**3GPP TSG-CT WG4 Meeting #111-eC4-224xxx**

**E-Meeting, 18th – 26th August 2022 *Revision of C4-224295***

|  |
| --- |
| *CR-Form-v12.2* |
| **CHANGE REQUEST** |
|  |
|  | **29.500** | **CR** | **0351** | **rev** | **1** | **Current version:** | **17.7.0** |  |
|  |
| *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:***  | API version in URI setting in indirect communication |
|  |  |
| ***Source to WG:*** | Huawei |
| ***Source to TSG:*** | CT4 |
|  |  |
| ***Work item code:*** | SBIProtoc16 |  | ***Date:*** | 2022-08-26 |
|  |  |  |  |  |
| ***Category:*** | A |  | ***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-16 (Release 16)Rel-17 (Release 17)Rel-18 (Release 18)Rel-19 (Release 19)* |
|  |  |
| ***Reason for change:*** | For Indirect Communications with or without delegated discovery, when sending a request to the SCP, the NF service consumer will set the ":path" in pseudo-headers with the real path of the target URI, including the **<apiName>/<apiVersion>/<apiSpecificResourceUriPart>.**The NF service consumer may include the preferred-api-versions query parameter in "3gpp-Sbi-Discovery-\*" headers to indicate the SCP to select a target NF instance that supports the indicated API versions.To avoid the mismatch of the API major version supported by the selected NF, and the major version included in the target URI, the NF service consumer shall include the major version same as the one in the target URI in the preferred-api-versions query parameter.If no NF profile is found matching the MAJOR version included in the received target URI, the SCP shall reject the service request message with a reason indicates the error. The NF service consumer may retry the service request with a different MAJOR version. |
|  |  |
| ***Summary of change:*** | Include the definition on how to set the API major version in preferred-api-versions query parameter during Indirect Communications with delegated discovery. |
|  |  |
| ***Consequences if not approved:*** | Incorrect major version in the preferred-api-versions query parameter may cause procedure failure. |
|  |  |
| ***Clauses affected:*** | 5.2.7.4, 6.10.2.4 |
|  |  |
|  | **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's revision history:*** |  |

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

#### 5.2.7.4 SCP/SEPP

The SCP or SEPP shall be able to forward the HTTP status codes defined in Table 5.2.7.2-1 from HTTP Server to HTTP client. In addition, it shall be able to generate HTTP status codes to indicate failures during indirect communication (e.g. see clauses 6.10.3.2 and 6.10.6), error handling (see clause 6.10.8), detection and handling of loop path (see clause 6.10.10) and SCP or SEPP overload control (see clause 6.4) as defined in Table 5.2.7.4-1 and Table 5.2.7.4-2.

If the SCP or SEPP detects a loop in the routing path of an HTTP request, it should reject the request with the HTTP status code "400 Bad Request (MSG\_LOOP\_DETECTED)".

If the received HTTP request contains payload body larger than the SCP or SEPP is able to process, the SCP or SEPP shall reject the HTTP request with the HTTP status code "413 Payload Too Large".

An HTTP status code "429 Too Many Requests (NF\_CONGESTION\_RISK)" is sent, when the SCP or SEPP detects that a given NF Service Consumer is sending excessive traffic which, if continued over time, may lead to (or may increase) an overload situation in the SCP or SEPP. If the SCP or SEPP decides to redirect HTTP requests to another less loaded SCP or SEPP, it may send the HTTP status code "307 Temporary Redirect" or "308 Permanent Redirect" with the cause attribute set to "SCP\_REDIRECTION" (see clause 6.10.9) / "SEPP\_REDIRECTION" as defined in Table 5.2.7.4-2.

The SCP or SEPP should map status codes to the most similar 3xx/4xx/5xx HTTP status code specified in Table 5.2.7.4-1 and Table 5.2.7.4-2. If no such code is applicable, it should use "400 Bad Request" status code for errors caused by client side or "500 Server Internal Error" status code for errors caused on server side.

Table 5.2.7.4-1: Protocol and application errors generated by the SCP/SEPP

|  |  |  |
| --- | --- | --- |
| Protocol or application Error | HTTP status code | Description |
| INVALID\_API | 400 Bad Request | The HTTP request contains an unsupported API name or API version in the URI. |
| INVALID\_MSG\_FORMAT | 400 Bad Request | The HTTP request has an invalid format. |
| INVALID\_QUERY\_PARAM | 400 Bad Request | The HTTP request contains an unsupported query parameter in the URI. (NOTE 1) |
| MANDATORY\_QUERY\_PARAM\_INCORRECT | 400 Bad Request | A mandatory query parameter, or a conditional query parameter but mandatory required, for an HTTP method was received in the URI with semantically incorrect value. (NOTE 1) |
| OPTIONAL\_QUERY\_PARAM\_INCORRECT | 400 Bad Request | An optional query parameter for an HTTP method was received in the URI with a semantically incorrect value that prevents successful processing of the service request. (NOTE 1) |
| MANDATORY\_QUERY\_PARAM\_MISSING | 400 Bad Request | Query parameter which is defined as mandatory, or as conditional but mandatory required, for an HTTP method is not included in the URI of the request. (NOTE 1) |
| MANDATORY\_IE\_INCORRECT | 400 Bad Request | A mandatory IE (within a variable part of an "apiSpecificResourceUriPart" or within an HTTP header), or conditional IE but mandatory required, for an HTTP method was received with a semantically incorrect value. (NOTE 1)  |
| OPTIONAL\_IE\_INCORRECT | 400 Bad Request | An optional IE (within an HTTP header) for an HTTP method was received with a semantically incorrect value that prevents successful processing of the service request. (NOTE 1) |
| MANDATORY\_IE\_MISSING | 400 Bad Request | A mandatory IE (within the variable part of an "apiSpecificResourceUriPart" or within an HTTP header), or conditional IE but mandatory required, for an HTTP method is not included in the request. (NOTE 1) |
| UNSPECIFIED\_MSG\_FAILURE | 400 Bad Request | The request is rejected due to unspecified client error. (NOTE 2) |
| NF\_DISCOVERY\_FAILURE | 400 Bad Request | The request is rejected by the SCP because no NF Service Producer can be found matching the NF service discovery factors (see clause 6.10.6). |
| INVALID\_DISCOVERY\_PARAM | 400 Bad Request | The request is rejected by the SCP because it contains an unsupported discovery parameter (i.e. unknown 3gpp-Sbi-Discovery-\* header) (see clause 6.10.3.2).(NOTE 1) |
| MSG\_LOOP\_DETECTED | 400 Bad Request | The request is rejected because message loop is detected. |
| MISSING\_ACCESS\_TOKEN\_INFO | 400 Bad Request | The request is rejected due to missing information in the service request that prevents the SCP from requesting an access token to the Authorization Server. See clause 6.10.3.5. |
| VERSION\_NOT\_SUPPORTED | 400 Bad Request | The request is rejected by the SCP because no NF Service Producer can be found matching the MAJOR version received in the URI of the service request message. See clause 6.10.3.2. |
| ACCESS\_TOKEN\_DENIED | 403 Forbidden | The request is rejected due to the Authorization Server rejecting to grant an access token to the SCP. See clause 6.10.3.5. |
| PLMNID\_MISMATCH | 403 Forbidden | The request is rejected by the SEPP due to the PLMN ID in the bearer token carried in the "Authorization" header of the reconstructed message does not match the PLMN ID of the N32-f context. |
| REQUESTED\_PURPOSE\_NOT\_ALLOWED | 403 Forbidden | The request is rejected due to requested purpose provided in the HTTP request is not allowed by the policy. See clause 6.14. |
| INCORRECT\_LENGTH | 411 Length Required | The request is rejected due to incorrect value of a Content-length header field. |
| NF\_CONGESTION\_RISK | 429 Too Many Requests | The request is rejected due to excessive traffic which, if continued over time, may lead to (or may increase) an overload situation. |
| INSUFFICIENT\_RESOURCES | 500 Internal Server Error | The request is rejected due to insufficient resources. |
| UNSPECIFIED\_NF\_FAILURE | 500 Internal Server Error | The request is rejected due to unspecified reason at the SCP or SEPP. (NOTE 3) |
| SYSTEM\_FAILURE | 500 Internal Server Error | The request is rejected due to generic error condition in the SCP or SEPP. |
| NF\_FAILOVER | 500 Internal Server Error | The request is rejected by the SCP due to the unavailability of the NF, and the requester may trigger an immediate re-selection of an alternative NF based on this information. |
| NF\_SERVICE\_FAILOVER | 500 Internal Server Error | The request is rejected by the SCP due to the unavailability of the NF service, and the requester may trigger an immediate re-selection of an alternative NF service based on this information. |
| MAX\_SCP\_HOPS\_REACHED | 502 Bad Gateway | The request is rejected due to the maximum number of allowed SCP hops has been reached when relaying the request message to the target NF. |
| NF\_DISCOVERY\_ERROR | 502 Bad Gateway | The request is rejected due to the receipt of an 5xx or 429 response from the NRF during an NF Discovery procedure the SCP initiated to fulfil the request.  |
| NF\_CONGESTION | 503 Service Unavailable | The SCP or SEPP experiences congestion and performs overload control, which does not allow the request to be processed. (NOTE 4) |
| TIMED\_OUT\_REQUEST | 504 Gateway Timeout | The request is rejected due a request that has timed out at the HTTP client (see clause 6.11.2).  |
| TARGET\_NF\_NOT\_REACHABLE | 504 Gateway Timeout | The request is not served as the target NF is not reachable (see clause 6.10.8.2). |
| NRF\_NOT\_REACHABLE | 504 Gateway Timeout | The request is not served due to the NRF being unreachable (see clause 6.10.8.2). |
| NOTE 1: "invalidParams" attribute shall be included in the "ProblemDetails" data structure indicating unsupported, missing or incorrect IE(s) or 3gpp-Sbi-Discovery-\* header(s).NOTE 2: This application error indicates error in the HTTP request and there is no other application error value that can be used instead.NOTE 3: This application error indicates error condition in the SCP/SEPP and there is no other application error value that can be used instead.NOTE 4: If the reason for rejection is a temporary overload, the SCP/SEPP may include in the response a Retry-After header field to indicate how long the service is expected to be unavailable. |

Table 5.2.7.4-2: Redirect responses generated by the SCP/SEPP

|  |  |  |
| --- | --- | --- |
| Cause value | HTTP status code | Description |
| SCP\_REDIRECTION | 307 Temporary Redirect308 Permanent Redirect | The request is redirected to a different SCP (see clause 6.10.9).  |
| SEPP\_REDIRECTION | 307 Temporary Redirect308 Permanent Redirect | The request is redirected to a different SEPP (see clause 6.10.9). |

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

#### 6.10.3.2 Conveyance of NF Discovery Factors

When the NF service consumer is configured to use delegated service discovery, it shall include in the HTTP/2 request message the necessary NF service discovery factors to be used by the SCP to perform the NF service discovery procedures and the Service access authorization procedures (see clause 13.4.1.3.2 of 3GPP TS 33.501 [17]) on behalf of the NF service consumer. The latter shall convey these NF service discovery factors using the"3gpp-Sbi-Discovery-\*" request headers. How to set the values of these "3gpp-Sbi-Discovery-\*" request headers is detailed in clause 5.2.3.2.7. The NF service consumer should also include at least the target NF type and service name in the corresponding "3gpp-Sbi-Discovery-\*" request header(s) in its request to the SCP. The NF service consumer may indicate the NRF to use, e.g. as a result of an NSSF query, by including the 3gpp-Sbi-Nrf-Uri header with the NRF API URIs.

If the NF service consumer delegates the reselection of a target NF service instance to the SCP (see clause 6.5 of 3GPP TS 23.527 [38]), the NF service consumer shall also include "3gpp-Sbi-Discovery-\*" headers in an HTTP/2 request targeting an existing resource context in the NF service producer, if the "3gpp-Sbi-Routing-Binding" header is not included in the HTTP/2 request message (e.g. when no binding information was received from the NF service producer during the resource creation, or if the NF service consumer does not support the binding procedures), to enable the SCP to reselect an NF service producer instance, e.g. if the NF service producer instance indicated in the "3gpp-Sbi-Target-apiRoot" header or target URI is not reachable. Additionally, regardless of whether a 3gpp-Sbi-Routing-Binding" header is included or not in the HTTP/2 request message, the NF service consumer should include at least the target NF type and the service name in the corresponding "3gpp-Sbi-Discovery-\*" request header(s) in its request to the SCP.

NOTE 1: Other 3gpp-Sbi-Discovery-\*" request header(s) can also be included in any service request sent to an SCP, regardless of whether the 3gpp-Sbi-Routing-Binding" header is included or not in the HTTP/2 request message, to convey requester's information necessary for the NRF to validate whether the requester is allowed to discover and access a given NF (see NOTE 12 of Table 6.2.3.2.3.1-1 of 3GPP TS 29.510 [8]).

NOTE 2: A request including a 3gpp-Sbi-Routing-Binding header needs not include the requested S-NSSAI in the corresponding 3gpp-Sbi-Discovery-\*" request header, since if the NF service producer supports different sets of NF service instances serving different network slices, the NF Service Set ID in the binding indicaton is available for reselecting an NF service instance (see clauses 5.2.3.2.5 and 6.12.1).

If the NF service consumer includes more than one service name in the 3gpp-Sbi-Discovery-service-names header, the service name corresponding to the service request shall be listed as the first service name in the header.

NOTE 3: The SCP can assume that the service request corresponds to the first service name in the header.

An NF service consumer should also include "3gpp-Sbi-Discovery-\*" headers in an HTTP/2 request targeting an existing resource context in the NF service producer to enable the SCP to perform the Service access authorization procedures (see clause 13.4.1.3.2 of 3GPP TS 33.501 [17]).

Likewise, an NF service producer may also include 3gpp-Sbi-Discovery-\*" headers in a notification or callback request, if the "3gpp-Sbi-Routing-Binding" header is not included in the HTTP/2 request message, to enable the SCP to reselect a different NF service consumer instance, e.g. if the NF service consumer instance indicated in the "3gpp-Sbi-Target-apiRoot" header or target URI is not reachable. Additionally, regardless of whether a 3gpp-Sbi-Routing-Binding header is included or not in the HTTP/2 request message, the NF service producer should include at least the target NF type (i.e. the type of the NF service consumer) in the corresponding "3gpp-Sbi-Discovery-\*" request header(s) in its request to the SCP, if available. See clause 6.6 of 3GPP TS 23.527 [38].

When the 3gpp-Sbi-Selection-Info header is included in a HTTP request message and if the SCP supports this header, the SCP shall use it together with 3gpp-Sbi-Routing-Binding or 3gpp-Sbi-Discovery-\* heads whichever available.

Based on SCP configuration, an SCP deciding to address a next-hop SCP for a service request may delegate the NF instance and/or service instance discovery and selection to subsequent SCPs, in which case it shall forward the "3gpp-Sbi-Discovery-\*" request headers to the next-hop SCP.

When receiving a request containing "3gpp-Sbi-Discovery-\*" request headers and a selection/reselection of the target NF service instance is required, the SCP shall take into account all the NF service discovery factors contained in the "3gpp-Sbi-Discovery-\*" request headers to perform the selection or reselection. The SCP should use the NRF indicated in the 3gpp-Sbi-Nrf-Uri header if this header is present in the request. It is also possible for the SCP to be internally configured to fulfil these service discovery tasks without interacting with the NRF.

If the service request contains "3gpp-Sbi-Discovery-\*" request header(s) that are not supported by the SCP, the latter should include the corresponding query parameters in the discovery request to the NRF. Based on operator policy, the SCP may alternatively reject the request and return a response with the status code "400 Bad Request" to the NF service consumer with an "INVALID\_DISCOVERY\_PARAM" error.

If the service request does not contain the 3gpp-Sbi-Discovery-preferred-api-versions header, the SCP shall select the NF instance and/or service instance supports the MAJOR version received in the URI of the service request message. Otherwise, the preferred API MAJOR version included in the 3gpp-Sbi-Discovery-preferred-api-versions header shall be same as the MAJOR version received in the URI of the service request message. The SCP shall reject the request and return a response with the status code "400 Bad Request" to the NF service consumer with a "VERSION\_NOT\_SUPPORTED" error if no NF profile is found matching the MAJOR version.

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