**3GPP TSG-SA5 Meeting #155 *S5-24325d1***

Jeju, South Korea, 27 - 31 May 2024 Revision of S5-242839

**Source: Ericsson España S.A.**

**Title: pCR TR 28.879 Configuring discovery policy for an external MnS consumer**

**Document for: Approval**

**Agenda Item: 6.19.21**

# 1 Decision/action requested

***The group is asked to discuss and approve the proposal.***

# 2 References

[1] SP-231728: "New SID: Study on Enhanced OAM for management exposure to external consumers".

[2] 3GPP TR 28.879: " Study on OAM for service management and exposure to external consumers".

[3] 3GPP TS 23.222: "Functional architecture and information flows to support Common API Framework for 3GPP Northbound APIs; Stage 2"

[4] 3GPP TS 29.222: "Common API Framework for 3GPP Northbound APIs; stage 3"

# 3 Rationale

Among the study objectives in [1], WT-1 is focused on communication services and the relationship with network provisioning solutions such as network slicing, from concept and modelling viewpoints. The actual sub-objectives defined within WT-1 are detailed below:

“

* ***WT-1.1*** *Identify generic requirements for exposure of SA5 management services to external consumers, irrespective of the vertical industry.*
* ***WT-1.2*** *Identify 1) potential mechanisms to discover management service producers and their respective capabilities while leveraging as much as possible the existing solutions and extending where necessary. Compare existing solutions (e.g., CAPIF, EGMF, MnS Registry and/or MSAC) that could be leveraged. 2) procedures for exposure of management services based on CAPIF, EGMF, MnS Registry, MSAC or a combination thereof. Some of the identified gaps for use of CAPIF in SA5 are listed in S5-236381 clause 4.1.2.*
* ***WT-1.3*** *Identify potential requirements that would be provided to the access control (MSAC) work item.*
* ***WT-1.4*** *Study whether and how SA5 defined exposure mechanisms fit within the GSMA Open Gateway framework. This framework includes OPG, CAMARA and TM Forum*

”.

In SA5#154, it was agreed to define the External MnS consumer as “An MnS consumer that has discovered an MnS via a discovery mechanism which is not defined in 3GPP SA5. CAPIF is an example of a framework providing such discovery mechanism”. This definition is in TR 28.879 [2], clause 3.1.

CAPIF is a framework with a lot of built-in capabilities. The figure below provides a non-exhaustive summary of the different procedures relevant in CAPIF. For further details on the stage 2 and 3 of these procedures, see [3]-[4].

A black screen with white text

Description automatically generated

This contribution proposes to use CAPIF as exposure framework.

Once the MnS producer has published the relevant information (i.e., information on which capabilities from supported MnS(s) the MnS producer wants to expose through CAPIF), the external MnS consumers are ready to get onboarded into CAPIF. However, before this, there is the enrolment phase. In this phase, represented in green in the figure above, the CAPIF administrator enrols the external MnS consumer into the admin portal.

Clause 8.3 in [2] notes the following for the enrolment phase: “**the API invoker has visibility to APIs information (e.g., API catalogue or dashboard – central place for the API provider to manage which APIs are displayed, giving API invoker the ability to enroll for**). A key question is raised here: how the API provider can manage which APIs are displayed? The API provider may define a discovery policy, and configure it accordingly in the system.

This discovery policy allows the API provider 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. The CAPIF administrator uses the discovery policy and other enrolment information to generate an onboarding credential (OAuth2.0 access) of the API invoker. This credential and other CCF details (address, root CA certificate) are sent to the API invoker, so that it can reach out to CCF to initiate the onboarding (e.g., the API invoker becomes a valid CAPIF user).
* Discover and subsequently access to, once the 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 discovery policy on the search results matching the query criteria, and filter them accordingly.

The present pCR aims to focus on the discovery policy configuration use case, which:

* leverages the procedure marked in green in the figure above.
* allows addressing WT-1.2 and WT-1.3 in [1].

# 4 Detailed proposal

It is proposed to make the following changes in the latest version of TR 28.879 [1].

|  |
| --- |
| **Begin Change** |

# 2 References

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

- References are either specific (identified by date of publication, edition number, version number, etc.) or non‑specific.

- For a specific reference, subsequent revisions do not apply.

- For a non-specific reference, the latest version applies. In the case of a reference to a 3GPP document (including a GSM document), a non-specific reference implicitly refers to the latest version of that document *in the same Release as the present document*.

[1] 3GPP TR 21.905: "Vocabulary for 3GPP Specifications".

[2] 3GPP TS 28.533: “Management and orchestration; Architecture Framework”.

[3] 3GPP TS 28.622: “Telecommunication management; Generic Network Resource Model (NRM) Integration Reference Point (IRP); Information Service (IS)”

[4] 3GPP TS 28.537: “Management and orchestration; Management capabilities”.

[5] 3GPP TS 23.222: "Functional architecture and information flows to support Common API Framework for 3GPP Northbound APIs; Stage 2"

[6] SP-231669: "LS on collaboration and alignment of 3GPP defined application enablers with GSMA Open Gateway".

[7] 3GPP [TS 23.434](https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3587): "Service Enabler Architecture Layer for Verticals (SEAL); Functional architecture and information flows".

[8] 3GPP [TS 23.255](https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3843): "Application layer support for Vehicle-to-Everything (V2X) services; Functional architecture and information flows".

[9] 3GPP [TS 23.286](https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3562): "Application layer support for Uncrewed Aerial Systems (UAS) services; Functional architecture and information flows".

[10] 3GPP [TS 23.545](https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3948): "Application layer support for Factories of the Future (FF) ".

[11] 3GPP [TS 23.542](https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=4156): "Application layer support for Personal IoT Networks".

[12] 3GPP [TS 23.554](https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3818): "Application architecture for MSGin5G Service; Stage 2".

[13] 3GPP [TS 29.222](https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3450): "Common API Framework for 3GPP Northbound APIs; stage 3".

[14] 3GPP [TS 33.122](https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3420): "Security aspects of Common API Framework (CAPIF) for 3GPP Northbound APIs".

[15] "The Ecosystem for Open Gateway NaaS API Development", white paper, June 2023 [[link](https://www.gsma.com/solutions-and-impact/gsma-open-gateway/wp-content/uploads/2023/05/The-Ecosystem-for-Open-Gateway-NaaS-API-development.pdf)]

[16] "GSMA Operator Platform Group – Requirements and Architecture", version 5.0, July 2023 [[link](https://www.gsma.com/futurenetworks/wp-content/uploads/2023/07/OPG.02-v5.0-Operator-Platform-Requirements-and-Architecture.pdf)]

[17] 3GPP TS 28.532: "Management and orchestration; Generic management services".

[18] 3GPP [TS 28.531](https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3274): "Management and orchestration; Provisioning"

[19] 3GPP [TS 23.435](https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=4092): "Procedures for Network Slice Capability Exposure for Application Layer Enablement Service"

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

[y] 3GPP TS 28.319: “Management and orchestration; Access control for management services”

|  |
| --- |
| **Second Change** |

# 3 Definitions of terms, symbols and abbreviations

## 3.1 Terms

For the purposes of the present document, the terms given in 3GPP TR 21.905 [1] and the following apply. A term defined in the present document takes precedence over the definition of the same term, if any, in 3GPP TR 21.905 [1].

**External MnS consumer**: An MnS consumer that has discovered an MnS via a discovery mechanism which is not defined in 3GPP SA5. CAPIF [5] is an example of a framework providing such discovery mechanism.

**MnS consumer:** defined in TS 28.533[2].

**MnS producer:** defined in TS 28.533[2].

## 3.2 Symbols

For the purposes of the present document, the following symbols apply:

<symbol> <Explanation>

## 3.3 Abbreviations

For the purposes of the present document, the abbreviations given in 3GPP TR 21.905 [1] and the following apply. An abbreviation defined in the present document takes precedence over the definition of the same abbreviation, if any, in 3GPP TR 21.905 [1].

5GC 5G Core

CAPIF Common API Framework

CCF CAPIF Core Function

CSP Communication Service Provider

EAS Edge Application Server

ECS Edge Configuration Server

EDN Edge Data Network

EEC Edge Enabler Client

EES Edge Enabler Server

FF Factories of the Future

GSMA GSM Association

MnS Management Service (see TS28.533[2])

NaaS Network as a Service

NEF Network Exposure Function

NOP Network Operator

NSACF Network Slice Access Control Function

NSCE Network Slice Capability Enablement

NWDAF Network Data Analytics Function

OAM Operation, Administration and Maintenance

OPAG Operator Platform API Group

OPG Operator Platform Group

SEAL Service Enabler Abstraction Layer

UAS Uncrewed Aerial Systems

V2X Vehicle-to-Everything

VAE Vertical App Enabler

WAS Whole Agreement Services

WG Working Group

AAA Authentication, Authorization and Accounting

|  |
| --- |
| **Third Change** |

## 5.1 Exposure of management services

### 5.1.y Use case Y: Configuring discovery policy for an external MnS consumer.

#### 5.1.y.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 policy on a per API invoker basis. This policy, defined during the API invoker enrolment phase, 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. The CAPIF administrator uses the discovery policy and other enrolment information to generate an onboarding credential (OAuth2.0 access) of the API invoker. This credential and other CCF details (address, root CA certificate) are sent to the API invoker, so that it can reach out to CCF to initiate the onboarding (e.g., the API invoker becomes a valid CAPIF user).
* 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 discovery policy on the search results matching the query criteria, and filter them accordingly.

It is worth noting that 3GPP specifications do not provide details nor guidelines for discovery policy definition; actually, the policy format (information elements and constraints) is entirely to the operator discretion.

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 [y] 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 policies for each external MnS consumer. The aim of these policies is to limit their visibility over the published MnS information, either at onboarding time (when the external MnS consumer becomes an onboarded API invoker) or at operation time (when the external MnS consumer issues discovery requests). The discovery policies can define filters at two levels:

* First, the policy 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 policy specifies whether the MOI is visible or not.
* Secondly, for each visible MOI, the policy allows limiting what the external MnS consumer can see regarding:
  + Attributes supported by the MOI.
  + 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 policy can be configured on the CCF, so that this policy can be bonded to the API invoker during the enrolment phase. This bonding allows setting the visibility that this API invoker will have over its lifetime, from onboarding to offboarding, including all stages in between. This configuration can be done through OAuth2.0 access token, by mapping discovery policy into token scope values.

#### 5.1.y.2 Potential requirements

**PREQ-FS\_MExpo-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-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-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-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-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 adaptations from those originally defined in 3GPP TS 28.319 [y], but not applicable for external MnS consumers.

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

#### 5.1.y.3 Potential solutions

##### 5.1.y.3.i Potential solution i: Using AccessRule class for discovery policy definition

###### 5.1.y.3.i.1 Introduction

class (TS 28.319 [y], clause 7.3.3)

|  |  |
| --- | --- |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |

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 Authenticaon, Authorization and Accounting (AAA) server.

This solution proposes using the existing AccessRule class to define discovery policies for external MnS consumer.

###### 5.1.y.3.i.2 Description



It is proposed to use AccessRule to generate discovery policies 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-01 and PREQ-FS\_MExpo-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-03 and PREQ-FS\_MExpo-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-05.
* “actions”: this attribute is not useful for the discovery policy configuration use case. 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. However, how they map to OAuth 2.0 Scope values is standardized.

##### 5.1.y.3.j Potential solution j: Using Role class for discovery policy definition

Role class (TS 28.319 [y], 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 discovery policies for external MnS consumer.

###### 5.1.y.3.i.2 Description

This solution is similar as in 5.1.y.3.j , with the exception that the policy conveys information from the access rules associated to this role.

##### 5.1.y.3.k Potential solution k: Mapping policy definition into OAuth2.0 access token.

###### 5.1.y.3.k.1 Introduction

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

###### 5.1.y.3.k.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 [x], and shown in the table below (see Table C.2.2-1 from 3GPP TS 33.122 [x]).

|  |  |
| --- | --- |
| 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 either by:

* CAPIF administrator, which also communicates with CCF to configure local/admin policies.
* Authorization MnS producer.

Once configured with the discovery policy, the CCF can use the policy with API invoker over CAPIF-1 interface. To enforce the policy, the CCF needs to contact with the entity hosting the accessRule and/or roles. An example of this entity can be the Authorization MnS producer.

5.1.y.4 Evaluation of potential solutionsSolutions “i” and “j” allow fulfilling the requirements PREQ-FS\_Mexpo-01, PREQ-FS\_Mexpo-02, PREQ-FS\_Mexpo-03, PREQ-FS\_Mexpo-04 and PREQ-FS\_Mexpo-05, providing controllable granularity on which published MnS information is discoverable by an external MnS consumer.

Solution “k” proposes using OAuth2.0 access token scope for configuring discovery policy into the CCF. Since scope has a limited space to capture information, using accessRules (solution “i”) can be problematic, due to the large information that accessRule class conveys; Role (solution “j”) might be more appropriate instead.

NOTE: How accessRules/Roles are to reach out the consumer is yet to be defined. Based on the agreement, we might need to send a LS to SA3 to update CAPIF token scope.

Editor's Note: This clause provides the evaluation of potential solutions.

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