**3GPP TSG-SA4 Meeting #129e  *S4-241535***

**Online, 19. – 23. August 2024**

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| *CR-Form-v12.3* | | | | | | | | |
| **CHANGE REQUEST** | | | | | | | | |
|  | | | | | | | | |
|  | **26.510** | **CR** | **0006** | **rev** | **-** | **Current version:** | **18.0.2** |  |
|  | | | | | | | | |
| *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:*** | [5GMS\_Pro\_Ph2]: Correction of OAuth access token usage by the Media AF | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Source to WG:*** | Ericsson LM | | | | | | | | | |
| ***Source to TSG:*** | S4 | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Work item code:*** | 5GMS\_Pro\_Ph2 | | | | |  | ***Date:*** | | | 2024-08-13 |
|  |  | | | |  | |  | | |  |
| ***Category:*** | **F** |  | | | | | ***Release:*** | | | Rel-18 |
|  | *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-17 (Release 17) Rel-18 (Release 18) Rel-19 (Release 19)  Rel-20 (Release 20)* | |
|  |  | | | | | | | | | |
| ***Reason for change:*** | | The highlevel authorization procedure separating an Authorization Server functions from the API Provider function (the Media AF) is standardized. It is however currently not clear, that the API Provider Function should allow access, when an access token with the appropriate information, at least with target resource, 5GMS features and scopes is presented by the API Invoker. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Summary of change:*** | | The specification is corrected by adding a normative checking step for determining the authorzation by evaluating the access token information. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Consequences if not approved:*** | | The OAUTH security procedure is not functional. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Clauses affected:*** | | 7.4.2, 7.4.3 | | | | | | | | |
|  | |  | | | | | | | | |
|  | | **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:*** | |  | | | | | | | | |

## 7.4 Security

### 7.4.1 General

The Media AF shall enable secure provision of information in the Media Delivery System by authenticated and authorised Media-aware Applications or Media Application Providers.

### 7.4.2 Authorising Media Application Provider access to the Media AF at reference point M1

When a Media Application Provider deployed outside the Trusted DN attempts to access a Media AF deployed inside the Trusted DN, the Media Delivery System shall authenticate and authorise the Media Application Provider.

Access to the Maf\_Provisioning API of the Media AF by the Media Application Provider at reference point M1 may be authorised by means of the OAuth 2.0 protocol specified in RFC 6749 [47]), using the *client credentials* authorization grant. Based on the content of the issued access token, the Media AF shall determine whether the Media Application Provider is authorised to invoke a given provisioning operation in terms of the targeted resource and HTTP method, and hence the underlying Media Delivery feature.

NOTE: The provisioning and negotiation of the security method is not specified in this release.

When CAPIF (see TS 29.222 [48]) is used for external API exposure:

- The CAPIF core function shall play the role of authorization server, the Media AF shall play the role of resource server and the Media Application Provider shall play the role of client.

- Before invoking any service operation exposed by the Media AF, the Media Application Provider shall negotiate the security method (PKI, TLS-PSK or OAuth 2.0) with the CAPIF core function and shall ensure that the Media AF has the required credentials to authenticate access tokens subsequently presented by the Media Application Provider (see clauses 5.6.2.2 and 6.2.2.2 of TS 29.222 [48]).

- If PKI or TLS-PSK is the selected security method between the Media Application Provider and the Media AF shall, upon invocation of a Maf\_Provisioning service operation by the Media Application Provider at reference point M1, retrieve the authorisation information from the CAPIF core function as described in clause 5.6.2.4 of TS 29.222 [48].

- If OAuth 2.0 [47] is the selected security method between the Media Application Provider and the Media AF, the Media Application Provider shall, prior to invoking Maf\_Provisioning service operations on the Media AF at reference point M1, obtain an access token from the authorization server (CAPIF core function) by invoking the Obtain\_Authorization service operation specified in clause 5.6.2.3.2 of TS 29.222 [48].

Otherwise:

- The Media AF shall play the role of both authorization server and resource server, and the Media Application Provider shall play the role of client.

- The Media Application Provider shall obtain an access token from the authorization server (Media AF) using the client credentials authorization grant specified in section 4.4 of RFC 6749 [47] prior to invoking Maf\_Provisioning service operations on the resource server (Media AF) at reference point M1.

### 7.4.3 Authorising Media Session Handler access to the Media AF at reference point M5

When a Media Session Handler deployed in a Media Client attempts to access a Media AF deployed inside the Trusted DN, the Media Delivery System shall authenticate and authorise the Media Session Handler.

Access to the Maf\_SessionHandling API of the Media AF by the Media Session Handler at reference point M5 shall be authorised by means of the OAuth 2.0 protocol specified in RFC 6749 [47], using the *client credentials* or *authorization code* flow grant types. Based on the content of the issued access token, the Media AF shall determine whether the Media Session Handler is authorised to invoke a given provisioning operation in terms of the targeted resource and HTTP method, and hence the underlying Media Delivery feature.

NOTE: The provisioning and negotiation of the security method is not specified in this release.

When CAPIF (see TS 29.222 [48]) is used for external API exposure:

- The CAPIF core function shall play the role of authorization server, the Media AF shall play the role of resource server and the Media Session Handler shall play the role of client.

- Before invoking any service operation exposed by the Media AF, the Media Application Provider shall negotiate the security method (PKI, TLS-PSK or OAuth 2.0) with the CAPIF core function and shall ensure that the Media AF has the required credentials to authenticate access tokens subsequently presented by the Media Application Provider (see clauses 5.6.2.2 and 6.2.2.2 of TS 29.222 [48]).

- If PKI or TLS-PSK is the selected security method between the Media Session Handler and the Media AF shall, upon invocation of a Maf\_SessionHandling service operation by the Media Session Handler at reference point M1, retrieve the authorisation information from the CAPIF core function as described in clause 5.6.2.4 of TS 29.222 [48].

- If OAuth 2.0 [47] is the selected security method between the Media Session Handler and the Media AF, the Media Session Handler shall, prior to invoking Maf\_SessionHandling service operations on the Media AF at reference point M5, obtain an access token from the authorization server (CAPIF core function) by invoking the Obtain\_Authorization service operation specified in clause 5.6.2.3.2 of TS 29.222 [48].

Otherwise:

- Either the Media AF shall play the role of both authorization server and resource server, or the Media AF shall play the role of the resource server and the Media Application Provider plays the role of the authorization server. The Media Session Handler shall play the role of client.

- The Media Session Handler shall obtain an access token from the authorization server using either the client credentials grant specified in section 4.4 of RFC 6749 [47] or the authorization code grant specified in section 4.1 of [47] prior to invoking Maf\_Provisioning service operations on the resource server (Media AF) at reference point M5.