**3GPP TSG-SA5 Meeting #140-eS5-216181**

**e-meeting, 15 - 24 November 2021**

**Source: Huawei**

**Title: Concept definition for Exposed Management Service**

**Document for: Approval**

**Agenda Item: 6.5.4**

# 1 Decision/action requested

***For approval***

# 2 References

[1] 3GPP TR 28.824 V0.3.0 Management and orchestration; Study on network slice management capability exposure

# 3 Rationale

TR 28.824 [1] does not include a clear definition of the concept of Exposed Management Service, in particular how an Exposed Management Service differs from a traditional 3GPP Management Service.

# 4 Detailed proposal

This contribution proposes to make the following changes in [1].

|  |
| --- |
| **1st change** |

#### 4.1.1.1 Exposed Management Services

If a network slice provider wishes to expose network slice management services to customers, the network slice provider may expose an API. The network slice provider may choose to expose an API which is compliant to 3GPP Technical Specifications. In the particular case that the network slice provider exposes an API which complies with the specification for a 3GPP Management Service, this API is known as an exposed Management Service (eMnS).

Exposed MnS (eMnS) represents the MnS that can be exposed by MnS producer to the external MnS consumer. eMnS may rely on a dedicated MnF (e.g. EGMF defined in 3GPP or function defined in other standard like TMF) that manages the exposure aspects.

Editor’s notes: Whether eMnS is exposed transparently to external MnS consumer via BSS or being processed through a dedicated exposure platform is FFS.

#### 4.1.1.2 Exposure of Management Services

Exposure of management services supports the case that an external MnS consumer which is outside 3GPP management system can indrectly access management capability offered by MnS producer within 3GPP management system. Even though the eMnS complies with the same Technical Specification as a MnS, the actual operational behavior and managed data may be constrained by the network slice provider.

|  |
| --- |
| **2nd change** |

## 5.1 Network slice management capability exposure

### 5.1.1 Description

A use case of network slice management capability exposure can be described as follows:

1. NSP selects the MnS that can be exposed externally.

2. NSP decides on any constraints that shall be applied to the MnS when it is exposed externally. For example, NSP may decide to disallow certain operations, limit the Managed Object Instances that may be managed, or aggregate/anonymize sensitive data.

3. NSP implements and deploys a Management Function which consumes the MnS, applies any constraints, and exposes the resulting functionality as an eMnS.

4. NSP may publish the eMnS in a service catalog or service directory.

### 5.1.2 Issue and gaps

Gap:

Whether and how to publish eMnS which can be exposed to BSS to a suitable eMnS producer for network management capability exposure is not specified in existing 3GPP management system.

## 5.x Network slice management capability consumption

### 5.x.1 Description

A use case of network slice management capability consumption can be described as follows:

1. In order to enable the consumption of network slice related eMnS, a NSC firstly makes a contract with the NSP, which contains the agreement on what eMnS optionally under what condition can be consumed. The condition can be certain constraint of eMnS consumption based on the contract, e.g. the access quota of certain eMnS, the access frequency of certain eMnS, etc. The NSC negotiates its specific requirements for the network slice management capability consumption with the NSP. The negotiation can be done via the following ways:

a) For NSC which is small enterprise, it can directly have a view on the network slice related management capability through the BSS (e.g. by using Service Catalog). Based on that, the NSC can select the network slice related eMnSs which will be covered by the contract.

b) For NSC which is large enterprise (i.e. Internet giants that have their own service customer), it can select the network slice related eMnSs that are available to be exposed offline (e.g. through a F2F meeting). The NSP can proceed with the service ordering through BSS based on the contract.

2. The BSS may interact with the OSS in order to complete certain configuration (i.e. permission regarding what eMnS, optionally under what condition, can be consumed) regarding the consumption of eMnS based on the customized requirement from the NSC.

3. NSP authorizes NSC to consume the eMnS as defined in the contract, and provides the relevant authentication keys to NSC.

4. The NSC can get access to the network slice related management capability offered by eMnS producer within 3GPP management system. The access may need the interaction with BSS (e.g. through Service Catalog).

### 5.x.2 Issue and gaps

Gap:

NSC needs to apply for the access of network slice management capability through BSS. However, there is no discussion and agreement on whether an eMnS is exposed transparently through the BSS or being processed through a dedicated exposure platform before exposing to the NSC.

The definition and the format of permission for the consumption of network slice related eMnS and its potential impact on internal interface with BSS is not discussed in current SA5 work.

|  |
| --- |
| **End of changes** |