**3GPP TSG-SA5 Meeting #141-eS5-221714d3**

**e-meeting, 17 - 26 January 2022**

**Source: Alibaba**

**Title: Key issue and solution on exposure without going through BSS**

**Document for: Approval**

**Agenda Item: 6.5.2**

# 1 Decision/action requested

***The group is asked to agree the text in detailed proposal.***

# 2 References

Not applicable

# 3 Rationale

This contribution proposes key issue and solution on exposure without going through BSS.

# 4 Detailed proposal

|  |
| --- |
| **First 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] TM Forum TMF622 Product Order API REST Specification

[3] TM Forum TMF641 Service Ordering API

[4] TM Forum TMF652 Resource Order Management API

[5] 3GPP TS 28.531: "Management and orchestration; Concepts, use cases and requirements"

[6] 3GPP TS 28.202: "Charging management; Network slice management charging in the 5G System (5GS); Stage 2"

[7] 3GPP TR23.700-99 “Study on Network Slice Capability Exposure for Application Layer Enablement (NSCALE)”

[8] 3GPP TS23.434 “Service Enabler Architecture Layer for Verticals (SEAL); Functional architecture and information flows.”

[9] 3GPP TS 28.541: "Management and orchestration; 5G Network Resource Model (NRM); Stage 2 and stage 3"

[10] 3GPP TS 28.533: "Management and orchestration; Architecture framework"

|  |
| --- |
| **second change** |

## 5.11 Key Issue #11: Network slice management capability exposure without going through BSS

### 5.11.1 Description

Use cases regarding exposure without going through BSS has been introduced in Section 6. NSC can make contract with the NSP or CSP regarding exposure via BSS. Upon the completion of the contact, the NSC can directly get access to the OSS within the NSP or CSP for access the exposed MnS. Several key issues exist for the use cases. For example, how does the NSC identifies the address of MnS producer within the OSS for the exposed MnS and how to consume the exposed MnS directly from OSS needs to be addressed. In addition, how does the NSC obtains the copy of a part of the Network Operator’s MIB also needs to be addressed.

### 5.11.2 Potential solutions

#### 5.11.2.1 Potential solution #1: Exposed MnS consumption without going through BSS

This clause introduces the solution for the use case where only NSP is involved and the use case where the NSP has BSS and need to leverage the CSP OSS to provide exposed MnS for the NSC.

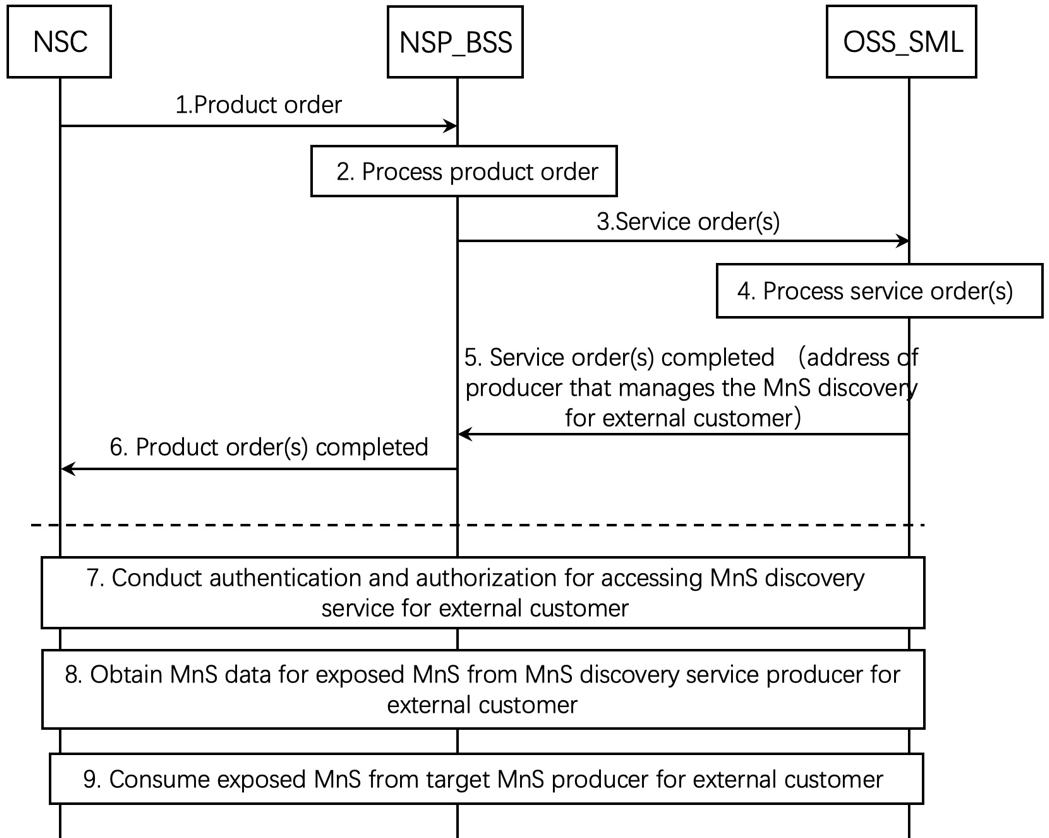


Figure 5.11.2.1-1 Exposed MnS consumption without going through BSS

1. The NSP receives a product order from the NSC through BSS. The interface used towards the BSS is specified by TM Forum specifications [2].

2. The BSS processes the product order and when applicable converts it to appropriate service order(s) for the OSS Service Management Layer. This is internal to BSS and there are no interface requirements.

3. The OSS Service Management Layer receives a service order from the BSS. The interface used is specified by TM Forum specifications [3].

4. The MnS producer for NSC (e.g. NSMF) on the OSS Service Management Layer processes the service order and when applicable converts it to appropriate request(s) for the OSS Network Management Layer as requests for management and orchestration of resources. In addition, MnS producer on the OSS Service Management Layer can decides to expose MnS directly from OSS\_SML and prepares the address of MnS discovery service producer for NSC that can be accessed by the NSC and related authorization information (e.g. token) for accessing the MnS discovery service for NSC. The service order may trigger a procedure of resource order with OSS\_NML.

5. The MnS producer for NSC on OSS Service Management Layer notifies the BSS that the service order has been completed. In addition, the notification may contain the address of producer that manages the MnS discovery service for NSC to access and also a copy of a part of Network Operator’s MIB which is related to the exposed MnSs that the NSC requests. The interface used is specified by TM Forum specifications [3].

Network

NOTE 2: The Network Operator’s exchange information required to use each other service can be captured in product and service orders to the right abstraction level and naming of entities.

NOTE 3: The MnS discovery service producer for NSC can be within the OSS or outside the OSS.

6. The BSS notifies the NSC that the product order has been completed. In addition, the address of MnS discovery producer for NSC and the related authorization information (e.g. token) for accessing the MnS discovery service for NSC are sent to the NSC by the product order completed message. The interface used the interface towards the BSS is specified by TM Forum specifications [2].

7. If the notification in step 6 contains the address of MnS discovery service producer for NSC, the NSC conducts authentication and authorization for accessing exposed MnS discovery service.

8. After the authentication and authorization, the NSC obtains the MnS data for exposed MnS, which contains the information of the exposed MnS instance and the address of target MnS producer for NSC.

9. After obtaining the information of the MnS data for exposed MnS, the NSC identifies the target MnS producer for NSC and consumes the exposed MnS. To consider the security, the MnS producer may leverage a dedicated MnF which controls the exposure governance as a proxy for exposing MnS.

### 5.11.3 Conclusion

The following issues are identified in the clause 5.11:

- The management capability exposure governance specified in TS 28.533 [10] should be updated to describe how the NSC consume the MnS based on **REQ-NSCE-03**.

|  |
| --- |
| **Third change** |

# 6 Potential requirements for network management capability exposure

## 6.2 Potential requirements related to exposure without going through BSS

* **REQ-NSCE-03** The 3GPP management system may provide capabilities to authenticate and authorize NSC to consume exposed MnS directly from 3GPP management system.

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