**3GPP TSG-SA5 Meeting #143-eS5-223231**

**e-meeting, 09 -17 May 2022**

**Source: Ericsson, TEF**

**Title: Filtering, enrichment and converting of management information**

**Document for: Discussion**

**Agenda Item: 6.5.22.1**

# 1 Decision/action requested

**Discuss and agree the recommendation in section 4.4.**

# 2 References

[1] 3GPP TR [28.](https://www.3gpp.org/DynaReport/28532.htm)824: "Management and orchestration; Study on network slice management capability exposure"

# 3 Rationale

In the discussion on exposure of management capability a number of alternatives have been identified using CAPIF. This is documented in clause x in the TR 28.824, see reference [1]. Questions were raised regarding the use of translation in alternative 1. Translation effectively means the following, filtering, enrichment and/or conversion of an API.

The reason for doing the translation is to be able to provide an API that fulfils the following market requirement for it to be user friendly meaning that APIs shall hide telco complexity and make them easy to use to 3rd parties with no telco expertise/background. This may also mean that they need to be adapted for a specific type of 3rd party whose business expertise and jargon lies outside 3GPP (e.g. manufacturing and agriculture).

# 4 Detailed proposal

## 4.1 Architecture

The architecture in figure 4.1.1 is based on the solution for exposure via CAPIF alternative 1 described in clause 7.9.1 of TR 28.824, see reference [1]. The translation which was discussed during #142e meeting has been added to the architecture and is shown in figure 4.1.1 as “Filtering, enrichment, conversion”. An example can be found in the CAMARA project where they translate the standard APIs to a customized version. Filtering is removing of information elements (attributes and classes), enrichment is adding information from other MnS or other sources outside OAM, converting is changing information elements through for example combing information elements or mapping information elements.

**Figure 4.1.1 Location of translation using the CAPIF framework for exposing management APIs**.

**MnS Consumers**

**MnS Producers**

API Invoker

CAPIF-1e

CAPIF-1

CAPIF-2e

CAPIF-2

CAPIF-3

CAPIF-4

CAPIF-5

Provisioning

Performance Management

Streaming

File Data Reporting

Heartbeat

Fault

 Management

API Invoker

CAPIF core function

API Exposing Function

API Publishing Function

API Management Function

PLMN trust domain

Filtering, enrichment, conversion

## 4.2 Procedure

### 4.2.1 description of procedure



Figure 4.2.1.1 Procedure for consumption of exposed MnS after service order is completed

NOTE: For simplicity reasons the CAPIF Core Function and API Provider defined in TS 23.222 are combined into Exposure governance and any communication between them is also not included.

1) The CAPIF\_Core receives an authenticating and authorization request from the NSC\_Application based on the identity and other information required for authentication and authorization of the NSC\_Application.

2) The CAPIF\_Core processes the authentication and authorization request.

3) The CAPIF\_Core provides the appropriate response to the NSC\_Application.

4) The CAPIF\_Core receives a request for the discovery of service APIs information.

5) The CAPIF\_Core processes the discovery.request.

6) The CAPIF\_Core provides the appropriate response to the NSC\_Application.

7) The API\_Provider receives an authorization request from the NSC\_Application based on the identity and other information required for authorization of the NSC\_Application.

8) The API\_Provider processes the authorization request.

9) The API\_Provider provides the appropriate response to the NSC\_Application

10) The API\_Provider receives a request for the invocation of the service API(s) from the NSC\_Application.

11) The API\_Provider processes (and optionally may filter, enrich and/or convert) the invocation request.

12) The OSS receives request from API\_Provider for MnS.

13) The OSS provides the appropriate response to the API\_Provider.

14) The API\_Provider processes (and optionally may filter, enrich and/or convert) the response from the OSS

15) The API\_Provider provides the appropriate response to the NSC\_Application.

### 4.2.2 Detailed description of step 10-15

Once the NSC\_Application has been authenticated and authorizated the NSC\_Application can start to send API\_Invocation requests (step 10). Each request is processed by the API\_Provider where the API\_Provider may optionally translate into several MnS requests (step 11). Translation means filtering, enrichment and/or conversion of the request to MnS request(s) (step 12). As part of the processing of the request the API\_Provider may also invoke other services e.g. charging.

When all MnS reponses have been received (step 13 and step 14) the API\_Provider may optionally translate this into a single API\_Invocation reponse (step 15).

## 4.3 Observations

The procedure described in 4.2 would allow for handling of the exposed APIs to be completely separated from the MnS(s) and be more adaptable to the NSC Application needs

The procedure described in 4.2 would also allow for invocation of other services than MnS(s) that may be required to fulfil the need of the NSC Application.

NOTE: The procedure is only applicable to alternative 1 described in TR 28.824 [1]

NOTE: Filtering, enrichment and converting in this alternative is out of scope of SA5

## 4.4 Recommendations

The architecture described in 4.1 and the procedure described in 4.2 should be a recommended solution for exposure of management services in SA5 specifications.

NOTE: The recommendation is only applicable to alternative 1 described in TR 28.824 [1]

## Annex A UML code: Procedure for consumption of exposed MnS after service order is completed

@startuml

skinparam sequence {

ArrowColor Black

ActorBorderColor Black

ActorBackgroundColor White

ParticipantBorderColor Black

ParticipantBackgroundColor White

LifeLineBorderColor Black

}

skinparam NoteBackgroundColor White

skinparam NoteBorderColor White

skinparam NoteColor White

skinparam shadowing false

hide footbox

autonumber

participant NSC\_Application

box "Exposure governance" #white

 participant CAPIF\_Core

 participant API\_Provider

end box

participant OSS

NSC\_Application --> CAPIF\_Core : Authentication and authorization request

CAPIF\_Core -> CAPIF\_Core: process request

NSC\_Application <-- CAPIF\_Core : Authentication and authorization response

NSC\_Application --> CAPIF\_Core : Discovery request

CAPIF\_Core -> CAPIF\_Core: process request

NSC\_Application <-- CAPIF\_Core : Discovery response

NSC\_Application --> API\_Provider : Authentication and authorization request

API\_Provider -> API\_Provider: process request

NSC\_Application <-- API\_Provider : Authentication and authorization response

group may be repeated

NSC\_Application --> API\_Provider : API Invocation request

API\_Provider -> API\_Provider: process request\n(may include translation)

group may be repeated

API\_Provider --> OSS: MnS request

API\_Provider <-- OSS: MnS response

end

API\_Provider -> API\_Provider: process response\n(may include translation)

NSC\_Application <-- API\_Provider : API Invocation response

end

@enduml