described in subclause 5.2.6.

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

### 4.4.9 Procedures for Communication Pattern Parameters Provisioning

One or more set of CP parameters may be provisioned by the SCS/AS for a single UE or a group of UEs.

In order to create resources for one or more CP parameter set(s), the SCS/AS shall send an HTTP POST message to the SCEF for the "CP provisioning Subscription" resource, including one or more new provisioned CP parameter set(s). The body of HTTP POST message shall include External Identifier or MSISDN for a single UE or External Group ID for a group of UEs, SCS/AS Identifier and one or more set of CP information associated with CP parameter set Id(s).

After receiving the HTTP POST message, the SCEF shall check if the SCS/AS is authorised. The SCEF may also check if the number of CP parameter sets(s) reaches the limitation based on operator policy or configuration.

After validation, the SCEF shall for each received CP parameter set Id, assign an SCEF Reference ID which may be derived from the CP parameter set Id, and send Update CP Parameter Request message to the HSS for delivering the CP parameter set(s) as specified in 3GPP TS 29.336 [11].

After receiving result from the HSS, if the result is successful, the SCEF shall create a resource "Individual CP Provisioning Subscription" and the corresponding sub-resources "Individual CP set Provisioning" each represents a successfully provisioned CP parameter set indicated by the HSS and respond to the SCS/AS with a 201 Created including Location header field containing the URI for the created subscription resource "Individual CP Provisioning Subscription" and the sub-resource(s) "Individual CP set Provisioning" corresponding to each successful CP parameter set within the "self" attribute in the "cpParameterSet" attribute; otherwise, the SCEF shall not create any resource and shall respond to the SCS/AS with a corresponding failure code as described in subclause 5.2.6. If not all CP parameters sets are provisioned successfully (i.e. the HSS indicates failure for some or all CP parameter sets and/or the SCEF does not accept the CP parameter provisioning (e.g. one or more CP Set Identifiers in the request are already present in existing subscriptions)), the SCEF shall also include CP report(s) within attribute "cpReports" with a list of failed CP Set Identifier(s) and the corresponding failure code as specified in table 5.10.2.3.5-1 in the body of the HTTP response.

In order to add new CP parameter set(s), update and/or remove the existing CP parameter set(s) for one or more CP parameter set Id(s), the SCS/AS may send an HTTP PUT message to the SCEF for the "Individual CP Provisioning Subscription" resource requesting to add new CP parameter set(s) by creating new resource(s), change some created properties (e.g. Validity Time) of the existing resource(s), and/or remove some or entire properties of the existing resource(s). After receiving the HTTP PUT message, the SCEF shall send the CP parameter changes to the HSS as specified in 3GPP TS 29.336 [11]. After receiving the response from the HSS with a successful code, if the HSS indicates all CP parameter sets or some CP parameter sets are provisioned successfully, the SCEF shall create or update the corresponding sub-resource(s) "Individual CP set Provisioning" each represents a successfully provisioned CP parameter set indicated by the HSS and send an HTTP response to the SCS/AS with a 200 OK status code and include a list of successful CP parameter set(s) in the body of the HTTP response. Otherwise, the SCEF shall not create or update the resource(s) and shall send an HTTP response to the SCS/AS with a corresponding failure code as described in subclause 5.2.6. If not all CP parameters sets are provisioned successfully (i.e. the HSS indicates failure for some or all CP parameter sets and/or the SCEF does not accept the CP parameter provisioning (e.g. one or more CP Set Identifiers in the request are already present in existing subscriptions)), the SCEF shall also include CP report(s) within attribute "cpReports" with a list of failed CP Set Identifier(s) and the corresponding failure code as specified in table 5.10.2.3.5-1 in the body of the HTTP response.

The SCS/AS may send a HTTP PUT message to the SCEF for the "Individual CP set Provisioning" resource requesting to replace an individual resource identified by the CP parameter set Id. The body of the HTTP PUT message shall include set of CP information. After receiving such request, the SCEF shall interact with the HSS as specified in 3GPP TS 29.336 [11]. After receiving the response from the HSS with a successful code, the SCEF shall update the resource and send an HTTP response to the SCS/AS with a 200 OK status code; otherwise, the SCEF shall not update the resource and shall send an HTTP response to the SCS/AS with a corresponding failure code as described in subclause 5.2.6. If the provisioning of the CP set fails (i.e. the HSS returns failure for the CP set or the SCEF does not accept the CP set provisioning), the SCEF shall reject the request with a corresponding status code, and include the attribute "cpReports" with the corresponding failure code as specified in table 5.10.2.3.5-1 and the CP Set Identifier for which the provisioning has failed.

The SCS/AS may send an HTTP DELETE message to the SCEF requesting to delete an individual CP set resource "Individual CP set Provisioning". After receiving such request, the SCEF shall determine the SCEF Reference ID for Deletion associated with the CP parameter set Id, and interact with the HSS as specified in 3GPP TS 29.336 [11]. After receiving the response from the HSS, the SCEF shall delete the addressed resource and send an HTTP response to the SCS/AS with a 204 No Content status code.

The SCS/AS may send an HTTP DELETE message to the SCEF requesting to delete an individual subscription resource "Individual CP Provisioning Subscription". After receiving such request, the SCEF shall determine the SCEF Reference ID (s) for Deletion associated with the CP parameter set Id(s) and interact with the HSS as specified in 3GPP TS 29.336 [11]. After receiving the response from the HSS, the SCEF shall delete the addressed resource and its sub-resources addressed by "Individual CP set Provisioning" and send an HTTP response to the SCS/AS with a 204 No Content status code.

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

### 4.4.10 Procedures for PFD Management

The PFDs associated with application identifier(s) may be created, updated or removed by the third party SCS/AS as defined in 3GPP TS 23.682 [2].

In order to create PFDs resources for one or more external Application Identifier(s), the SCS/AS shall send an HTTP POST message to the request URI of the resource "PFD Management Transactions" including one or more set of PFDs for external Application Identifier(s). The body of the HTTP POST message shall include external Application Identifier(s) and PFDs associated with its PFD Identifier(s), an Allowed Delay may be included for the external Application Identifier(s) as well.

After receiving the HTTP POST message, if the SCS/AS is authorized, the SCEF shall provision the PFDs to the PFDF as defined in 3GPP TS 29.250 [26]. When receiving the response from the PFDF, the SCEF shall send an HTTP response to the SCS/AS with a corresponding status code. If one or more external application identifiers are provisioned successfully, the SCEF shall create an "Individual PFD Management Transaction" resource for the request and he corresponding sub-resources "Individual Application PFD Management" each represents a successfully provisioned external application identifier. The SCEF shall respond to the SCS/AS with a 201 Created including Location header field containing the URI for the created transaction resource "Individual PFD Management Transaction" and the sub-resource(s) "Individual Application PFD Management" corresponding to each external application identifier within the "self" attribute in the "PfdData" data type, the SCEF shall also include PFD report(s) with a list of external Application Identifier(s) and result(s) in the body of the HTTP response if some application(s) are not provisioned successfully (i.e. the PFDF returns failure and/or the SCEF does not accept the PFD provisioning (e.g. one or more external Application Identifiers in the request are already present in existing transactions)).

In order to update the PFDs for an existing individual transaction, the SCS/AS shall send an HTTP PUT message to URI of the resource "Individual PFD Management Transaction" including one or more set of PFDs for external Application Identifier(s). After receiving the HTTP PUT message, the SCEF shall make the change and send the change to the PFDF (i.e. add/update/remove PFDs) as defined in 3GPP TS 29.250 [26]. After receiving the response from the PFDF, the SCEF shall send an HTTP response to the SCS/AS with a corresponding status code. The SCEF shall create or update the corresponding sub-resource(s) "Individual Application PFD Management" each represents a successfully provisioned external application identifier, and also include PFD report(s) with a list of external Application Identifier(s) and result(s) in the body of the HTTP response if some application(s) are not provisioned successfully (i.e. the PFDF returns failure and/or the SCEF does not accept the PFD provisioning (e.g. one or more external Application Identifiers in the request are already present in existing transactions)).

NOTE 1: When the PUT for "Individual PFD Management Transaction" is received in the SCEF, SCEF can use partial update or full update towards the PFDF.

In order to remove the PFDs for an existing individual transaction, the SCS/AS shall send an HTTP DELETE message to the URI of the resource "Individual PFD Management Transaction". After receiving such request, the SCEF shall delete the "Individual PFD Management Transaction" resource and its "Individual Application PFD Management" sub-resouce(s), and shall interact with the PFDF as defined in 3GPP TS 29.250 [26]. After receiving the response from the PFDF, the SCEF shall send an HTTP response to the SCS/AS with a corresponding status code.

For the POST message to the resource "PFD Management Transactions" or the PUT message to the resource "Individual PFD Management Transaction", if the provisioning of all application(s) fails (i.e. the PFDF returns failure and/or the SCEF does not accept the PFD provisioning), the SCEF shall respond with 500 Internal Server Error status code, and include the attribute "pfdReports" with the corresponding failure reason as specified in table 5.11.2.2.3-1 and the external Application Identifier(s) for which the provisioning has failed.

In order to update the PFDs for an existing external Application Identifier, the SCS/AS shall send an HTTP PUT message to the resource "Individual Application PFD Management" to update the full set of PFDs of an existing resource. After receiving the HTTP PUT message, the SCEF shall make the change and send the change to the PFDF (i.e. add/update/remove PFDs) as defined in 3GPP TS 29.250 [26]. After receiving the response from the PFDF, the SCEF shall send an HTTP response to the SCS/AS with a corresponding status code.

NOTE 2: When the PUT for "Individual Application PFD Management" is received in the SCEF, SCEF can use partial update or full update towards the PFDF.

In order to update the PFDs for an existing external Application Identifier, the SCS/AS may also send an HTTP PATCH message to URI of the resource "Individual Application PFD Management" to partially update PFDs. After receiving the HTTP PATCH message, the SCEF shall make the change and send the change to the PFDF (i.e. add/update/remove PFDs) as defined in 3GPP TS 29.250 [26]. After receiving the response from the PFDF, the SCEF shall send an HTTP response to the SCS/AS with a corresponding status code.

In order to remove the PFDs for an existing individual application, the SCS/AS shall send an HTTP DELETE message to the resource "Individual Application PFD Management". After receiving such request, the SCEF shall delete the resource and interact with the PFDF as defined in 3GPP TS 29.250 [26]. After receiving the response from the PFDF, the SCEF shall send an HTTP response to the SCS/AS with a corresponding status code.

For the PUT/PATCH message to the resource "Individual Application PFD Management", if the provisioning of the application fails (i.e. the PFDF returns failure or the SCEF does not accept the PFD provisioning), the SCEF shall reject the request with a corresponding status code, and include the attribute "pfdReports" with the corresponding failure code as specified in table 5.11.2.2.3-1 and the external Application Identifier for which the provisioning has failed.

If the SCEF receives PFD management notification including the PFD failure report from the PFDF (as defined in 3GPP TS 29.250 [26]) and if the feature PfdMgmtNotification is supported, the SCEF shall notify the SCS/AS with an HTTP POST message, identified by the notification destination URI received during the PFD provisioning, to notify the failure result for the PFD management by including the PfdReport data type in the body of the message. Within the PfdReport data type, the SCEF shall include the impacted application id(s) within the "externalAppIds" attribute, the "failureCode" attribute set to "PARTIAL\_FAILURE". In addition, if the SCEF receives the location area(s) of PCEF/TDF(s) which are unable to enforce the PFD(s) from the PFDF, the SCEF shall include the location area(s) within the "locationArea" attribute of the PFD report(s). After receiving the HTTP POST message, the SCS/AS shall send a HTTP response with "204 No Content" status code.

NOTE 3: How the SCS/AS reacts to the failed PFD provisioning is left to implementation.

NOTE 4: The SCEF maps the 3GPP network area(s) to the geographic area(s) or civic address(es) if the 3GPP network area(s) is not allowed to be exposed to the 3rd party according to the operator policy.

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

### 4.4.11 Procedures for Enhanced Coverage Restriction Control

The procedures are used by an SCS/AS to query the status of, or to configure the enhanced coverage restriction for a UE via the T8 interface as defined in 3GPP TS 23.682 [2].

In order to query the current status of enhanced coverage restriction, the SCS/AS shall send an HTTP POST message to the SCEF using the query custom operation as defined in subclause 5.12.13.2. The body of the HTTP POST message shall include External Identifier or MSISDN.

In order to configure the enhanced coverage restriction, the SCS/AS shall send an HTTP POST message to the SCEF using the configure custom operation as defined in subclause 5.12.13.3. The body of the HTTP POST message shall include External Identifier or MSISDN and the Enhanced Coverage Restriction setting (i.e. allowed-PLMN-List or restricted-PLMN-List).

Upon receiving the HTTP POST message from the SCS/AS, the SCEF shall check:

- if the SCS/AS is authorized to perform the request. If not the SCEF shall respond to the SCS/AS with a status code set to 401 Unauthorized.

- if the request is malformed. If it is malformed, the SCEF shall respond to the SCS/AS with a status code set to 400 Bad Request.

- if the SCS/AS has exceeded its quota of submitting requests. If so the SCEF shall respond to the SCS/AS with a status code set to 403 Forbidden and may indicate the failure reason "QUOTA\_EXCEEDED" (i.e. the quota exceeded) within the "cause" attribute of the "ProblemDetails" structure in the HTTP POST response.

- if the SCS/AS has exceeded its rate of submitting requests. If so the SCEF shall respond to the SCS/AS with a status code set to 429 Too Many Requests in the HTTP POST response.

The SCEF shall send a Configuration Information Request to the HSS to query or configure the setting of Enhanced Coverage Restriction as defined in 3GPP TS 29.336 [11].

Upon receipt of the response from the HSS, the SCEF shall send an HTTP response to the SCS/AS with a 200 OK message for query or configure custom operation and include the Enhanced Coverage Restriction Data from HSS into the HTTP response.

If the SCEF receives a response with an error code from the HSS, the SCEF shall respond to the SCS/AS with a corresponding failure code as described in subclause 5.2.6.

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

#### 4.4.12.2 Configuration Request for an individual UE

If the configuration request from the SCS/AS is for an individual UE, the SCEF shall send the Configuration Information Request command to the HSS via S6t as defined in 3GPP TS 29.336 [11].

Upon receipt of the response from the HSS, the SCEF shall,

- for the HTTP POST message, create a new resource "Individual NP Configuration" addressed by a URI that contains the SCS/AS identifier and an SCEF-created configuration identifier, and send an HTTP POST response to the SCS/AS with "201 Created" status code, the final suggested configuration parameter(s) (if modified), the indication(s) for the discarded parameter(s) (if discarded), and a location header field containing the URI for the created resource.

- for the HTTP PUT or PATCH message, update the active resource "Individual NP Configuration", and send an HTTP response to the SCS/AS with "200 OK" status code, the final suggested network parameter(s) (if modified), the indication(s) for the discarded parameter(s) (if discarded).

If the SCEF receives a response with an error code from the HSS, the SCEF shall not create or update the resource and shall respond to the SCS/AS with a corresponding failure code as described in subclause 5.2.6.

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

#### 4.4.12.3 Configuration Request for a group of UEs

If the configuration request from the SCS/AS is for a group of UEs, the SCS/AS shall provide the Notification Destination Address, the SCEF shall send the Configuration Information Request command to the HSS via S6t as defined in 3GPP TS 29.336 [11].

Upon receipt of the successful response indicating that group processing is in progress from the HSS before beginning the processing of individual UEs, the SCEF shall,

- for the HTTP POST message, create a resource "Individual NP Configuration" addressed by a URI that contains the SCS/AS identity and an SCEF-created configuration identifier. The SCEF shall send an HTTP POST response to the SCS/AS including a location header field containing the URI for the created resource and a "201 Created" status code to acknowledge the SCS/AS of the successful group processing request.

- for the HTTP PUT or PATCH message, update the resource "Individual NP Configuration" addressed by the requested URL, and shall send "200 OK" status code to acknowledge the SCS/AS of the successful group processing request in the HTTP response message.

If the SCEF receives a response with an error code from the HSS, the SCEF shall not create or update the resource and shall respond to the SCS/AS with a corresponding failure code as described in subclause 5.2.6.

Upon receipt of the processing result of the individual UEs from the HSS, the SCEF shall send an HTTP POST request message with a reference to the related network parameter configuration and a list of processing result for the group members to the SCS/AS.

The SCS/AS shall send an HTTP response to acknowledge the SCEF about the handling result of the received request.

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

### 4.4.13 Procedures for setting up an AS session with required QoS

This procedure is used to set up an AS session with required QoS for the service as defined in 3GPP TS 23.682 [2].

For initial AS session creation, the SCS/AS shall send an HTTP POST message to the SCEF for the "AS Session with Required QoS Subscriptions" resource. The body of HTTP POST message shall include SCS/AS Identifier, UE IP address, IP Flow description, QoS reference and notification destination address. And it may also include time period and/or traffic volume for sponsored data connectivity purpose.

After receiving the HTTP POST message, the SCEF shall authorize the request and may check if the total number of requested QoS reference has exceeded the limit for the SCS/AS. If the authorization is successful, the SCEF shall map the SCS/AS Identifier to AF Application Identifier, and if required, map the SCS/AS Identifier to ASP Identity and Sponsor Identity.

NOTE 1: Before the QoS reference is mapped to Rx parameters, the SCEF can perform a mapping from the name space of the 3rd party SCS/AS to the name space of the operator.

NOTE 2: The QoS reference referring to pre-defined QoS information in the SCEF can be mapped to media component descriptions (e.g. bandwidth, media type) according to SLA.

If the authorization performed by the SCEF is successful, then the SCEF shall act as an AF to interact with the PCRF via the Rx interface as defined in 3GPP TS 29.214 [10] or 3GPP TS 29.201 [13] and trigger a PCRF initiated IP-CAN Session Modification. The SCEF shall also request to be notified about the transmission resource status, i.e. INDICATION\_OF\_SUCCESSFUL\_RESOURCES\_ALLOCATION, INDICATION\_OF\_RELEASE\_OF\_BEARER, INDICATION\_OF\_FAILED\_RESOURCES\_ALLOCATION, and optionally INDICATION\_OF\_LOSS\_OF\_BEARER and INDICATION\_OF\_RECOVERY\_OF\_BEARER. If the time period and/or traffic volume are received from the AF, the SCEF should subscribe to the PCRF on the USAGE\_REPORT event.

The SCEF, after receiving the AAA message over the Rx interface from the PCRF with successful result code, shall create a resource "Individual AS Session with Required QoS Subscription" which represents AS session, addressed by a URI that contains the SCS/AS identity and an SCEF-created AS session identifier, and shall respond to the SCS/AS with a 201 Created message, including the result in the body of the HTTP response and a Location header field containing the URI for the created resource. The SCS/AS shall use the URI received in the Location header in subsequent requests to the SCEF to refer to this AS session. Otherwise, the SCEF shall send an HTTP response to the SCS/AS with a corresponding status code and include the result in the body of the HTTP response. If the SCEF receives a response with an error code from the PCRF, the SCEF shall not create the resource and respond to the SCS/AS with a corresponding failure code as described in subclause 5.2.6.

In order to update the established AS session, the SCS/AS may send an HTTP PUT message to the SCEF for the "Individual AS Session with Required QoS Subscription" resource requesting to replace all properties in the existing resource, addressed by the URI received in the response to the request that has created the resource. The UE IP address shall remain unchanged from previously provided values. After receiving such message, the SCEF shall make the change and interact with the PCRF to modify the Rx session (as defined in 3GPP TS 29.214 [10] or 3GPP TS 29.201 [13]). After receiving the response with successful result code from the PCRF, the SCEF shall replace all properties of the existing resource, send an HTTP response to the SCS/AS with a corresponding status code, and include the result in the body of the HTTP response. If the SCEF receives a response with an error code from the PCRF, the SCEF shall not update the resource and respond to the SCS/AS with a corresponding failure code as described in subclause 5.2.6.

The SCS/AS may also send an HTTP PATCH message to the SCEF for the "Individual AS Session with Required QoS Subscription" resource requesting to change some created properties (e.g. Flow Description). After receiving the HTTP PATCH message, the SCEF shall make the change and interact with the PCRF to modify the Rx session (as defined in 3GPP TS 29.214 [10] or 3GPP TS 29.201 [13]). After receiving the response from the PCRF, the SCEF shall send an HTTP response to the SCS/AS with a corresponding status code and include the result in the body of the HTTP response.

If the SCEF receives a traffic plane notification (e.g. the usage threshold is reached or transmission resource lost), or if the SCEF gets informed that the Rx session is terminated (e.g. due to a release of PDN connection), the SCEF shall send an HTTP POST message including the notified event (e.g. session terminated) and the accumulated usage (if received from the PCRF) to the callback URI "notificationUri" provided by the SCS/AS during the creation of individual AS Session with Required QoS Subscription. The SCS/AS shall respond with an HTTP response to confirm the received notification.

In order to remove the established AS session, the SCS/AS shall send an HTTP DELETE message to the SCEF for the "Individual AS Session with Required QoS Subscription" resource. After receiving the HTTP DELETE message, the SCEF shall remove all properties and interact with the PCRF to terminate the Rx session (as defined in 3GPP TS 29.214 [10] or 3GPP TS 29.201 [13]). After receiving the response from the PCRF, the SCEF shall send an HTTP response to the SCS/AS with a corresponding status code and include the accumulated usage (if received from the PCRF).

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