**3GPP TSG-CT WG4 Meeting #103-eC4-212abc**

**E-Meeting, 14th – 23rd April 2021 *was* C4-212274**

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| *CR-Form-v12.1* | | | | | | | | |
| **CHANGE REQUEST** | | | | | | | | |
|  | | | | | | | | |
|  | **29.510** | **CR** | **0504** | **rev** | **1** | **Current version:** | **17.1.0** |  |
|  | | | | | | | | |
| *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:*** | Access token request verification | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Source to WG:*** |  | | | | | | | | | |
| ***Source to TSG:*** | CT4 | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Work item code:*** | SBIProtoc16 | | | | |  | ***Date:*** | | |  |
|  |  | | | |  | |  | | |  |
| ***Category:*** | **A** |  | | | | | ***Release:*** | | |  |
|  | *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:*** | | 3GPP TS 33.501 clause 13.4.1.1.2 Service Request Process specifies that the NRF may verify the input parameters (e.g., NF type) in the access token request match with the corresponding ones in the public key certificate of the NF service consumer. 3GPP TS 29.510 miss the corresponding description. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Summary of change:*** | | The NRF may verify the access token request before making the decision on authorization. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Consequences if not approved:*** | | Services will be consumed via forged access token request. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Clauses affected:*** | | 5.4.2.2.1. | | | | | | | | |
|  | |  | | | | | | | | |
|  | | **Y** | **N** |  | | | |  | | |
| ***Other specs*** | |  | **X** | Other core specifications | | | | TS/TR ... CR ... | | |
| ***affected:*** | |  | **X** | Test specifications | | | | TS/TR ... CR ... | | |
| ***(show related CRs)*** | |  | **X** | O&M Specifications | | | | TS/TR ... CR ... | | |
|  | |  | | | | | | | | |
| ***Other comments:*** | | This CR does not change OpenAPI. | | | | | | | | |
|  | |  | | | | | | | | |
| ***This CR's revision history:*** | | Rev1:  Improve the new added text in 5.4.2.2.1 | | | | | | | | |

**\*\*\*\*\*\*\***

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

#### 5.4.2.2 Get (Access Token Request)

##### 5.4.2.2.1 General

This service operation is used by an NF Service Consumer to request an OAuth2 access token from the authorization server (NRF).



Figure 5.4.2.2.1-1: Access Token Request

1. The NF Service Consumer shall send a POST request to the "Token Endpoint", as described in IETF RFC 6749 [16], clause 3.2. The "Token Endpoint" URI shall be:

{nrfApiRoot}/oauth2/token

where {nrfApiRoot} represents the concatenation of the "scheme" and "authority" components of the NRF, as defined in IETF RFC 3986 [17].  
  
The OAuth 2.0 Access Token Request includes in the body of the HTTP POST request shall contain:

- An OAuth2 grant type set to "client\_credentials";

- The "scope" parameter indicating the names of the NF Services that the NF Service Consumer is trying to access (i.e., the expected NF service names);

- The NF Instance Id of the the NF Service Consumer requesting the OAuth2.0 access token;

- NF type of the NF Service Consumer, if this is an access token request not for a specific NF Service Producer;

- NF type of the expected NF Service Producer, if this is an access token request not for a specific NF Service Producer;

- The NF Instance Id of the expected NF Service Producer, if this is an access token request for a specific NF Service Producer;

- Home and Serving PLMN IDs, if this is an access token request for use in roaming scenarios (see clause 13.4.1.2 of 3GPP TS 33.501 [15]).

The request may additionally contain:

- the NF Set ID of the expected NF service producer instances, if this is an access token request not for a specific NF Service Producer.

The NF Service Consumer shall use TLS for mutual authentication with the NRF in order to access this endpoint, if the PLMN uses protection at the transport layer. Otherwise the NF Service Consumer shall use NDS or physical security to mutually authenticate with the NRF as specified in clause 13.3.1 of 3GPP TS 33.501 [15].

The NRF may verify the input attributes (e.g., NF type) in the access token request match with the corresponding ones in the public key certificate of the NF service consumer. If the verification is successful, other authorization check shall be performed, otherwise, the request shall be rejected immediately.

2a. On success, "200 OK" shall be returned, the payload body of the POST response shall contain the requested access token and the token type set to value "Bearer". The response in addition:

- should contain the expiration time for the token as indicated in IETF RFC 6749 [16] unless the expiration time of the token is made available by other means (e.g. deployment-specific documentation); and

- shall contain the NF service name(s) of the requested NF service producer(s), if it is different from the scope included in the access token request (see IETF RFC 6749 [16]).

The access token shall be a JSON Web Token (JWT) as specified in IETF RFC 7519 [25]. The access token returned by the NRF shall include the claims encoded as a JSON object as specified in clause 6.3.5.2.4 and then digitally signed using JWS as specified in IETF RFC 7515 [24] and in clause 13.4.1 of 3GPP TS 33.501 [15].

The digitally signed access token shall be converted to the JWS Compact Serialization encoding as a string as specified in clause 7.1 of IETF RFC 7515 [24].

2b. On failure or redirection:

- If the access token request fails at the NRF, the NRF shall return "400 Bad Request" status code, including in the response payload a JSON object that provides details about the specific error that occurred.

- In the case of redirection, the NRF shall return 3xx status code, which shall contain a Location header with an URI pointing to the endpoint of another NRF service instance.

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