**3GPP TSG-CT WG4 Meeting #98eC4-203xxx**

**E-Meeting, 02nd – 12th June 2020 (was C4-203042)**

|  |
| --- |
| *CR-Form-v12.0* |
| **CHANGE REQUEST** |
|  |
|  | **29.500** | **CR** | **0129** | **rev** | **1** | **Current version:** | **15.5.0** |  |
|  |
| *For* [***HE******LP***](http://www.3gpp.org/3G_Specs/CRs.htm#_blank)*on using this form: comprehensive instructions can be found at* [*http://www.3gpp.org/Change-Requests*](http://www.3gpp.org/Change-Requests)*.* |
|  |

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

|  |
| --- |
|  |
| ***Title:***  | WWW-Authenticate Header |
|  |  |
| ***Source to WG:*** | Hewlett-Packard Enterprise |
| ***Source to TSG:*** | CT4 |
|  |  |
| ***Work item code:*** | 5GS\_Ph1-CT |  | ***Date:*** | 2020-05-04 |
|  |  |  |  |  |
| ***Category:*** | **A** |  | ***Release:*** | Rel-15 |
|  | *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-12 (Release 12)**Rel-13 (Release 13)Rel-14 (Release 14)Rel-15 (Release 15)Rel-16 (Release 16)* |
|  |  |
| ***Reason for change:*** | Per RFC 6750, for the "WWW-Authenticate" header with the challenge scheme set to "Bearer", one or more auth-param attributes must be present.However, TS 29.500 specifies the auth-param "realm" attribute for an API request without the OAuth2.0 access token. But there is no specification on which auth-param should be included in the "WWW-Authenticate" header for an API request with an invalid OAuth2.0 access token.It is proposed that the auth-param "realm" attribute is included in the "WWW-Authenticate" header for an API request without the OAuth2.0 access token and for an API request with an invalid OAuth2.0 access token. In addition, for an API request with an invalid OAuth2.0 access token, an error code “invalid\_token” should be included. |
|  |  |
| ***Summary of change:*** | * Remove condition "the access without an OAuth2.0 access token failed" for the "realm" attribute
* Add error code “invalid\_token”
 |
|  |  |
| ***Consequences if not approved:*** | FASMO. Inconsistence with the OAuth 2.0 Authorization Framework will lead to interoperability issues as the current text is not in line with RFC 6750. |
|  |  |
| ***Clauses affected:*** | 6.7.3 |
|  |  |
|  | **Y** | **N** |  |  |
| ***Other specs*** |  | **X** |  Other core specifications  | TS/TR ... CR ...  |
| ***affected:*** |  | **X** |  Test specifications | TS/TR ... CR ...  |
| ***(show related CRs)*** |  | **X** |  O&M Specifications | TS/TR ... CR ...  |
|  |  |
| ***Other comments:*** |  |
|  |  |
| ***This CR's revision history:*** | Rev 1: Rewording based on C4-202510 |

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

### 6.7.3 Authorization of NF service access

As specified in clause 13.4.1 of 3GPP TS 33.501 [17] OAuth 2.0 (see IETF RFC 6749 [22]) may be used for authorization of NF service access. All NFs and the NRF shall support the OAuth 2.0 authorization framework with "Client Credentials" grant type as specified in clause 4.4 of IETF RFC 6749 [22] , except that there is no "Authorization" HTTP request header in the access token request.

The NRF shall act as the Authorization Server providing "Bearer" access tokens (IETF RFC 6750 [23]) to the NF service consumers to access the services provided by the NF service providers.

If an NF service (i.e API) receives an OAuth 2.0 access token in the "Authorization" HTTP request header field, the NF service shall validate the access token, its expiry and its access scope before allowing access to the requested resource, as specified in clause 7 of IETF RFC 6749 [22].

An NF service consumer shall support OAuth 2.0.

For request/response semantics service operations and for the subscribe and unsubscribe operations of subscribe/notify semantics service operations, an NF service consumer may use OAuth 2.0 for the authorization of the API access, based on local configuration.

When Oauth2 authorization is used, the NF service consumer shall use the token received from NRF as a "Bearer" token and include it in the Authorization header of the HTTP service requests, as described in IETF RFC 6750 [23] clause 2.1.

An NF service producer shall decide to accept or reject an API request without the OAuth2.0 access token in the "Authorization" HTTP request header field, based on local configuration.

If an NF service producer rejects an API request without the OAuth2.0 access token or an API request with an invalid OAuth2.0 access token, it shall return the HTTP "401 Unauthorized" status code together with the "WWW-Authenticate" header as specified in IETF RFC 7235 [21], where:- the scheme for challenge in the "WWW-Authenticate" header shall be set to "Bearer" (IETF RFC 6750 [23]).

 - the "realm" attribute shall be set to the URI of the service (i.e API URI)for which failed, in the case of request / response service operations.

- the "error" attribute shall be set to "invalid\_token", as described in IETF RFC 6750 [23], if the request contained a token which was deemed as invalid by the NF service producer (e.g. it is expired, malformed...); if the request did not contain a token, the "error" attribute shall not be included.

For the notify operation of subscribe/notify semantics service operations, in this release of this specification OAuth 2.0 access token is not used.

When an NF service consumer receives a "401 Unauthorized" status code with a "WWW-Authenticate" header containing "Bearer" as the scheme for challenge it shall not repeat the same request without an OAuth2.0 access token or with an access token that has been already used. The NF service consumer may repeat the same request with a new OAuth 2.0 access token.

NOTE: If a NF service producer accepts a request without the OAuth 2.0 access token, based on local policy, it is assumed that such accesses are allowed based on trust relationships and hence full access to the resource as it would have been otherwise allowed, is provided.

\* \* \* End of Change \* \* \* \*