**3GPP TSG-SA5 Meeting #144-e *S5-224287***

e-meeting, 27 June - 1 July 2022

**Source: Ericsson, Deutsche Telekom**

**Title: Potential solution for management capability exposure alternative 1**

**Document for: Approval**

**Agenda Item: 6.9.6.3**

# 1 Decision/action requested

The group is asked to approve the proposal

# 2 References

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

[2] [S5-223744](https://www.3gpp.org/ftp/tsg_sa/WG5_TM/TSGS5_143e/Docs/S5-223744.zip) Discussion paper on filtering, enrichment and converting of management information.docx

# 3 Rationale

The study report, see reference [1] identifies 3 scenarios for management capability exposure using the CAPIF framework. The 3 alternatives are documented in clause 7.9 as alternative 1, 2 and 3.

Potential solutions have been identified for alternative 2 and alternative 3, these are documented in clause 7.10. The potential solution for alternative 1 is missing. This contribution proposes to add potential solution for alternative 1. The solution is based on the procedure which was discussed at the #143e meeting and can be found in reference [2].

# 4 Detailed proposal

**First change**

## 7.x Potential solution for management capability exposure alternative 1

This solution supports exposure via CAPIF alternative 1 as defined in 7.9.1.

The procedure described in Figure 7.x.1 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 7.x.1 would also allow for invocation of other services than MnS(s) that may be required to fulfil the need of an NSC Application.

NOTE: Filtering, enrichment and converting represents an optional translation of MnS APIs into service APIs, for the case where 3rd party consumption requires them. The decision on whether this translation is needed, and how to apply it (translation internals) is out of scope of SA5

 

Figure 7.x.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.

Once the NSC\_Application has been authenticated and authorized 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).

**Second change**

## A.X UML code for Figure 7.x.1

@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

.

**End of changes**