**3GPP TSG- Meeting # *S4-240675***

**,**

|  |
| --- |
| *CR-Form-v12.2* |
| **CHANGE REQUEST** |
|  |
|  |  | **CR** |  | **rev** | **-** | **Current version:** |  |  |
|  |
| *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 | **X** | Radio Access Network |  | Core Network | **X** |

|  |
| --- |
|  |
| ***Title:***  | : Stage 2 corrections to support Oauth 2.0 authorization |
|  |  |
| ***Source to WG:*** |  |
| ***Source to TSG:*** |  |
|  |  |
| ***Work item code:*** | 5GMS\_Ph2 |  | ***Date:*** | 03.11.2023 |
|  |  |  |  |  |
| ***Category:*** |  |  | ***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 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-16 (Release 16)Rel-17 (Release 17)Rel-18 (Release 18)Rel-19 (Release 19)* |
|  |  |
| ***Reason for change:*** |  |
|  |  |
| ***Summary of change:*** | The OpenAPI definitions within TS 26.510 are extended for the usage of Oauth 2.0 (according to the SA3 guidelines) for 5GMS protocols based on the conclusions in TR 26.804, clause 6.9. |
|  |  |
| ***Consequences if not approved:*** |  |
|  |  |
| ***Clauses affected:*** | 5.2.5 (new), 5.3.3 (new), Annex X (new) |
|  |  |
|  | **Y** | **N** |  |  |
| ***Other specs*** |  | **X** |  Other core specifications  |  |
| ***affected:*** |  | **X** |  Test specifications |  |
| ***(show related CRs)*** |  | **X** |  O&M Specifications |  |
|  |  |
| ***Other comments:*** |  |
|  |  |
| ***This CR's revision history:*** |  |

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

### 5.2.5 Procedures for downlink media streaming with per-application authorisation

#### 5.2.5.1 General

This clause defines procedures by which a 5GMSd Application Provider authorises a 5GMSd-Aware Application to access specific network features of the 5GMS System at reference point M5.

#### 5.2.5.2 Authorisation based on access token

The 5GMSd Application Provider provides a different access token (e.g. a random string) via M8 to each 5GMSd-Aware Application, so that each application can identify itself uniquely to the 5GMSd AF.

The 5GMSd-Aware Application passes the access token (via an M6 API call) to the Media Session Handler. When the Media Session Handler invokes a media session handling operation at reference point M5, it presents the access token to the 5GMSd AF. Upon receipt of such an access token, the 5GMSd AF verifies whether the access token is valid. If the token is valid, the 5GMSd-Aware Application is authorized to invoke the operation.

The access token is provided e.g. during the login procedure or is requested at a later stage.

The call flow is depicted below, assuming that the authorization token is provided with the application service login response.



Figure 5.2.5.2‑1: Call flow for authorisation based on access token

The steps are as follows:

1. When the user wants to use the 5GMSd-Aware Application to consume e.g. video content, the user needs to authenticate with the application and the 5GMSd Application Provider at reference point M8. (In some cases, this authorization can be cached/stored by the application, so that the user is not always challenged to provide the login credentials.)

NOTE: The application may be a native application (e.g. an Android application) or a browser application.

2. Based on the login credentials supplied in the previous step, the 5GMSd Application Provider determines the policy rights to which this application service subscription is entitled (e.g. the user may have subscribed to an SD quality video service or a 4K quality video service). According to the subscription entitlement level, the 5GMSd Application Provider creates an access token and passes this token back to the application with the login response.

3. When the 5GMSd-Aware Application (immediately or later) invokes the Media Session Handler to activate media session handling for a media delivery session, the application passes the access token to the Media Session Handler. The authorization token may embed a user identifier, or the user identifier may be passed as separate (anonymised) parameter.

4. When the Media Session Handler invokes a media session handling operation on the 5GMSd AF at reference point M5, it provides the the access token, e.g. as an HTTP query parameter.

5. The 5GMSd AF verifies the access token with the 5GMSd Application Provider.

6. If the 5GMSd AF has verified that the 5GMSd-Aware Application is authorised to invoke the media session handling operation (based on the token), the 5GMSd AF carries out the requested operation. (This may involve further interaction with the PCF or NEF.)

#### 5.2.5.2 Authorisation based on redirection

Editor’s Note: This section describes a redirection-based flow, leveraging the OAuth Authorization Code grant type.

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

### 5.3.3 Baseline provisioning procedure with authorization

This clause describes the baseline procedure to provision the features using the 5GMS System to support authorisation of media session handling for downlink media streaming per clause 5.2.5. The steps in the call flow sequence are as follows with differences from the baseline call flow in clause 5.3.2 highlighted in **bold.**

NOTE 1: SLA negotiations between the 5GMSd Application Provider and the 5GMS System provider are outside the scope of the present specification and are included in the figure below for illustrative purposes only.



Figure 5.3.3-1: High-level procedure for provisioning the 5GMS System
for downlink media streaming sessions

Steps:

1. The 5GMSd Application Provider discovers the address (URL) of the 5GMSd AF (M1d) for Session Provisioning. **During the self-onboarding procedure, the 5GMSd Application Provider obtains the API access credentials.**

2. The 5GMSd Application Provider authenticates itself with the system. This procedure reuses existing authentication/authorization procedures, e.g. as defined for CAPIF [13]. **The 5GMSd AF** **acts here as OAuth Authorization Server and also as OAuth Resource Server.** **The 5GMSd Application Provider obtains an access token which is used for any subsequent operation invocations at reference point M1.**

3. The 5GMSd Application Provider creates a Provisioning Session, providing its 5GMSd Application Provider identifier as input. 5GMSd Application Provider queries the capabilities and authorized features.

4. The 5GMSd Application Provider specifies one or more 5GMSd features in the Provisioning Session.A set of authorized features is activated, such as content consumption measurement, logging, collection and reporting; QoE metrics measurement, logging, collection and reporting; dynamic policy; network assistance; and content hosting (including ingest).

 One or more *External service identifiers* are supplied by the 5GMSd Application Provider to support the later retrieval of Service Access Information from the 5GMSd AF by the Media Session Handler.

 When the content hosting feature is offered and selected, the 5GMS Application Provider configures the content hosting behaviour of the 5GMSd AS. This Content Hosting Configuration is specified in clause 5.4 and includes selecting the ingest protocol and format, caching and proxying of media objects, content preparation, access protection (e.g. URL signing) and indicating a target distribution area (e.g. through geofencing).

 When the dynamic policy feature is offered and selected, the 5GMSd Application Provider specifies a set of policies which can be invoked for the unicast downlink streaming session. The UE becomes aware of the selected policies in the form of a list of valid Policy Template Ids.

 When the content consumption measurement, logging, collection and reporting feature is offered and selected, the 5GMSd Application Provider indicates the desired reporting interval. When the 5GMSd Application Provider has delegated Service Access Information handling to the 5GMS System, then location reporting is also selected or de-selected.

 When the QoE metrics measurement, logging, collection and reporting feature is offered and selected, the 5GMSd Application Provider provides configuration input on the QoE post processing. When the 5GMSd Application Provider has delegated Service Access Information handling to the 5GMS System, then more detailed metrics reporting is configured.

 When the edge computing feature is offered and selected, the 5GMSd Application Provider provides one or more Edge Resources Configurations that can be used to support either client-driven management or Application Provider-driven management of edge resources associated with the Provisioning Session.

 When the event data processing feature is offered and selected, the 5GMSd Application Provider provides one or more Event Data Processing Configurations that determine how, in the scope of the Provisioning Session, content consumption and QoE metrics collected from the UE and application logs collected from the 5GMSd AS are processed into events and exposed to subscribers.

5. When content hosting is desired, the 5GMSd AF interacts with the 5GMSd AS at reference point M3d to allocate M2d resources and to configure the ingest format by means of a Content Hosting Configuration (defined in clause 5.4) which may reference Server Certificates and Content Preparation Templates, as required. The 5GMSd AS responds with the M2d content ingest address.

6. The 5GMSd AF compiles the Service Access Information. The Service Access Information contains access details and options such as the Provisioning Session identifier, M5d (Media Session Handling) addresses for content consumption reporting, QoE metrics reporting, dynamic policy, network assistance, etc. When content hosting is offered and has been selected in step 4, then also M4d (Media Streaming) information such as the DASH MPD is included.

7. The 5GMSd AF provides the results to the 5GMSd Application Provider.

a. When the 5GMSd Application Provider has selected full Service Access Information, then the results are provided in the form of addresses and configurations for M2d (Ingest), M5d (Media Session Handling) and M4d (Media Streaming).

b. When the 5GMSd Application Provider delegated the Service Access Information handling to the 5GMS System, then a reference to the Service Access Information (e.g., a URL) is provided. The Media Session Handler fetches the full Service Access Information later from the 5GMSd AF.

8. When content hosting is offered and has been selected in step 4, the 5GMSd Application Provider can start supplying content at the M2d ingest interface. In the case of progressive download or on-demand DASH sessions, the 5GMSd Application Provider makes the content assets available. In the case of Live DASH streaming sessions, the 5GMSd Application Provider starts supplying the live content.

9. The 5GMSd Application Provider executes Service Announcement and updates the UEs (during the lifetime of the Provisioning Session).

Optional:

10. The 5GMSd Application Provider may update the Provisioning Session.

Depending on the parameters of the Provisioning Session:

11. The 5GMSd AF may send event-related or periodic notifications to the 5GMSd Application Provider.

According to schedule, or upon request:

12. The 5GMSd Application Provider may manually terminate the Provisioning Session (at any time). All associated resources are released. Content may be removed from the 5GMSd AS. The 5GMSd Application Provider may configure a schedule for Provisioning Session termination.

13. The 5GMSd AF sends a notification upon Provisioning Session termination.

The 5GMSd AF may request the creation or reuse of one or more network slices for distributing the content of the provisioned session. If more than one network slice is provisioned for the distribution of the content of a session, the list of allowed S‑NSSAIs shall be conveyed to the target UEs (e.g. through URSP or through M5d or M8d).

NOTE 2: The 5GMSd AS(s) serving the content are only accessible through the DNN(s) used by the network slice(s) provisioned for the distribution of that content.

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

Annex X (informative):
Collaboration models for per-application authorisation

# X.1 Introduction

Operation of certain 5GMS services may include an SLA between the Application Provider and the 5GMS System provider. In this context, "Per-application authorisation" refers to scenarios where one or more 5GMS-Aware Application is hosted on the same UE and can access services only from the associated 5GMS Application Provider.

The 5GMS System provider may offer one common 5GMS AF serving all 5GMS Application Providers or separate logical 5GMS AFs,each serving a single 5GMS Application Provider.

In the following, two example scenarios are described:

- A single UE hosting multiple 5GMS-Aware Applications from different 5MGS Application Providers.

- A single 5GMS Application Provider offers different subscription levels.

# X.2 UE hosting multiple applications

This collaboration scenario focuses on cases where one or more 5GMS-Aware Applications are hosted on the same UE and are using the same 5GMS Client. This may be the case when the Media Session Handler in the 5GMS Client is provided as a common Operating System service. The Media Session Handler in the 5GMS Client supports isolation between different 5GMS-Aware Application contexts.



Figure X.2-1: Per-application authorisation collaboration scenario

Each 5GMS-Aware Application uses an M8 reference point instance to connect to its 5GMS Application Provider.

The 5G System provider offers a common 5GMS AF within the Trusted DN. The 5GMS AF supports request and provider isolation so that 5GMS Application Provider #1 and #2 do not interfere with each other.

EXAMPLE 1: 5GMS Application Provider #1 has agreed different charging conditions from 5GMS Application Provider #2. The 5GMS System ensures that only 5GMS-Aware Application #1 can benefit from the conditions agreed with 5GMS Application Provider #1.

EXAMPLE 2: 5GMS-Aware Application #1 is entitled to receive higher network QoS than 5GMS-Aware Application #2.

# X.2 Applications with multiple subscription levels

This collaboration scenario focuses on cases where a 5GMS Application Provider offers multiple subscription levels to its consumers, for example the user of 5GMS-Aware Application #1 is entitled to the "Premium Connectivity" subscription level while the user of 5GMS-Aware Application #2 is entitled only to the "Default Connectivity" level.



Figure X.3-1: Per-Application authorisation collaboration scenario

Each 5GMS-Aware Application uses an M8 reference point instance to connect to its 5GMS Application Provider. The 5GMS Application Provider is aware about the different user subscription levels.

The 5G System provider offers a common 5GMS AF within the Trusted DN. Using an appropriate authorisation mechanism, the 5GMS AF determines that 5GMS-Aware Application #1 is entitled to higher bit rates than 5GMS-Aware Application #2.

\*\*\*\* Last Change \*\*\*\*