**3GPP TSG- Meeting Post # *S4-240919***

**, revision of S4aI240060**

|  |
| --- |
| *CR-Form-v12.2* |
| **CHANGE REQUEST** |
|  |
|  |  | **CR** |  | **rev** | **3** | **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:*** | **F** |  | ***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. This CR is adding and clarifying the stage 2 procedures.  |
|  |  |
| ***Consequences if not approved:*** |  |
|  |  |
| ***Clauses affected:*** | 5.2.5 (new), 5.3.3 (new), 6.2.2.3 (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:*** | S4aI240060, S4-240842, S4-240675 |

# Background

Clause 6.2 of TS 23.222



Figure 6.2-1: Functional model for the CAPIF

The CAPIF is hosted within the PLMN operator network. The API invoker is typically provided by a 3rd party application provider who has service agreement with PLMN operator. The API invoker may reside within the same trust domain as the PLMN operator network.

The API invoker within the PLMN trust domain interacts with the CAPIF via CAPIF-1 and CAPIF-2. The API invoker from outside the PLMN trust domain interacts with the CAPIF via CAPIF-1e and CAPIF-2e. The API exposing function, API publishing function and API management function of the API provider domain within the PLMN trust domain interacts with the CAPIF core function via CAPIF-3, CAPIF-4 and CAPIF-5 respectively.

The CAPIF core function provides CAPIF APIs to the API invoker over CAPIF-1 and CAPIF-1e. The API exposing function provides the service APIs to the API invoker over CAPIF-2 and CAPIF-2e.

NOTE 1: The communication between API exposing function and CAPIF core function, between API publishing function and CAPIF core function and between API management function and CAPIF core function over CAPIF-3, CAPIF-4 and CAPIF-5 respectively can be API based.

The detailed information of the APIs provided by CAPIF core function is specified in clause 10.

NOTE 2: The security aspects of CAPIF-1, CAPIF-1e, CAPIF-2 and CAPIF-2e are under SA3 responsibility and out of scope of the present document.

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

# 2 References

[23222] 3GPP TS 23.222: "Common API Framework for 3GPP Northbound APIs".

[33122] 3GPP TS 33.122: "Security aspects of Common API Framework (CAPIF) for 3GPP northbound APIs".

[RFC6749] IETF RFC 6749: "The OAuth 2.0 Authorization Framework", October 2012.

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

### 4.10.2 Baseline parameters of 3GPP Service URL for 5G Media Streaming

The parameters in table 4.10.2-1 may be included explicitly or implicitly in the 3GPP Service URL when it is used to launch a 5G Media Streaming session:

Table 4.10.2-1: Baseline parameters of 3GPP Service URL for 5G Media Streaming

|  |  |  |
| --- | --- | --- |
| Parameter | Use | Description |
| Service type | M | Uniquely indicating either downlink 5G Media Streaming or uplink 5G Media Streaming. |
| External service identifier | M | A globally unique service identifier nominated by the 5GMS Application Provider that resolves to a Provisioning Session in the 5GMS System. |
| 5GMS AF endpoint addresses | 0..N | Endpoint address(es) for 5GMS AF instance(s) to be used by the Media Session Handler at reference point M5. Any of the provided addresses may be used for media session handling of this 3GPP Service URL.Present only in the case where the 5GMS AF is deployed outside the Trusted DN. |
| 5GMS AF access token | 0..1 | A token that is presented by the Media Session Handler to the 5GMS AF at reference point M5 that asserts its right to invoke the media session handling operations exposed by the 5GMS AF. |
| Media Entry Point URLs | 0..N | URLs of Media Entry Points on a 5GMS AS to be launched by the Media Session Handler after successful initiation of media session handling and establishment of communication with the Media Stream Handler (Media Player or Media Streamer). |
| Acceptable media types | C | Indicating a set of media types acceptable to the 5GMS-Aware Application for a 5G Media Streaming session.Present if no Media Entry Point is provided. This value is used by the Media Session Handler to select the appropriate Media Entry Point provided by the 5GMS AF. |
| Acceptable media profiles | C | Indicating a set of acceptable conformance profiles for a 5G Media Streaming session.Present if no Media Entry Point is provided. This value is used by the Media Session Handler to select the appropriate Media Entry Point provided by the 5GMS AF. |

The 3GPP Service URL for 5G Media Streaming may also include information to support handling of eMBMS or MBS delivery.

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

## 4.11 Security architecture

### 4.11.1 General

The 5GMS architecture may support the Common API Framework (CAPIF) as specified in TS 23.222 [23222] for the interactions across security trust boundaries defined in clause 4.11.2.

### 4.11.2 Mapping of CAPIF to 5GMS architecture

#### 4.11.2.1 Provisioning a trusted 5GMS AF from a 5GMS Application Provider in the Trusted or External DN at reference point M1

Aligned with the provisions for securing northbound APIs defined in TS 33.122 [33122], access to the provisioning operations of the 5GMS AF at reference point M1 may be authorised by means of the OAuth 2.0 framework defined in RFC 6749 [RFC6749]. In this case, the CAPIF core function defined in TS 29.222 [29222] plays the role of authorization server, the 5GMS AF plays the role of resource server and the 5GMS Application Provider plays the role of client.

When CAPIF is supported at reference point M1, the 5GMS Application Provider in the Trusted or External DN shall be authenticated and authorised by the CAPIF core function before it is permitted to create, modify or remove the provisioned services in the trusted 5GMS AF at reference point M1. To successfully invoke provisioning operations at reference point M1, the 5GMS Application Provider is required to present a valid access token that has previously been issued to it by the CAPIF core function at CAPIF‑1/1e.



Figure 4.11.2.1-1: Mapping of 5G Media Streaming architecture to CAPIF
for 5GMS Application Provider provisioning trusted 5GMS AF

When CAPIF is supported at reference point M1, then:

- The 5GMS AF shall support the CAPIF API provider domain functions (i.e. CAPIF-2/2e, CAPIF-3, CAPIF-4 and CAPIF-5 as specified in TS 23.222 [33]).

- The Maf\_Provisioning service shall be exposed to the 5GMS Application Provider at reference point CAPIF-2/2e, realising reference point M1.

Procedures for provisioning access to the 5GMS AF are defined in clause 5.3.3 (downlink media streaming) and 6.2.2.3 (uplink media streaming).

#### 4.11.2.2 Configuring a trusted 5GMS AS from a 5GMS AF in the Trusted or External DN at reference point M3

Aligned with the provisions for securing northbound APIs defined in TS 33.122 [33122], access to the configuration operations of the 5GMS AS at reference point M3 may be authorised by means of the OAuth 2.0 framework defined in RFC 6749 [RFC6749]. In this case, the CAPIF core function defined in TS 29.222 [29222] plays the role of authorization server, the 5GMS AS plays the role of resource server and the 5GMS AF plays the role of client.

When CAPIF is supported at reference point M3, the 5GMS AF in the Trusted or External DN shall be authenticated and authorised by the CAPIF core function before it is permitted to create, modify or remove the configurations in the trusted 5GMS AS at reference point M3. To successfully invoke configuration operations at reference point M3, the 5GMS AF is required to present a valid access token that has previously been issued to it by the CAPIF core function at CAPIF‑1/1e.



Figure 4.11.2.2-1: Mapping of 5G Media Streaming architecture to CAPIF
for 5GMS AF provisioning trusted 5GMS AS

When CAPIF is supported at refernece point M3, then:

- The 5GMS AS shall support the CAPIF API provider domain functions (i.e. CAPIF-2/2e, CAPIF-3, CAPIF-4 and CAPIF-5 as specified in TS 23.222 [33]).

- The Mas\_Configuration service shall be exposed to the 5GMS AF at reference point CAPIF-2/2e, realising reference point M3.

Procedures for provisioning access to the 5GMS AS are defined in clause 5.3.X (downlink media streaming) and 6.2.2.X (uplink media streaming).

#### 4.11.2.3 Invoking a 5GMS AF in the Trusted DN from a Media Session Handler at reference point M5

Aligned with the provisions for securing southbound APIs defined in TS SS.NNN [SSNNN], access to the media session handling operations of the 5GMS AF at reference point M5 may be authorised by means of the OAuth 2.0 framework defined in RFC 6749 [RFC6749]. In this case, the [CAPIF core function defined in TS 29.222 [29222]|5GMS Application Provider] plays the role of authorization server, the 5GMS AF plays the role of resource server and the Media Session Handler plays the role of client.

When CAPIF is supported at reference point M5, the *Resource owner-aware Northbound API Access* (RNAA) model is recommended as defined in clause 6.2.3 of TS 23.222 [33]. The Media Session Handler in the 5GMS Client shall be authenticated and authorised by the CAPIF core function before it is permitted to invoke media session handling operations on the 5GMS AF at reference point M5. To successfully invoke media session handling operations at reference point M5, the Media Session Handler in the 5GMS Client is required to present a valid access token that has previously been issued to it by the CAPIF core function at CAPIF‑1.



Figure 4.11.2.3‑1: Mapping of 5G Media Streaming architecture to CAPIF
for a 5GMS Client accessing the 5GMS AF

When CAPIF is supported at reference point M5, then:

- The 5GMS AF shall support the CAPIF API provider domain functions (i.e. CAPIF-, CAPIF-3, CAPIF-4 and CAPIF-5 as specified in TS 23.222 [33]).

- The Maf\_SessionHandling service shall be exposed to the Media Session Handler in the 5GMS Client at reference point CAPIF-2e, realising reference point M5.

Procedures used by the 5GMS Application Provider to provision future access to the 5GMS AF by Media Session Handlers are defined in clause 5.3.3 (downlink media streaming) and 6.2.2.3 (uplink media streaming).

Procedures for authorising access to the 5GMS AF by the Media Session Handler under the control of the 5GMS-Aware Application are defined in clause 5.2.5 (downlink media streaming) and 6.3.3 (uplink media streaming).

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

### 5.2.5 Procedures for downlink media streaming with per-application authorisation of media session handling operations

#### 5.2.5.1 Overview

This clause defines procedures by which a 5GMSd Application Provider authorises a 5GMSd-Aware Application to invoke media session handling operations on the 5GMSd AF at reference point M5d.

#### 5.2.5.2 Authorisation of media session handling at M5d 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 instance can identify itself uniquely to the 5GMSd AF. The access token is provided, for example, during the login procedure or is requested at a later stage. The validity of access tokens is often limited in time. The 5GMSd-Aware Application may need to refresh the access token depending on the token validity.

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 authorised to invoke the operation.

When the OAuth 2.0 architecture [RFC6749] is used, the 5GMSd Application Provider acts as authorization server, the 5GMSd-Aware Application acts as client and the 5GMSd AF acts as resource server.

The call flow is depicted below.



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 authorisation may be cached/stored by the application, so that the user is not always challenged to provide the login credentials.)

NOTE 1: 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.

NOTE 2: Access tokens may be long-lived. The 5GMSd-Aware Application may need to refresh the access token, depending on its validity period.

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 access token may embed a user identifier, or the user identifier may be passed as separate (anonymised) parameter.

NOTE 3: The access token may be included as a parameter of the 3GPP Service URL used to launch media session handling (see table 4.10.2‑1).

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 request header.

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.)

#### 5.2.5.3 Authorisation of media session handling at M5d based on redirection

When the OAuth 2.0 [RFC6749] Authorization Code grant type is used, either the 5GMSd Application Provider or the 5GMSd AF acts as authorization server, as shown in figure 5.2.5.3‑1. The Media Session Handler acts as client and the 5GMSd AF acts as resource server.

|  |  |
| --- | --- |
|  |  |
| a. 5GMSd Application Provider acts as authorization server | b. 5GMSd AF acts as authorization server |

Figure 5.2.5.3‑1: Alternative deployments of authorization server

The call flow is depicted below.



NOTE: The AuthZ function is realised by the 5GMSd Application Provider or by the 5GMSd AF.

Figure 5.2.5.3‑2: Call flow for authorisation based on access token

1. 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 only the session access information.

2. When the Media Session Handler invokes a media session handling operation on the 5GMSd AF (M5 Service) at reference point M5...

3. ...the 5GMSd AF identifies that authorisation is required for accessing the requested service. The 5GMSd AF sends a redirect to the Media Session Handler, which is forwarded to the 5GMSd-Aware Application.

4. The 5GMSd-Aware Application requests an access token from the authorization server, which is realised either by the 5GMSd Application Provider (at reference point M8u) or by the 5GMSd AF (at reference point M5u).

5. After determining the policy rights of the requesting 5GMSd-Aware Application, the Authorization Service creates an access token and provides it to the 5GMSd-Aware Application.

6. The 5GMSd-Aware Application attempts to activate the media session handling operation again, this time providing the access token obtained in the previous step as an additional input paramrter.

7. The Media Session Handler invokes the media session handling operation again, this time providing the obtained access token.

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

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

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

### 5.3.3 Baseline provisioning procedure with authorisation of 5GMSd Application Provider

This clause describes the baseline procedure to provision the features using the 5GMS System with authorisation of the 5GMSd Application Provider to support subsequent authorisation of media session handling for downlink media streaming per clause 5.2.5. When CAPIF is used, the authorization server is realised by the CAPIF core function, as shown in figure 5.2.5.3‑1a. Otherwise, it is realised by the 5GMSd AF, as shown in figure 5.2.5.3‑1b.

|  |  |
| --- | --- |
| a. CAPIF core function acts as authorization server | b. 5GMSd AF acts asauthorization server |

Figure 5.3.3‑1: Alternative deployments of authorization server

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: Service Level Agreement (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.



NOTE: When CAPIF is used, the AuthZ function is realised by the Authorizaton Service of CAPIF Core Function. Otherwise, the AuthZ function is realised by the 5GMSd AF.

Figure 5.3.3-2: 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/authorisation procedures, e.g. as defined for CAPIF [13]. **The AuthZ subfunction of the5GMSd AF** **acts here as OAuth authorization server. The 5GMSd AF acts 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 authorised features.

4. The 5GMSd Application Provider specifies one or more 5GMSd features in the Provisioning Session.A set of authorised 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 \*\*\*\*

#### 6.2.2.3 Baseline provisioning procedure with authorisation

This clause describes the baseline procedure to provision the features using the 5GMS System with authorisation of the 5GMSu Application Provider to support subsequent authorisation of media session handling for uplink media streaming per clause 5.2.5.When CAPIF is used, the authorization server is realised by the CAPIF core function, as shown in figure 6.2.2.3‑1a. Otherwise, the authorization server is realised by the 5GMSu AF, as shown in figure 6.2.2.3-1b.

|  |  |
| --- | --- |
| a. CAPIF core function acts as authorization server | b. 5GMSd AF acts asauthorization server |

Figure 6.2.2.3‑1: Alternative deployments of authorization server

NOTE 1: Service Level Agreement (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 6.2.2.3-1: High-level procedure for provisioning the 5GMS System
for uplink media streaming sessions

Steps:

1. The 5GMSu Application Provider discovers the address (URL) of the 5GMSu AF (M1) for Session Provisioning. **During the self-onboarding procedure, the 5GMSu Application Provider obtains the API access credentials.**

2. The 5GMSu Application Provider authenticates itself with the system. This procedure reuses existing authentication/authorisation procedures, e.g., as defined for CAPIF [13] or by t**he 5GMSu AF** **acting as OAuth authorization server. The 5GMSu AF acts as OAuth resource server.** **The 5GMSu Application Provider obtains an access token which is used for any subsequent operation invocations at reference point M1.**

2. The 5GMSu Application Provider creates a Provisioning Session, providing its 5GMSu Application Provider identifier as input. 5GMSu Application Provider queries the capabilities and authorised features.

3. The 5GMSuApplication Provider specifies one or more 5GMSu features in the Provisioning Session. A set of authorised features is activated, such as content dynamic policy; network assistance; and content publishing (including egest).

 When the content publishing feature is offered and selected, the 5GMS Application Provider provides a Content Publishing Configuration to configure the content publishing behaviour of the 5GMSu AS (see next step), including selecting the uplink ingest protocol and format, content preparation and egest protocol and format.

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

 When the edge computing feature is offered and selected, the 5GMSu 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.

4. When content publication is desired, the 5GMSu AF interacts with the 5GMSu AS at reference point M3u to configure any necessary Server Certificates and/or Content Publishing Templates and to allocate resources for M2u egest protocol and format by means of a Content Publishing Configuration. The 5GMSu AS responds to the 5GMSu AF with the M2u content egest address.

5. The 5GMSu AF compiles the Service Access Information. The Service Access Information contains access details and options such as the Provisioning Session identifier, M5u (Media Session Handling) addresses for uplink entry point, dynamic policy, network assistance, etc.

6. The 5GMSu AF provides the results to the 5GMSu Application Provider.

The following steps:

7. When the 5GMSu Application Provider has selected full Service Access Information, the results are provided in the form of addresses and configurations for M2u (content egest), M5u (Media Session Handling) and M4u (Media Uplink Streaming). The 5GMSu Application Provider provides a subset of this information to the 5GMSu-Aware Application through M8u.

8. When the 5GMSu-Aware Application decides to activate the streaming service transmission, the Service Access Information is provided to the 5GMSu Client.

9. The 5GMSu Client requests the 5GMSu AF to initialise uplink media streaming (M5u), including reservation of any resources required for content preparation.

Or, alternatively:

10. The 5GMS-Aware Application requests the 5GMSu Client to start an uplink streaming session (M6u/M7u).

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

Then:

12. The 5GMSu Client streams the content to the 5GMSu AS.

13. When content publishing is offered and has been selected in step 4, the 5GMSu Application Provider can start retrieving the content from the M2u egest interface.

Optionally:

14. The 5GMSu Application Provider may update the Provisioning Session.

According to schedule, or upon request by the 5GMSu-Aware Application:

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

16. The 5GMSu AF sends a notification to the 5GMSu Client upon Provisioning Session termination.

The 5GMSu AF may request the creation or reuse of one or more network slices for ingesting the content of the provisioned session. If more than one network slice is provisioned for the ingest of the content of a session, the list of allowed S‑NSSAIs shall be conveyed to the target UE (e.g. through URSP or through M8u, step 7, or M5u, step 10).

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

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

## 6.3 Establishment of an uplink Media Streaming session

### 6.3.1 Overview

Editor’s Note: To be filled in.

### 6.3.2 Baseline procedure for establishment of an uplink media streaming session

The procedure allows a Media Streamer to establish an uplink streaming session with a 5GMSu AS.



Figure 6.3.2-1: Uplink media streaming session establishment

Steps:

1: During provisioning, the Media Streamer component of the 5GMSu Client is provisioned with basic information, such as the 5GMSu AF and 5GMSu AS addresses.

2: The 5GMSu-Aware Application acquires Service Access Information via reference point M8u or M5u according to the one of the procedures defined in clause 6.2.2.2.

3: The 5GMSu-Aware Application instructs the 5GMSu Client to start uplink media streaming according to one of the procedures defined in clause 6.2.2.2.

4: The 5GMSu Client establishes the uplink transport session.

5: The 5GMSu Client establishes the uplink media streaming session.

When client assistance is provisioned:

6: The 5GMSu Client establishes the assistance channel to the provisioned 5GMSu AF(s).

When server assistance is desired (e.g. for QoS or charging):

7: The 5GMSu AS establishes an assistance session with the 5GMSu AF.

8: The 5GMSu Client streams the content up to the 5GMSu AS.

### 6.3.3 Baseline procedure for establishment of an uplink media streaming session with per-application authorisation of media session handling operations

#### 6.3.3.1 Overview

This clause defines procedures by which a 5GMSu Application Provider authorises a 5GMSu-Aware Application to invoke media streaming operations on the 5GMSu AF at reference point M5u.

#### 6.3.3.2 Authorisation of media session handling at M5u based on access token

The 5GMSu Application Provider provides a different access token (e.g. a random string) via M8 to each 5GMSu-Aware Application, so that each application instance can identify itself uniquely to the 5GMSu AF. The access token is provided, for example, during the login procedure or is requested at a later stage. The validity of access tokens is often limited in time. The 5GMSu-Aware Application may need to refresh the access token depending on the token validity.

The 5GMSu-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 5GMSu AF. Upon receipt of such an access token, the 5GMSu AF verifies whether the access token is valid. If the token is valid, the 5GMSu-Aware Application is authorised to invoke the operation.

When the OAuth 2.0 architecture [RFC6749] is used, the 5GMSu Application provider acts as authorization server, the 5GMSu-Aware Application acts as client and the 5GMSu AF acts as resource server.

The procedure allows a Media Streamer to establish an uplink streaming session with a 5GMSu AS.



Figure 6.3.3-1: Uplink Streaming Session Establishment

Steps:

1: During provisioning, the Media Streamer component of the 5GMSu Client is provisioned with basic information, such as the 5GMSu AF and 5GMSu AS addresses.

2: 5GMSu-Aware Application seeks authorisation from the 5GMSd Application Provider providing, for example, a username and a password.

3: Upon successful authorisation, the 5GMSu-Aware Application obtains an uid and a token.

NOTE: Access tokens may not be long-lived. The 5GMSu-Aware Application may need to refresh the access token periodically, depending on its validity lifetime.

4: The 5GMSu-Aware Application acquires Service Access Information via reference point M8u or M5u according to the one of the procedures defined in clause 6.2.2.2.

5: The 5GMSu-Aware Application instructs the 5GMSu Client to start uplink media streaming according to one of the procedures defined in clause 6.2.2.2.

6: The 5GMSu Client establishes the uplink transport session.

7: The 5GMSu Client establishes the uplink media streaming session.

8: The provided access token is verified.

When client assistance is provisioned:

9: The 5GMSu Client establishes the assistance channel to the provisioned 5GMSu AF(s).

When server assistance is desired (e.g. for QoS or charging):

10: The 5GMSu AS establishes an assistance session with the 5GMSu AF.

11: The 5GMSu Client streams the content up to the 5GMSu AS.

#### 6.3.3.3 Authorisation of media session handling at M5u based on redirection

When the OAuth 2.0 [RFC6749] Authorization Code grant type is used, either the 5GMSu Application Provider or the 5GMSu AF acts as authorization server, as shown in figure 6.3.3.3‑1. The Media Session Handler acts as client and the 5GMSu AF acts as resource server.

|  |  |
| --- | --- |
|  |  |
| a. 5GMSu Application Provider acts as authorization server | b. 5GMSu AF acts as authorization server |

Figure 6.3.3.3‑1: Alternative deployments of authorization server

The call flow is depicted below.



Figure 5.2.5.3‑1: Call flow for authorisation based on access token

1. When the 5GMSu-Aware Application (immediately or later) invokes the Media Session Handler to activate media session handling for a media delivery session, the application passes only the session access information.

2. When the Media Session Handler invokes a media session handling operation on the 5GMSu AF at reference point M5u.

3. The 5GMSu AF identifies that authorization is required for accessing the requested service. The 5GMSu AF sends a redirect to the Media Session Handler, which is forwarded to the 5GMSu-Aware Application.

4. The 5GMSu-Aware Application requests an access token from the authorization server, which is realised either by the 5GMSu Application Provider (at reference point M8u) or by the 5GMSu AF (at reference point M5u).

5. After determining the policy rights of the requesting 5GMSu-Aware Application, the authorization server creates an access token and provides it to the 5GMSu-Aware Application.

6. The 5GMSu-Aware Application attempts to activate the service again, this time providing the access token obtained in the previous step as an additional input parameter.

7. The Media Session Handler invokes the media session handling operation again, this time providing the obtained access token.

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

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

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