**3GPP TSG-SA5 Meeting #156 *S5-244755***

**, , -**

**Source: Nokia**

**Title: Rel-19 pCR TR 28.879 Add solution for authorization of the external MnS consumer to access the management service API use case**

**Document for: Approval**

**Agenda Item: 6.19.21**

# 1 Decision/action requested

***In this box give a very clear / short /concise statement of what is wanted.***

# 2 References

[1] 3GPP TR 28.879, " Study on OAM for service management and exposure to external consumers".

# 3 Rationale

This pCR proposes to add a solution for the authorization of the external MnS consumer to access the management service API use case in clause 5.1.4 of TR 28.879 [1].

# 4 Detailed proposal

It is proposed that the following changes be made in clause 5.1.4 of TR 28.879 [1].

|  |
| --- |
| **First Change** |

### 5.1.4 Use case #4: Authorization of the external MnS consumer to access the management service API

#### 5.1.4.1 Description

After the external MnS consumer has discovered the available management services (now service APIs) at the CCF, the external MnS consumer proceeds to request the CCF for the authorization information to access the service API (see clause 8.11 of TS 23.222 [5] and clause 6.5.2.3 of TS 33.122 [14]) via the CAPIF-1e interface. This authorization information contains the actions (e.g., ALLOW, DENY) the external MnS consumer can perform on the discovered MnS producer. These actions might differ from what the external MnS consumer is authorized to discover from the CCF (depending on the configured discovery policy). However, currently, the CCF does not have this authorization information in order to generate the access token to grant external MnS consumers accessto the discovered service APIs (i.e., the management services).

Furthermore, after receiving the authorization information from the CCF, the external MnS consumer will proceed to access the management service at the MnS producer (the MnS producer is the CAPIF API exposing function (AEF)) via the CAPIF-2e interface. This implies that the MnS producer should be able to support the CAPIF-2e interface; however, it is safe to assume that this is already supported.

#### 5.1.4.2 Potential requirements

**PREQ-FS\_MExpo-Auth-01:** The 3GPP management system shall provide the CCF with the authorization information for an external MnS consumer.

#### 5.1.4.3 Potential solutions

###### 5.1.4.3.i.1 Introduction

This potential solution describes how the CCF can authorize the external MnS consumer to access the management service API.

###### 5.1.4.3.i.2 Description

To authorize an external MnS consumer to consume management service(s) at the MnS producer, the CCF can use the AccessRule class (defined in clause 7.3.3 in TS 28.319 [29]) to define the access rule for authorization. This access rule is identified by the ruleName attribute. The dataNodeSelector attribute of the AccessRule class can be used to select the resources to which the access rule will apply. These resources are either the managed objects (IOCs), instances of managed objects (MOIs), or their corresponding attribute(s).

For the selected resources under the dataNodeSelector attribute, the operations attribute is used to specify the operations (as specified in clause 11.1.1 in TS 28.532[17]) that can be applied to these resources.

For each resource and operation combination, the actions attribute permits what operation(s) the the external MnS consumer can perform on the resource.

To request for authorization to consume a specific service API, the external MnS consumer sends a "service API authorization request" (see clause 8.11 of TS 23.222[5]) to the CCF. The request should include the information provided in Table 5.1.4.3.i.2-1.

Table 5.1.4.3.i.2-1: Definition of type AccessTokenReq (Table extract from Table 8.5.4.2.6-1in TS 29.222 [13])

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Attribute name | Data type | P | Cardinality | Description | Equivalent MnS Info IOC attribute/comments |
| grant\_type | string | M | 1 | This attribute shall contain the grant type as "client\_credentials", or when the "RNAA" feature is supported, either "client\_credentials" or "authorization\_code".  (NOTE 3, NOTE 4) | Should be set to "client\_credentials" |
| client\_id | string | M | 1 | This attribute shall contain the API invoker Identifier.  (NOTE 3) | This is the same as the API invoker Id. |
| resOwnerId | ResOwnerId | O | 0..1 | Contains the identifier of the resource owner.  This attribute shall be present only when the access token request is used for RNAA. |  |
| client\_secret | string | O | 0..1 | This attribute when present shall contain the onboarding secret which is got during API invoker onboarding.  (NOTE 3) |  |
| scope | string | O | 0..1 | This attribute when present shall contain a list of AEF identifiers and its associated API names for which the access\_token is authorized for use.  It takes the format of 3gpp#aefId1:apiName1,apiName2,…apiNameX;aefId2:apiName1,apiName2,…apiNameY;…aefIdN:apiName1,apiName2,…apiNameZ  Using delimiter "#" after the discriminator "3gpp", ":" after AEF identifier, "," between API names and ";" between the last API name of the previous AEF identifier and the next AEF identifier. (NOTE 2)  Example: '3gpp#aef-jiangsu-nanjing:3gpp-monitoring-event,3gpp-as-session-with-qos;aef-zhejiang-hangzhou:3gpp-cp-parameter-provisioning,3gpp-pfd-management' |  |
| authCode | string | C | 0..1 | Contains the authorization code.  This attribute shall be included only when the access token request is used for RNAA and the OAuth "authorization code" grant type is used. | RNAA |
| redirect\_uri | string | O | 0..1 | Contains the redirection URI that was used to obtain the authorization code provided within the "authCode" attribute.  This attribute may be included only when the access token request is used for RNAA and the OAuth "authorization code" grant type is used.  (NOTE 3) | RNAA |
| NOTE 1: This data structure shall not be treated as a JSON object. It shall be treated as a key, value pair data structure to be encoded using x-www-urlencoded format as specified in clause 17.13.4.1 of W3C HTML 4.01 Specification [22].  NOTE 2: The scope may contain more space-delimited strings which further add additional access ranges to the scope, the definition of those additional strings is out of the scope of the present document.  NOTE 3: The "grant\_type", "client\_id", "client\_secret" and "redirect\_uri" attributes do not follow the related naming convention defined in clause 7.2.1. These attributes are however kept as currently defined in this specification in order to keep them aligned with corresponding claims defined in IETF RFC 6749 [23] and for backward compatibility considerations.  NOTE 4: The enumeration value "client\_credentials" or "authorization\_code" of the "grant\_type" attribute does not follow the related naming convention defined in clause 7.2.1. This enumeration is however kept as currently defined in this specification for backward compatibility considerations. | | | | |  |

When the CCF receives the "service API authorization request" (see clause 8.11 of TS 23.222[5]) from the external MnS consumer, the CCF first validates the request and generates the access token. Upon generating the access token, the CCF sends the "service API authorization response" with the access token information to the external MnS consumer. The generated access token is structured according to the information provided in Table 5.1.4.3.i.2-2.

Table 5.1.4.3.i.2-2: Access token response message parameters (Table extract from Table 8.5.4.2.7-1in TS 29.222 [13])



|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Attribute name | Data type | P | Cardinality | Description | Equivalent MnS Info IOC attribute/comments |
| access\_token | string | M | 1 | This IE shall contain JWS Compact Serialized representation of the JWS signed JSON object containing AccessTokenClaims (see clause 8.5.4.2.8).  (NOTE 2) |  |
| token\_type | string | M | 1 | This IE shall contain the token type (i.e. "Bearer").  (NOTE 2, NOTE 3) |  |
| expires\_in | DurationSec | M | 1 | This IE when present shall contain the number of seconds after which the access\_token is considered to be expired.  (NOTE 2) |  |
| scope | string | O | 0..1 | This IE when present shall contain a list of AEF identifiers and its associated API names for which the access\_token is authorized for use.  It takes the format of 3gpp#aefId1:apiName1,apiName2,…apiNameX;aefId2:apiName1,apiName2,…apiNameY;…aefIdN:apiName1,apiName2,…apiNameZ  Using delimeter "#" after the discriminator "3gpp", ":" after AEF identifier, "," between API names and ";" between the last API name of the previous AEF identifier and the next AEF identifier. (NOTE 1)  Example: '3gpp#aef-jiangsu-nanjing:3gpp-monitoring-event,3gpp-as-session-with-qos;aef-zhejiang-hangzhou:3gpp-cp-parameter-provisioning,3gpp-pfd-management' | This scope contains information that will be used by the management system to enforce authorization to consume management services. |
| NOTE 1: The scope may contain more space-delimited strings which further add additional access ranges to the scope, the definition of those additional strings is out of the scope of the present document.  NOTE 2: The "access\_token", "token\_type" and "expires\_in" attributes do not follow the related naming convention defined in clause 7.2.1. These attributes are however kept as currently defined in this specification for backward compatibility considerations.  NOTE 3: The enumeration value "Bearer" of the "token\_type" attribute does not follow the related naming convention defined in clause 7.2.1. This enumeration is however kept as currently defined in this specification for backward compatibility considerations. | | | | |  |

To consume the management service, the external MnS consumer provides the generated access token to the MnS producer via the CAPIF-2 interface (following the procedures described in clause 8.16 of TS 23.222[5]).

|  |
| --- |
| **End of Change** |