**3GPP TSG-SA5 Meeting #140-e *S5-216623***

 ***revision of* *S5-216403rev3***

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

**Source: Lenovo, Motorola Mobility**

**Title:**  pCR 28.824 Exposure to SA6 applications or mIddleware

**Document for: Approval,**

**Agenda Item: 6.5.4**

# 1 Decision/action requested

***Please approve***

# 2 References

# 3 Rationale

*Besides external consumers there may be other internal consumer that access management services. A scenario to highlight this is provided using SA6 middleware or applications as a consume of management services.*

# 4 Detailed proposal

Start of changes

# 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.”

Second change

##### 4.1.1.3.2 Exposure scenarios

Scenario 1: The NOP may interface to an external CSP that are doing the service management and have a machine to machine interface between the CSP’s "service manager" and the NOP’s "network manager" via BSS.



Figure 4.1.1.3.2-1 Service to network interface beeing an external interface

Scenario 2: The CSP might have a machine to machine interface towards their customers (e.g. a vertical) via their BSS. The CSP needs to have an interface towards NOP from their “service manager”. The NOP may have a machine to machine interface between the "service manager" and the "network manager" via BSS.



Figure 4.1.1.3.2-2 External customer interface to CSP

Scenario 3: The operator may have interface to other companies that are buying services and have machine to machine interface to the operators’s "service manager" via BSS.



Figure 4.1.1.3.2-3 BSS to customer interface being an external interface

Considering scenario 1, 2, and 3 the needs of an external customer always has to be reflected on the internal interface between NOP Network manager and CSP Service manager no matter how many companies are in the chain between the NOP and the External customer, Actions from a Vertical must be possible on the interface between NOP Network manager and CSP Service manager.

Scenario 4: Consumption of exposed MnS by applications

Editor’s note: This scenario doesn’t fit in the level of details of this section. Where to incorporate this section is FFS.

The operator has other non-management entities such as the middleware or application servers (AS) defined by 3GPP SA6 that could consume management services as shown in Figure X. In such a case the BSS may or may not be directly involved. An example of an external application could be a V2X application server may use the management system to provision V2X slices in a certain geography (AS2 or AS3 in Figure). An example for an internal application could be the operators eMBB application server discovering a newly supported coverage area and provisioning the operator eMBB network slice instance in that area (AS1 in Figure). AS1 and AS2 access the 3GPP management system from an operator internal enabler server (see TR23.700-99), another enabler server could be located in the vertical premises and therefore external to the operator. In TR23.700-99 both such options are considered. In this scenario the operator MnSs are directly access by internal or external entities (subject to prior agreements) without going through the BSS. In addition to application servers and application enabler server, any internal of external authorized application funcaion may also access exposed MnS.

In Figure X AS1 and AS2 may or may not be aware that they use exposed MnSs from the operator. The respective enabler serviers could hide this internal implementation. Bother enabler servers may access exposed MnS subject to respective authorization. However, it is likely that the application enabler server A and AF1 have direct access to management services without a BSS, whereas the application enabler server B and AF2 would need some sort of involvement of the BSS.



Figure X Exposure to application server within and outside operator network

End of changes