**3GPP TSG-SA5 Meeting #143-e *S5-223238rev1***

e-meeting, 9 - 17 May 2022

**Source: Huawei, Deutsche Telekom**

**Title: Update use case Exposure of network slice as a service**

**Document for: Approval**

**Agenda Item: 6.5.22.1**

# 1 Decision/action requested

***For approval***

# 2 References

[1] 3GPP TR 28.824 V0.6.0 Study on network slice management capability exposure

# 3 Rationale

The original sub use case in clause 5.6.1.1 doesn’t cover the scenario that directly exposing the network management capabilities from OSS/NML. Therefore, it is proposed to add a sub use case describing the exposure of network slice subnet as a service in clause 5.6. The new sub use case describes the scenario that the NSC can directly send eMnS consumption requests to NOP OSS/NML based on the service orders sent from NSC to NSP. In addition, it is proposed to remove the box with placeholder ‘EGMF’ in the Figure 5.6.1.1-1 and 5.6.1.1-2 as it is supposed to be shown in the corresponding solutions for use case 5.6.

The new changes are marked as "Huawei 3" based on S5-222276rev1 made in SA5#142e.

# 4 Detailed proposal

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

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

## 5.6 Exposure of network slice as a service

### 5.6.1 Description

This use case involves the following roles:

- NSP: Network Slice Provider

- NSC: Network Slice Customer

- NOP: Network Operator

- CSC: Communication Service Customer

- CSP: Communication Service Provider

, and the following systems:

- BSS: Business Support System

- OSS: Operations Support System, made up of the two following sub-systems:

- SML: Service Management Layer

- NML: Network Management Layer (for sake of simplicity, network management and network element / function management are both in the NML).

#### 5.6.1.1 Sub-use case 1: NSP and NOP play by the same organization

In this scenario, the following organizations play aforementioned roles as follows:

- Company-V, which has a contract with Company-A for the exposure directly via OSS, plays the role of NSC

- Company-A plays the role of NSP and NOP

- As NSP, it has:

- a BSS, e.g. to manage its customers, products, contracts, and

- a SML, to manage the services that support its products,

- As NOP, it has:

- its own 5G network (RAN + core). In this sub-use case, Company-A owns the whole set of network resources used by the service that can potentially support the service required by Company-V

- a NML, to manage the network resources used by services

NOTE: NSC may have connection with Company-A BSS for the product-level interaction. If not, the OSS/SML may have an embedded BSS functionalities for the product-level interaction.

##### 5.6.1.1.1 Exposure via OSS/SML



Figure 5.6.1.1.1 Sub-use case – NSP and NOP played by the same organization-exposure via OSS/SML

Company-A proposes the following product offering together with the exposure capability:

- Network Slice eMBB with the exposure capability of related KPI monitoring and alarm notification, etc. The monitored KPI are produced on OSS/SML based on the combination with other performance metrics that produced on OSS/NML.

In this sub-use case 1:

1. Company-V (as the NSC) gets the information regarding eMnSs that are available via the eMnS discovery service from the Company-A.

2. Company-V sends a request to Company-A (as the NSP) for the access to exposed MnS set ‘Network Slice eMBB’, which contains the exposure capabilities such as related KPI monitoring and alarm notification, etc. To achieve this, a candidate API is the interface with the MnF that controls the exposure governance (e.g. EGMF).

2.1 Company-A SML determines which service supports the exposed MnS being requested by Company-V.

2.2 Company-A OSS / SML sents a response, including the authentication materials (e.g. key, token) for access to the chosen exposed MnS.

3. The company-V can direct consume the exposed MnS (e.g. KPI monitoring and alarm notification) from SML of the Company-A’s 3GPP management system.

##### 5.6.1.1.2 Exposure via OSS/NML



Figure 5.6.1.1.2 Sub-use case – NSP and NOP played by the same organization-exposure via OSS/NML

Company-A proposes the following product offering together with the exposure capability:

- Network Slice eMBB with the exposure capability of RAN/ CN domain KPI monitoring and related alarm notification, etc. The monitored RAN/ CN domain KPI are produced on OSS/NML and there is no need to combine them through OSS/SML. In this case, the OSS/SML works for the connection between the products that ordered through NSP BSS and the network management services provided by NOP OSS/NML.

In this sub-use case 1:

1. Company-V (as the NSC) gets the information regarding eMnSs that are available via the eMnS discovery service from the Company-A.

2. Company-V sends a request to Company-A (as the NSP) for the access to exposed MnS set ‘Network Slice eMBB’, which contains the exposure capabilities such as related KPI monitoring and alarm notification, etc. To achieve this, a candidate API is the interface with the MnF that controls the exposure governance (e.g. EGMF).

2.1 Company-A SML determines which service supports the exposed MnS being requested by Company-V. Company-A SML notices that the exposed MnS being requested by Company-V can be solely produced by MnS producer implemented on OSS/NML without the need of combination with other MnS. 2.2 Company-A OSS/SML sends the request for accessing to the service that determined in step 2.1 to company-A OSS/NML.

2.3 Company-A OSS / NML sends a response to OSS/SML, including the authentication materials (e.g. key, token) for access to the chosen exposed MnS.

2.4 Company-A OSS/SML sends a response to Company-V, including the authentication materials (e.g. key, token) that received from OSS/NML.

3. The company-V can direct consume the exposed MnS (e.g. RAN/CN KPI monitoring and related alarm notification) from NML of the Company-A’s 3GPP management system.

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