**3GPP TSG-SA4 Meeting # 129e *S4-241536***

 **Online, 19. – 23. August 2024**

|  |
| --- |
| *CR-Form-v12.3* |
| **CHANGE REQUEST** |
|  |
|  | **26.512** | **CR** | **0079** | **rev** | **-** | **Current version:** | **18.2.1** |  |
|  |
| *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]: OAuth 2.0 security at Reference Point M3 |
|  |  |
| ***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 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-17 (Release 17)Rel-18 (Release 18)Rel-19 (Release 19) Rel-20 (Release 20)* |
|  |  |
| ***Reason for change:*** | An Authorization Server is introduced, but the authorization procedure is not standardized, which is ok. However, it is currently not clear, that the Service APIs should allow access, only when an access token with the appropriate information, like target resource, scopes, operations, etc, is presented by the API Invoker. |
|  |  |
| ***Summary of change:*** | A section on OAUTH 2.0 security procedures is added to the specification. For the reference point M1 and M5, a reference to the according sections in TS 26.510 is added. For reference point M3, an according authorization procedure is added. |
|  |  |
| ***Consequences if not approved:*** | No security defined for reference points in the 5G Media Streaming Architecture. |
|  |  |
| ***Clauses affected:*** | 6.6 (new) |
|  |  |
|  | **Y** | **N** |  |  |
| ***Other specs*** | **X** |  |  Other core specifications  | TS 26.510 CR0006 |
| ***affected:*** |  | **x** |  Test specifications |  |
| ***(show related CRs)*** |  | **x** |  O&M Specifications |  |
|  |  |
| ***Other comments:*** |  |
|  |  |
| ***This CR's revision history:*** |  |

## 6.6 Security

### 6.6.1 General

The 5GMS AF shall enable secure provision of information in the 5GMS System by authenticated and authorised 5GMS Application Providers or 5GMS-Aware Applications.

### 6.6.2 Authorising 5GMS Application Provider access to the 5GMS AF at reference point M1

Implementations of the 5GMS Application Provider shall comply with the authorisation provisions specified in clause 7.4.2 of TS 26.510 [56].

### 6.6.3 Authorising 5GMS AF access to the 5GMS AS at reference point M3

When a 5GMS AF deployed outside the Trusted DN attempts to access a 5GMS AS deployed inside the Trusted DN, the 5GMS System shall authenticate and authorise the 5GMS AF.

Access to the Mas\_Configuration API of the 5GMS AS by the 5GMS AF at reference point M3 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 access token, the 5GMS AS determines whether the 5GMS AF is authorised to invoke a given configuration operation in terms of the targeted resource and HTTP method, and hence the underlying 5GMS 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 5GMS AS shall play the role of resource server and the 5GMS AF shall play the role of client.

- Before invoking any service operation exposed by the 5GMS AS, the 5GMS AF shall negotiate the security method (PKI, TLS-PSK or OAuth 2.0) with the CAPIF core function and shall ensure that the 5GMS AS has the required credentials to authenticate access tokens subsequently presented by the 5GMS 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 5GMS AF and the 5GMS AS shall, upon invocation of a Mas\_Configuration service operation by the 5GMS AF at reference point M3, 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 5GMS AF and the 5GMS AS, the 5GMS AF shall, prior to invoking Mas\_Configuration service operations on the 5GMS AS at reference point M3, 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 5GMS AS shall play the role of both authorization server and resource server, and the 5GMS AF shall play the role of client.

- The 5GMS AF shall obtain an access token from the authorization server (5GMS AS) using the client credentials authorization grant specified in section 4.4 of RFC 6749 [47] prior to invoking Mas\_Configuration service operations on the resource server (5GMS AS) at reference point M3.

### 6.6.4 Authorising Media Session Handler access to the 5GMS AF at reference point M5

Implementations of the Media Session Handler shall comply with the authorisation provisions specified in clause 7.4.3 of TS 26.510 [56].