**3GPP TSG-CT WG4 Meeting #97eC4-202xxx**

**E-Meeting, 15th – 24th April 2020** *Revision of C4-202024*

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| *CR-Form-v12.0* | | | | | | | | |
| **CHANGE REQUEST** | | | | | | | | |
|  | | | | | | | | |
|  | **29.500** | **CR** | **0108** | **rev** | **1** | **Current version:** | **16.3.0** |  |
|  | | | | | | | | |
| *For* [***HE******LP***](http://www.3gpp.org/3G_Specs/CRs.htm#_blank)*on using this form: comprehensive instructions can be found at* [*http://www.3gpp.org/Change-Requests*](http://www.3gpp.org/Change-Requests)*.* | | | | | | | | |
|  | | | | | | | | |

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| ***Proposed change affects:*** | UICC apps |  | ME |  | Radio Access Network |  | Core Network | **X** |

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | | | | | | | | | | |
| ***Title:*** | Error handling for indirect communications | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Source to WG:*** | Nokia, Nokia Shanghai Bell, Cisco | | | | | | | | | |
| ***Source to TSG:*** | CT4 | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Work item code:*** | 5G\_eSBA | | | | |  | ***Date:*** | | | 2020-03-25 |
|  |  | | | |  | |  | | |  |
| ***Category:*** | **F** |  | | | | | ***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-12 (Release 12)* *Rel-13 (Release 13) Rel-14 (Release 14) Rel-15 (Release 15) Rel-16 (Release 16)* | |
|  |  | | | | | | | | | |
| ***Reason for change:*** | | A request from an HTTP client may traverse one or more SCPs and/or SEPPs and may fail at an SCP, SEPP or at the HTTP server.  The HTTP client should be able to figure out whether the request failed at its next hop SCP or SEPP, or at the HTTP server, e.g. to be able to adapt its behaviour for the on-going request or subsequent request accordingly.  For instance, the HTTP client may retry the request or send subsequent requests towards the same HTTP server via a different SCP or SEPP if the next hop SCP or SEPP rejected the initial request due to insufficient resources, or towards a different HTTP server (via the same or a different SCP or SEPP) if the HTTP server rejected the request due to insufficient resources.  The lack of information on the originator of the error also impedes trouble-shooting of network problems. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Summary of change:*** | | The originator of an HTTP error response should include a Server header indicating its type and identity.  An SCP or SEPP relaying an HTTP error response shall include a Via header indicating its type and identity.  An HTTP client can figure out the originator of the error, i.e. whether the request failed at the next hop SCP or SEPP or at the HTTP server, using the Via and/or Server headers received in the HTTP error response. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Consequences if not approved:*** | | An HTTP client cannot figure out the originator of an HTTP error, i.e. whether a request failed at SCP, SEPP or at the HTTP server, preventing it from adapting its behaviour for the on-going request or a subsequent request accordingly and causing failures of further requests. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Clauses affected:*** | | 5.2.2.2, 6.10.x (new) | | | | | | | | |
|  | |  | | | | | | | | |
|  | | **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 \* \* \* \*

#### 5.2.2.2 Mandatory to support HTTP standard headers

The HTTP request standard headers and the HTTP response standard headers that shall be supported on SBI are defined in Table 5.2.2.2-1 and in Table 5.2.2.2-2 respectively. Mandatory to support HTTP standard headers does not mean all the HTTP requests and responses carry the identified request and response headers respectively. It only means it is mandatory to support the processing of the identified headers in request and response message.

Table 5.2.2.2-1: Mandatory to support HTTP request standard headers

|  |  |  |
| --- | --- | --- |
| Name | Reference | Description |
| Accept | IETF RFC 7231 [11] | This header is used to specify response media types that are acceptable. |
| Accept-Encoding | IETF RFC 7231 [11] | This header may be used to indicate what response content-encodings (e.g gzip) are acceptable in the response. |
| Content-Length | IETF RFC 7230 [12] | This header is used to provide the anticipated size, as a decimal number of octets, for a potential payload body. |
| Content-Type | IETF RFC 7231 [11] | This header is used to indicate the media type of the associated representation. |
| Content-Encoding | IETF RFC 7231 [11] | This header may be used in some requests to indicate the content encodings (e.g gzip) applied to the resource representation beyond those inherent in the media type. |
| User-Agent | IETF RFC 7231 [11] | This header shall be mainly used to identify the NF type of the HTTP/2 client.  The pattern of the content should start with the value of NF type (e.g. udm, see NOTE 1) and followed by a "-" and any other specific information if needed afterwards. |
| Cache-Control | IETF RFC 7234 [20] | This header may be used in some HTTP/2 requests to provide the HTTP cache-control directives that the client is willing to accept from the server. |
| If-Modified-Since | IETF RFC 7232 [24] | This header may be used in a conditional GET request, for server revalidation. This is used in conjunction with the Last-Modified server response header, to fetch content only if the content has been modified from the cached version. |
| If-None-Match | IETF RFC 7232 [24] | This header may be used in a conditional GET request. This is used in conjunction with the ETag server response header, to fetch content only if the tag value of the resource on the server differs from the tag value in the If-None-Match header. |
| If-Match | IETF RFC 7232 [24] | This header may be used in a conditional POST or PUT or DELETE or PATCH request. This is used in conjunction with the ETag server response header, to update / delete content only if the tag value of the resource on the server matches the tag value in the If-Match header. |
| Via | IETF RFC 7230 [12] | This header shall be inserted by HTTP proxies and it may be inserted by an SCP and SEPP when relaying an HTTP request. |
| Authorization | IETF RFC 7235 [21] | This header shall be used if OAuth 2.0 based access authorization with "Client Credentials" grant type is used as specified in clause 13.4.1 of 3GPP TS  33.501 [17], clause 7 of IETF RFC 6749 [22] and IETF RFC 6750 [23]. |
| NOTE 1: The value of NF type in the User-Agent header shall comply with the enumeration value of Table 6.1.6.3.3-1 in 3GPP TS 29.510 [8]. | | |

Table 5.2.2.2-2: Mandatory to support HTTP response standard headers

|  |  |  |
| --- | --- | --- |
| Name | Reference | Description |
| Content-Length | IETF RFC 7230 [12] | This header may be used to provide the anticipated size, as a decimal number of octets, for a potential payload body. |
| Content-Type | IETF RFC 7231 [11] | This header shall be used to indicate the media type of the associated representation. |
| Location | IETF RFC 7231 [11] | This header may be used in some responses to refer to a specific resource in relation to the response. |
| Retry-After | IETF RFC 7231 [11] | This header may be used in some responses to indicate how long the user agent ought to wait before making a follow-up request. |
| Content-Encoding | IETF RFC 7231 [11] | This header may be used in some responses to indicate to the HTTP/2 client the content encodings (e.g gzip) applied to the resource representation beyond those inherent in the media type. |
| Cache-Control | IETF RFC 7234 [20] | This header may be used in some responses (e.g. NRF responses to queries) to provide HTTP response cache control directives. The cache directives "no-cache", "no-store", "max-age" and "must-revalidate" values shall be supported. |
| Age | IETF RFC 7234 [20] | This header may be inserted by HTTP proxies when returning a cached response. The "Age" header field conveys the sender's estimate of the amount of time since the response was generated or successfully validated at the origin server. The presence of an Age header field implies that the response was not generated or validated by the origin server for this request. |
| Last-Modified | IETF RFC 7232 [24] | This header may be sent to allow for conditional GET with the If-Modified-Since header. |
| ETag | IETF RFC 7232 [24] | This header may be sent to allow for conditional GET with the If-If-None-Match header or a conditional POST / PUT / PATCH / DELETE with the If-Match header. |
| Via | IETF RFC 7230 [12] | This header shall be inserted by HTTP proxies.  This header shall be inserted by an SCP or SEPP when relaying an HTTP error response (see clause 6.10.x). It may be inserted when relaying other HTTP responses.  When inserted by an SCP or SEPP, the pattern of the header should be formatted as follows:  - "SCP-<SCP FQDN>" for an SCP  - "SEPP-<SEPP FQDN>" for a SEPP |
| Allow | IETF RFC 7231 [11] | This header field shall be used to indicate methods supported by the target resource. |
| WWW-Authenticate | IETF RFC 7235 [21] | This header field shall be included when an NF service producer rejects a request with a "401 Unauthorized" status code (e.g when a request is sent without an OAuth 2.0 access token or with an invalid OAuth 2.0 access token). |
| Accept-Encoding | IETF RFC 7694 [33] | See clause 6.9 for the use of this header. |
| Server | IETF RFC 7231 [11] | This header should be inserted by the originator of an HTTP error response (see clause 6.10.x). It may be inserted otherwise.  When inserted by an NF, an SCP or a SEPP, the pattern of the header should be formatted as follows:  - "SCP-<SCP FQDN>" for an SCP  - "SEPP-<SEPP FQDN>" for a SEPP - "<NFType>-<NF Instance ID>" for an NF |

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

### 6.10.x Error Handling

#### 6.10.x.1 General

A request from an HTTP client (i.e. a service request from an NF service consumer, or a notification request from an NF service producer) may traverse one or more SCPs and/or SEPPs and may fail at an SCP, SEPP or at the HTTP server.

The HTTP client should be able to figure out whether the request failed at its next hop SCP or SEPP, or at the HTTP server, e.g. to be able to adapt its behaviour for the on-going request or subsequent request accordingly. For instance, the HTTP client may retry the request or send subsequent requests towards the same HTTP server via a different SCP or SEPP if an SCP or SEPP rejected a request due to insufficient resources, or towards a different HTTP server (via the same or a different SCP or SEPP) if the HTTP server rejected the request due to insufficient resources.

NOTE: An SCP or SEPP can also retry a request towards a different SCP or SEPP if a next hop SCP or SEPP rejected a request e.g. due to insufficient resources.

#### 6.10.x.2 Requirements for the originator of an HTTP error response

To enable an HTTP client to determine the originator of an HTTP error response, the originator of an error (e.g. HTTP server, SCP or SEPP) should include a Server header in the HTTP error response with the following information:

- the type of the NF or network entity generating the error, set to the NFType value as defined in clause 6.1.6.3.3 of 3GPP TS 29.510 [8], e.g. "SCP", "SEPP", "SMF";

- the identity of the NF or network entity generating the error, set to the FQDN of the SCP or SEPP, or to the NF Instance ID of the HTTP server.

NOTE: The information carried in the Server header can also be useful for trouble-shooting.

EXAMPLE 1: Error generated by an SCP: Server: SCP-scp1.operator.com

EXAMPLE 2: Error generated by a SEPP: Server: SEPP-sepp1.operator.com

EXAMPLE 3: Error generated by an SMF: Server: SMF-54804518-4191-46b3-955c-ac631f953ed8

The presence of a Server header set to the next hop SCP or SEPP or to the HTTP server in an HTTP error response shall be an indication for the HTTP client that the next hop SCP or SEPP or the HTTP server is the originator of the error.

#### 6.10.x.3 Requirements for an SCP or SEPP relaying an HTTP error response

To enable an HTTP client to determine the originator of an HTTP error response, e.g. when an HTTP server does not include a Server header in an HTTP error response, the SCP or SEPP that forwards the HTTP error response towards the HTTP client shall include a Via header in the HTTP error response with the following information:

- the type of the network entity forwarding the error, set to the NFType value as defined in clause 6.1.6.3.3 of 3GPP TS 29.510 [8], i.e. "SCP" or "SEPP";

- the identity of the network entity forwarding the error, set to the FQDN of the SCP or SEPP.

NOTE: The information carried in the Via header can also be useful for trouble-shooting.

EXAMPLE 1: Error forwarded by an SCP: Via: SCP-scp1.operator.com

EXAMPLE 2: Error forwarded by a SEPP: Via: SEPP-sepp1.operator.com

The presence of a Via header set to the next hop SCP or SEPP in an HTTP error response shall be an indication for the HTTP client that the next hop SCP or SEPP is not the originator of the error.

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