**3GPP TSG-SA5 Meeting #156 *S5-244751***

**, , -**

**Source: Nokia**

**Title: Rel-19 pCR TR 28.879 Updating the configuring discovery policy for an external MnS consumer 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 update clause 5.1.3 of TR 28.879 [1] in the following ways:

1) Replacing the term discovery policy by configured access control rules in order to be consistent with the terms already used in the access control of management services.

2) Ensuring that the use case is focused only on configuring the access control rules to enable the discovery of the management services at the CCF by the external MnS consumer after onboarding (as the use case name implies).

# 4 Detailed proposal

It is proposed that the following changes be made in clause 5.1.3 of TR 28.879 [1].

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

### 5.1.3 Use case #3: Configuring discovery information of an external MnS consumer.

#### 5.1.3.1 Description

The operator may not want that all service APIs published into CAPIF are discoverable to all API invokers; in fact, the operator may want to limit the visibility that certain API invokers have over published API information, according to the business agreements settled with the stakeholder owning the API invoker. To that end, the CCF shall be able to be configured with discovery information on a per API invoker basis. The discovery information, allows to specify the visibility for an API invoker, and therefore filter which service API information this API invoker can:

* Subscribe to, during the API invoker onboarding.

- Discover and subsequently access, once API invoker gets onboarded. Upon receiving a discovery request from the API invoker with certain query information (i.e., criteria for discovery matching service APIs), the CCF will apply the configured discovery information on the search results matching the query criteria and filter them accordingly.

When using the CAPIF as the framework to expose MnSs, the external MnS consumer plays the role of API invoker, and the published API information corresponds to the MnS information published into CCF compliant with ServiceAPIDescription (clause 8.2.4.2.2 from [5]). Likewise, for the cases where CAPIF and 3GPP management system belong both to the same administrative domain, the 3GPP management system administrator [29] also acts as CAPIF administrator.

However, there are two issues that deserve further analysis.

On the one hand, it is needed to discuss how 3GPP management system can help define discovery information for each external MnS consumer. The aim of the configured discovered informations is to limit their visibility over the published MnS information. The configured discovery information can define filters at two levels:

- First, the discovery information allows configuring which resources are made discoverable to the external MnS consumer. For each MOI which is under the management scope of the published MnS, the discovery information specifies whether the MOI is visible or not.

- Secondly, for each visible MOI, the discovery information allows limiting what the external MnS consumer can see regarding:

- CRUD operations and/or notifications associated to the MOI.

- Management data, e.g. performance and fault information, associated to the MOI.

On the other hand, it is needed to discuss how a defined discovery information can be configured on the CCF. This association allows setting the visibility that this API invoker will have over its lifetime, from onboarding to offboarding, including all stages in between. If needed, the discovery information can be updated over the API invoker’s lifetime.

#### 5.1.3.2 Potential requirements

**PREQ-FS\_MExpo-Disc-01:** The 3GPP management system shall provide the capability to configure which MOIs, among those ones that are within the scope of a published MnSs, are visible to an external MnS consumer. The filtered set of MOIs is referred to as discoverable MOIs.

**PREQ-FS\_MExpo-Disc-02:** The 3GPP management system shall provide the capability to configure, for a discoverable MOI, which attributes supported by this MOI are visible to an external MnS consumer.

**PREQ-FS\_MExpo-Disc-03:** The 3GPP management system shall provide the capability to configure, for a discoverable MOI, which CRUD operations associated to this MOI are visible to an external MnS consumer.

**PREQ-FS\_MExpo-Disc-04:** The 3GPP management system shall provide the capability to configure, for a discoverable MOI, which notifications associated to this MOI are visible to an external MnS consumer.

**PREQ-FS\_MExpo-Disc-05:** The 3GPP management system shall provide the capability to configure, for a discoverable MOI, which management data associated to this MOI are visible to an external MnS consumer.

NOTE: The above listed requirements are based on those originally defined in 3GPP TS 28.319 [29], but now applicable for external MnS consumers.

**PREQ-FS\_MExpo-Disc-06:** The 3GPP management system shall provide the means to map the configuration associated to discoverable MOIs to appropriate OAuth 2.0 access token.

#### 5.1.3.3 Potential solutions

##### 5.1.3.3.1 Potential solution #1: Using AccessRule class to support discovery information definition

###### 5.1.3.3.1.1 Introduction

AccessRule class (TS 28.319 [29], clause 7.3.3) enables providing granular control on what actions are visible over which resources, when certain conditions (filter criteria) are met. The table below provides a summary of the class attributes.

|  |  |
| --- | --- |
| **Attribute Name** | **S** |
| ruleName | M |
| dataNodeSelector | M |
| operations | M |
| actions | O |
| componentCData | O |

The different AccessRule instances are defined at design time and stored in a database accessible by 3GPP management system. An example of this database can be the operator’s Authentication, Authorization and Accounting (AAA) server.

This solution proposes using the existing AccessRule class to define discovery information for external MnS consumer. With this solution, it is proposed to fulfil the requirements PREQ-FS\_MExpo-Disc-01, PREQ-FS\_MExpo-Disc-02, PREQ-FS\_MExpo-Disc-03, PREQ-FS\_MExpo-Disc-04 and PREQ-FS\_MExpo-Disc-05.

###### 5.1.3.3.1.2 Description

It is proposed to use AccessRule to generate discovery information as follows:

- “dataNodeSelector”: it can be used not only to configure which MOI are visible (first level of filter), but also the visibility over the attributes of these MOIs. This allows fulfilling PREQ-FS\_MExpo-Disc-01 and PREQ-FS\_MExpo-Disc-02.

- “operations”: it can be used to specify which CRUD operations and/or notifications are visible for each MOI listed in the dataNodeSelector. This allows fulfilling PREQ-FS\_MExpo-Disc-03 and PREQ-FS\_MExpo-Disc-04.

- “componentCData”: it can be used to specify which management data are visible for each MOI listed in the dataNodeSelector. This allows fulfilling PREQ-FS\_MExpo-Disc-05.

- “actions”: The usage of this attribute is to grant authorization to the external MnS consumer when accessing service APIs over CAPIF-2/2e interface. However, this is a separate use case.

How “dataNodeSelector”, “operations” and “componentCData” are specifically mapped to generate the policy depends on the policy format decided by the operator. This format is not standardized.

##### 5.1.3.3.2 Potential solution #2: Using Role class for discovery information definition

###### 5.1.3.3.2.1 Introduction

Role class (TS 28.319 [29], clause 7.3.2) enables capturing multiple access rules. The table below provides a summary of the class attributes.

|  |  |
| --- | --- |
| **Attribute Name** | **S** |
| roleName | M |
| **Attribute related to role** |  |
| accessRulesList | M |

The different Role instances are defined at design time and stored in a database accessible by 3GPP management system. Examples of this database can be the operator’s Authentication, Authorization and Accounting (AAA) server.

This solution proposes using the existing Role class to define access control rules for external MnS consumer. With this solution, it is proposed to fulfil the requirements PREQ-FS\_MExpo-Disc-01, PREQ-FS\_MExpo-Disc-02, PREQ-FS\_MExpo-Disc-03, PREQ-FS\_MExpo-Disc-04 and PREQ-FS\_MExpo-Disc-05.

###### 5.1.3.3.2.2 Description

This solution is similar as in clause 5.1.3.3.1, with the exception that the discovery informations conveys information from the access rules associated to this role.

##### 5.1.3.3.3 Potential solution #3: Mapping policy definition into OAuth2.0 access token.

###### 5.1.3.3.3.1 Introduction

This solution focuses on meeting the requirement PREQ-FS\_MExpo-Disc-06.

###### 5.1.3.3.3.2 Description

The discovery policy is configured on the CCF, so the CCF can limit what the external MnS consumer can subscribe to (during the API invoker onboarding) and discover and subsequently access (once the API invoker gets onboarded). This configuration can be accomplished through OAuth 2.0 access token. The details and usage of this token when used in CAPIF are defined in 3GPP TS 33.122 [14] and shown in the table below (see Table C.2.2-1 from 3GPP TS 33.122 [14]).

|  |  |
| --- | --- |
| Parameter | Description |
| exp | REQUIRED. The expiration time of the access token. Implementers MAY provide for some small leeway, usually no more than a few minutes, to account for clock skew (not to exceed 30 seconds). |
| client\_id | REQUIRED. The identifier of the API Invoker making the API request as previously established with the CAPIF Core Function through onboarding. |
| scope | REQUIRED. A string containing a space-delimited list, comprising of the following as scopes associated with this token:  - List of Services per AEF (e.g. “AEF1:Service1,Service2,Service3,...,ServiceX;  AEF2:Service1,Service2,Service3,...,ServiceZ”) |

To configure the policy on the CCF, it is proposed to use scope parameter, which is a string containing a space-delimited list. The configuration can be done, for example by the CAPIF administrator, for the cases where this administrator is also administrator of the 3GPP management system (see TS 28.319 [29]).

Once configured with the discovery policy, the CCF can use the policy with the external MnS consumer over CAPIF-1 interface.

#### 5.1.3.4 Evaluation of potential solutions

Solutions #1 and #2 allow fulfilling the requirements PREQ-FS\_MExpo-Disc-01, PREQ-FS\_MExpo-Disc-02, PREQ-FS\_MExpo-Disc-03, PREQ-FS\_MExpo-Disc-04 and PREQ-FS\_MExpo-Disc-05, providing controllable granularity on which published MnS information can be consumed by an external MnS consumer.

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