**3GPP TSG- S4 Meeting #117e *S4-220148***

**, 17th February – 23rd February 2022**

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| *CR-Form-v12.2* | | | | | | | | |
| **Pseudo CHANGE REQUEST** | | | | | | | | |
|  | | | | | | | | |
|  | **26.804** | **CR** | **<CR#>** | **rev** | **<Rev#>** | **Current version:** | **<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 |  | Radio Access Network |  | Core Network |  |

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | | | | | | | | | | |
| ***Title:*** | [FS\_5GMS\_EXT]: Per App authorization | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Source to WG:*** | Ericsson LM | | | | | | | | | |
| ***Source to TSG:*** | S4 | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Work item code:*** | <Related\_WIs> | | | | |  | ***Date:*** | | | <Res\_date> |
|  |  | | | |  | |  | | |  |
| ***Category:*** | **<Cat>** |  | | | | | ***Release:*** | | | <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-16 (Release 16) Rel-17 (Release 17) Rel-18 (Release 18) Rel-19 (Release 19)* | |
|  |  | | | | | | | | | |
| ***Reason for change:*** | |  | | | | | | | | |
|  | |  | | | | | | | | |
| ***Summary of change:*** | | The intention of this pCR is to progress the authorization aspects for some 5G Media Streamig services. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Consequences if not approved:*** | |  | | | | | | | | |
|  | |  | | | | | | | | |
| ***Clauses affected:*** | |  | | | | | | | | |
|  | |  | | | | | | | | |
|  | | **Y** | **N** |  | | | |  | | |
| ***Other specs*** | |  |  | Other core specifications | | | | TS/TR ... CR ... | | |
| ***affected:*** | |  |  | Test specifications | | | | TS/TR ... CR ... | | |
| ***(show related CRs)*** | |  |  | O&M Specifications | | | | TS/TR ... CR ... | | |
|  | |  | | | | | | | | |
| ***Other comments:*** | |  | | | | | | | | |
|  | |  | | | | | | | | |
| ***This CR's revision history:*** | |  | | | | | | | | |

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

# 2 References

The following documents contain provisions which, through reference in this text, constitute provisions of the present document.

[87] Roger Pantos and William May, Jr., "HTTP Live Streaming", RFC 8216, August 2017.

[O1] IETF RFC 6749: "The OAuth 2.0 Authorization Framework".

[O2] IETF RFC 6750: "The OAuth 2.0 Authorization Framework: Bearer Token Usage".

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

## 5.9 Per-application-authorization

### 5.9.1 Description

Operation of certain 5GMSA and 5G System enabled services include an SLA between the Application Provider and the 5GMS System provider. Different solutions to enable per-application authorization should be studied. “Per-application authorization” refers to scenarios where one or more 5GMS-Aware Applications are hosted on the same UE (e.g. a SmartPhone) and may access services only from the associated 5GMS Application Provider.

The 5G System provider may offer one common 5GMSd AF or dedicated 5GMSd AFs. In the later case, the one 5GMSd AF instance services only a single 5GMSd Application Provider.

A set of example collaboration scenarios is described in the following clause.

OAUTH 2.0 [O1][O2] is commonly used to provide authorization to REFTful HTTP APIs. OAUTH separates the authorization server from the resource server. This typically simplifies deployments, since not every resource server such as HTTP server needs to also provide authorization functionality. The separation of the authorization server from the resource server allows reusing access credentials for different services or between different parties.

The OAUTH 2.0 architecture defines four main roles:

- *Resource Owner:* A user or entity which can authorize access to a resource.

- *Resource Server:* A function hosting the (protected) resource.

- *Client:* A function which desires to access the resource hosted on the resource server.

- *Authorization Server:* A function which authenticates the resource owner and provides different types of access tokens.

The roles can be visualized by the following example: A user stores some personal photos on cloud storage. When the user wants to print a photo using an external print service, rather than downloading the photo onto a local drive and then uploading the photo to the print service, the user can instead authorize the print service to fetch the photo from the protoected cloud storage. The resource owner here is the user. The resource server is the cloud storage. The print service is the client.

The 5GMS aware Application subsidizes access to QoS and other network resources for its own applications. To make sure only authorized applications are allowed to access these provisioned reousrces, it offers/configures an authorization server that will be used to authorize access to the network assistance resources provided by the 5GMS AF. The 5GMS AF acts as the *Resource Server*. The 5GMS aware Application acts as the *Resource Owner*, as it owns the Provisioning Session, which defines the QoS and charging policies. The *Client* is the MSH. The usage of OAuth 2.0 for the purpose of authorzing access to Network Function services is defined by SA3 in TS33.501 section 13.4.

### 5.9.2 Collaboration Scenarios

#### 5.9.2.1 Collaboration A: UE hosting multiple Applications

This collaboration scenario focuses on cases where one or more 5GMSd-Aware Applications are hosted on the same UE and are using the same 5GMSd Client. This may be the case when the 5GMSd Client is provided as an Operating System level service. The 5GMSd Client supports isolation of the different 5GMSd-Aware Applications.



Figure 5.9.2-1: Per-Application Authorization Collaboration Scenario

Each 5GMSd-Aware Application uses an M8d reference point instance to connect to its 5GMSd Application Provider.

The 5G System provider offers a common 5GMSd AF within the trusted DN. The 5GMSd AF supports request and provider isolation so that 5GMSd Application Provider #1 and #2 are not interfering with each other. For example, 5GMSd Application Provider#1 has agreed different charging conditions than Provider #2 and the 5G System should ensure that only 5GMSd-Aware Application #1 can benefit from the conditions. Another example is different QoS levels, e.g. 5GMSd-Aware Application #1 is entitled to receive higher QoS than Application #2.

#### 5.9.2.2 Collaboration B: Applications with multiple subscription levels

This collaboration scenario focuses on cases where an Application Provider is offering multiple subscription levels to its consumers, for example 4K Premium or SD Standard QoS. This example is inspired by the use case from TS 26.512 [16], Annex A.2.

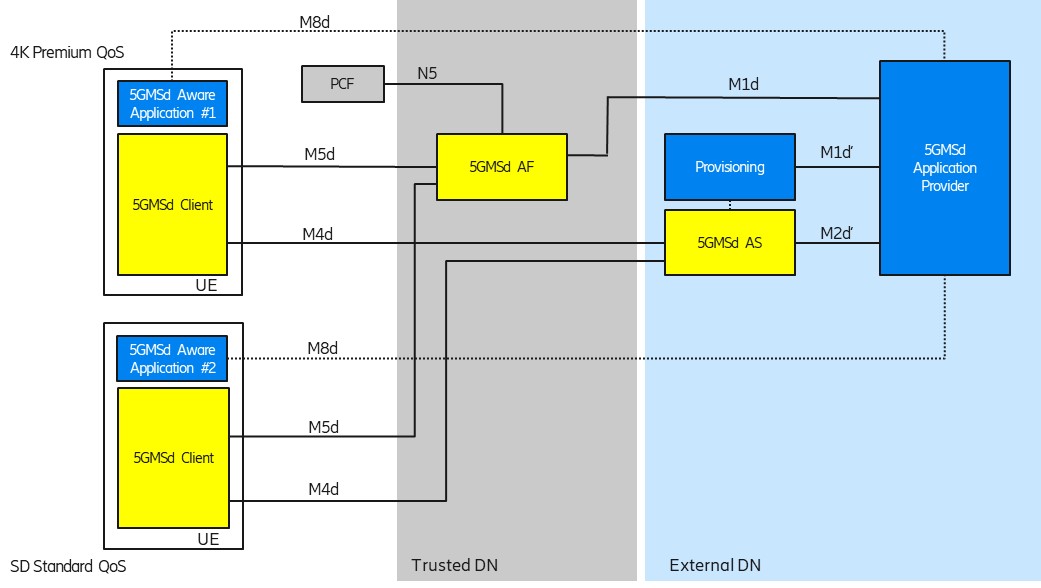


Figure 5.9.2-2: Per-Application Authorization Collaboration Scenario

Each 5GMSd-Aware Application uses an M8d reference point instance to connect to its 5GMSd Application Provider. The 5GMSd Application Provider is aware about the different subscription levels of the user.

The 5G System provider offers a common 5GMSd AF within the trusted DN. The 5GMSd AF needs to determine that 5GMSd Aware Application #1 is entitled to higher bit rates than 5GMSd-Aware Application #2.

### 5.9.3 Role distribution in the 5GMS deployments

The 5G Media Streaming architecture can be used for different application service offerings. Annex A in TS 26.512 [16] describes three different Dynamic Policy usage examples: Premium QoS, Conditional Zero Rating and Background Download. In all the three cases, different network features are used to realise the Dynamic Policy, e.g. an increase in network resource utilization when consuming HD content with the corresponding network QoS.

It is assumed in all three examples that the 5GMS Application Provider (and the Application Service Provider) has an agreement with the 5G System provider to use the relevant network feature.

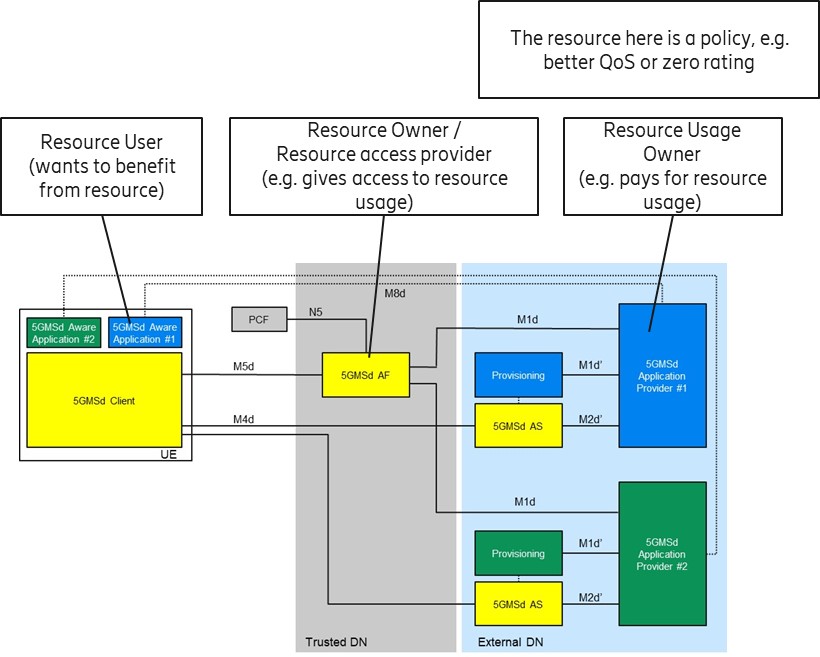


Figure 5.9.3-1: Applying rolls for 5G Media Streaming Architecture functions

Figure 5.9.2-1 illustrates the different roles and responsibilities:

- The resource in question is a network policy.

- The 5G System Provider is the resource owner in this case, since it provides the 5G connectivity service.

- The 5GMSd-Aware Application is the Resource User. It instructs the 5GMSd Client to activate a certain dynamic policy, based on the service subscription and the selected content.

- The 5GMS Application Provider is the Resource Usage Owner. It checks that the requested dynamic policy matches the application service subscription. For example (with reference to clause A.2 in TS 26.512 [16]), when the user has an HD video subscription, the user should only be authorised to activate a dynamic policy corresponding to the HD operating point.

### 5.9.4 Mapping to 5G Media Streaming and High-Level Call Flows

Editor’s Note: Map the key topics to basic functions and develop high-level call flows.

### 5.9.5 Potential open issues

Editor’s Note: Identify the issues that need to be solved.

### 5.9.6 Candidate Solutions

#### 5.9.6.1 General

#### 5.9.6.2 Solution 1: Use of a Callback for authorization

This solution is based on the concept that the 5GMS AF can contact the 5GMS Application Provider (ASP) whenever a new Dynamic Policy is activated by a 5GMS Client.

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

When activating a Dynamic Policy, the 5GMS-Aware Application passes the token (via an M6 API call) to the Media Session Handler. When the Media Session Handler desires to activate a dynamic policy, it presents the authorization token to the 5GMS AF by invoking an M5 operation. Upon receit of such a token, the 5GMS AF executes a callback to the 5GMS Application Provider in order to verify, whether this authorization token is valid. When the token is valid, the UE application is authorized to activate this policy.

The authorization token is provided e.g. during the login procedure or is requested at a later stage. The UE Application may fetch metadata for the media assets at some stage.

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



Figure 5.9.6.2-1: Usage of a callback for policy activation authorization

The steps are as follows:

1. When the user wants to use the 5GMS-Aware Application to consume e.g. video content, the user needs to authenticate with the application and the 5GMS Application Provider. (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. The 5GMS 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 5GMS Application Provider creates an authorization token and passes this token together with the login response back to the application.

3. When the 5GMS-Aware Application (immediately or later) invokes the Media Session Handler to activate the network service from the 5GMS AF, the application passes the authorization token to the Media Session Handler. The authorization token can embed a user identifier, or the user identifier may be passed as separate (anonymised) parameter.

4. When the Media Session Handler activates a dynamic policy, it provides the the token to the 5GMS AF, e.g. as an HTTP query parameter.

5. The 5GMS AF then verifies the authorization token with the 5GMS Application Provider, using a callback function.

This callback URL can be stored by the 5GMS AF together with the Policy Template parameters so that the use of the network policy resource can be revalidated periodically with the 5GMSd Application Provider.

6. When the 5GMS AF has verified that the 5GMS Aware Application is authorized to active the dynamic policy (based on the token), the 5GMS AF invokes the appropriate procuedres on the NEF or PCF. For example, the 5GMS AF triggers the addition of a QoS flow by invoking the Nnef\_AFsessionWithQoS service.

#### 5.9.6.3 Solution 2: Time-limited authorization token provisioning

In order to reduce the number of callbacks, tokens with a limited validity duration may be provisioned with the 5GMS AF and the 5GMS-Aware Applications.

In this solution the 5GMSd Application Provider provisions a set of valid authorization tokens, including expiry time, in the 5GMS AF in advance via M1.

As in Solution 1, the Media Session Handler passes an authorization token when invoking the 5GMS AF at M5. The 5GMA AF authorizes the Media Sesssion Handler’s request based on this token.

Since the token validity is time-limited, the 5GMS Application Provider must periodically update the set of valid authorization tokens provisioned at the 5GMS AF and the 5GMS-Aware Application is responsible for refreshing the token used by the Media Session Handler. For example, the application may be configured to periodically fetch a new token from the 5GMS Application Provider.



Figure 5.9.6.3-1: Usage of time-limited tokens for policy activation authorization

The steps are as follows:

1. The 5GMS Application Provider provisions tokens on the 5GMS AF before any 5GMS-Aware Application tries to activate any Dyanmic Policy. The token is provisioned together with the Policy Template definitions.

2. When a user (and the 5GMS-Aware Application) successfully authenticates with the 5GMS Application Provider, the 5GMS-Aware Application receives a time-limited authorization token. The 5GMS-Aware Application typically stores the token.

The difference with Solution 1 is the use of the token by the 5GMS AF:

3. When a 5GMS-Aware Application wishes to activate a Dynamic Policy, it provides the authorization token to the 5GMS AF. The 5GMS AF then validates the token using a simple lookup against it list of currently valid tokens without reference to the 5GMS Application Provider.

### 5.9.7 Conclusions

The Key Issue explores the usage of OAuth 2.0 for per-application authorization of different 5G System features. It is recommended to specify the usage of OAuth 2.0 (according to the SA3 guidelines) within a normative work item.

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