**3GPP TSG-SA5 Meeting #148e *S5-233356***

Electronic meeting, Online, 17 -25 April 2023

**Source: Huawei**

**Title: Correction of terminologies**

**Document for: Approval**

**Agenda Item: 6.9.5.5**

# 1 Decision/action requested

***The group is asked to discuss and approval.***

# 2 References

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

# 3 Rationale

This document is to correct the terminologies, unclear expression and wrong reference number. The correction is based on version 0.1.1 of TR 28.824 which has not been uploaded to 3GPP archive yet.

# 4 Detailed proposal

It is proposed to make the following changes to TR 28.824 [1].

|  |
| --- |
| **1st Change** |

#### 4.1.4.2 Procedure invoking internal service order after receiving product order from NSC

The procedure for invoking a service order internal to the NSP after receiving a product order from an NSC is shown in Figure 4.1.4.2.1. The interface through which the NSC can order a product from the NSP is on BSS level. The steps as shown in Figure 4.1.4.2.1 are described in the subsequent paragraphs.



Figure 4.1.4.2.1 Procedure invoking internal service order after receiving product order from NSC

1) The NSP receives a product order from the NSC through the interface to BSS. The interface between the NSC and BSS of the NSP is used.

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 between the BSS of the NSP and the OSS\_SML of the NSP is used.

4) 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. This is internal to the OSS Service Management Layer and there are no interface requirements.

5) The OSS Network Management Layer receives a request from the OSS Service Management Layer. An interface between the OSS Service Management Layer and OSS Network Management Layer may be used.

6) The OSS Network Management Layer processes the request and when applicable converts it to appropriate request(s) for the network. An interface between the OSS Network Management Layer and Network Layer (not shown) may be used.

7) The OSS Network Management Layer notifies the OSS Service Management Layer that the resource order(s) have been completed. An interface between the OSS Service Management Layer and the Network Layer may be used.

8) The OSS Service Management Layer notifies the BSS that the service order has been completed. The interface between the OSS Service Management Layer and the BSS is used.

9) The BSS notifies the NSC that the product order has been completed. The NSC may start using the services included in the product order. The interface between the NSC and the BSS is used.

#### 4.1.4.3 Procedure invoking external product order after receiving product order from NSC

The procedure for invoking a product order external to the NSP after receiving a product order from an NSC is shown in Figure 4.1.4.3.1. The interface through which the NSC can order a product from the NSP is on BSS level. The steps as shown in Figure 4.1.4.3.1 are described in the subsequent paragraphs.



Figure 4.1.4.3.1 Procedure invoking external product order after receiving product order from NSC

1) The NSP receives a product order from the NSC through the interface to BSS. The interface between the NSC and BSS of the NSP is used.

2) The NSP BSS processes the product order and when applicable converts it to appropriate product order(s) towards a 3rd party CSP BSS. This is internal to BSS and there are no interface requirements.

NOTE: When the BSS\_NSP receives a product order, the BSS\_NSP splits the product order into service orders. A service order that can be fulfilled by the NSP will be processed by the NSP\_OSS\_SML (see also Figure 4.1.4.2.1) while a service order that cannot be fulfilled by NSP will be ordered from the CSP through a product order.

3) The CSP BSS receives a product order from the NSP BSS. The interface between the BSS of the CSP and the BSS of the NSP is used.

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

5) The CSP OSS receives a service order from the CSP BSS. The interface between the BSS and the OSS both belonging to the CSP is used.

6) The CSP OSS processes the service order until the service order is completed.

7) The CSP OSS notifies the CSP BSS that the service order has been completed. The interface between the OSS and the BSS both belonging to the CSP is used.

8) The CSP BSS notifies the NSP BSS that the product order has been completed. The interface between the BSS of the CSP and the BSS of the NSP is used.

9) The BSS notifies the NSC that the product order has been completed. The NSC may start using the services included in the product order.

#### 4.1.4.4 Procedure invoking external service order after receiving product order from NSC

The procedure for invoking a service order external to the NSP after receiving a product order from an NSC is shown in Figure 4.1.4.4.1. The interface through which the NSC can order a product from the NSP is on BSS level. The steps as shown in Figure 4.1.4.4.1 are described in the subsequent paragraphs.



Figure 4.1.4.4.1 Procedure invoking external service order after receiving product order from NSC

1) The NSP receives a product order from the NSC through the interface to BSS. The interface between the NSC and BSS of the NSP is used.

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

3) The NSP OSS receives a service order from the NSP BSS. The interface between the OSS and the BSS, both belonging to the same NSP, is used.

4) The OSS processes the service order and when applicable converts it to appropriate service order(s) for a 3rd party CSP OSS. This is internal to the OSS producer and there are no interface requirements.

5) The CSP OSS receives a service order from the NSP OSS producer. The interface between the OSS of the CSP and the OSS of the NSP is used.

6) The CSP OSS processes the service order until the service order is completed. This is internal to the OSS producer and there are no interface requirements.

7) The CSP OSS notifies the CSP BSS that the service order has been completed. The interface between the OSS and the BSS, both belonging to the same CSP, is used.

8) The CSP OSS notifies the NSP OSS producer (may occur at the same time as or before step 7) that the service order has been completed. The interface between the OSS of the CSP and the OSS of the NSP is used.

9) The NSP BSS notifies the NSC that the product order has been completed. The NSC may start using the services included in the product order.

4.1.4.5 Procedure for product onboarding



**Figure 4.1.4.5.1 Procedure related to product onboarding**

1. OSS\_SML obtains 3GPP management services in the network through management service discovery;
2. OSS\_SML governs the rules and policies of MnS and configures the available MnS (e.g. exposed MnS) to BSS\_NSP. For example, if the RAN NE is dedicated to external customers, the performance monitoring service of a RAN NE should be exposed. Otherwise, it should not be exposed;
3. Optionally, the BSS\_NSP may send information to request the list of available services from OSS\_SML;
4. OSS\_SML provides the list of available services to BSS\_NSP;
5. BSS\_NSP configures (groups or package the services into a product) the services from OSS\_SML such that they can be exposed to NSC;
6. NSC should request the product catalogue from BSS\_NSP.
7. BSS\_NSP provides product catalogue to NSC.

 Editor’s Note: “EGMF can have the functionality of exposed MnS data. Whether registration to an external discovery system is FFS.”

4.1.4.6 Procedure for consumption of exposed MnS after service order is completed

The procedure for consumption of an exposed MnS after the product and service orders are completed is shown in figure 4.1.4.6.1. The MnS is produced by the MnS producer located in the OSS of the NSP.

An MnS may already be produced before CAPIF 1 service is requested. The CAPIF 2/2e service is a filtered, enriched and/or converted version of the MnS. The transformation, filtering, enrichment, or conversion of MnS APIs into service APIs is optional. The details of how this transformation, filtering and/or enrichment are to be done are out of scope of SA5.

Editor’s Note: There exist initiatives such as CAMARA [21] which are working in this translation.

Filtering is removing of information elements (attributes and classes), enrichment is adding information elements from other MnSs or other sources outside OAM, and converting is changing information elements through for example combining or mapping information elements. The CAPIF 2/2e service is provided by the API\_Provider\_domain\_function and consumed by the NSC\_Application. The API\_Provider\_domain\_function uses the MnS(s) produced to provide the CAPIF 2/2e service.



**Figure 4.1.4.6.1 Procedure for consumption of exposed MnS after service order is completed**

NOTE1: For simplicity reasons the CAPIF Core function and API Provider domain function defined in TS 23.222 [14] are combined and any communication between them is also not included.

NOTE2: The procedure is only applicable to “Exposure via CAPIF alternative 1” described in clause 7.9.1.

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

3) The CAPIF\_Core\_function provides the response with the result of the authentication and authorization to the NSC\_Application.

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

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

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

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

8) The API\_Provider\_domain\_function processes the authorization request.

9) The API\_Provider\_domain\_function provides the response with the result of the authentication and authorization to the NSC\_Application.

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

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

12) The MnS\_Producers receive requests from the API\_Provider\_domain\_function for MnS.

13) The MnS\_Producers provide the appropriate responses to the API\_Provider\_domain\_function.

14) The API\_Provider\_domain\_function processes (and optionally may filter, enrich and/or convert) the response from the MnS\_Producers.

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

NOTE: Each response in the steps does not always need to trigger the next request.

|  |
| --- |
| **2nd Change** |

4.2.3 Issue #3: EGMF/MCEG

The Exposure Governance Management Function (EGMF) was originally defined in TS 28.533 [11] as an MnF providing management capability exposure governance (MCEG). However, the current definition needs more elaboration on the following questions:

* The functional scope of management capability exposure governance, and its relationship with the access control and with existing API GW solutions in carrier networks.
* The impact of management capability exposure governance on the Network Slice NRM fragment. Is it within the scope of SA5 or not? If in-scope, then:
	+ what NSC related information (e.g., NSC id, NSC granted capabilities) does the NSP send to the NOP?
	+ how does the NOP manage this information in relation to the existing NetworkSlice and NetworkSliceSubnet IOCs?
* The need to standardize EGMF. Does SA5 really need to define this MnF? Doesn’t this approach mean moving away from producer centric model of SA5, i.e., focus on service producers rather than MnFs?
* If EGMF standardization is within the scope of SA5, then does SA5 need to provide details on EGMF internals? Does SA5 need to decide whether the EGMF is positioned on the Network Management Layer (NML), or the Service Management Layer (SML), or BSS layer?

|  |
| --- |
| **End of change** |