**3GPP TSG-SA5 Meeting #142-e *S5-223266rev2***

**e-meeting, 4 - 12 April 2022**

**Source: China Southern Power Grid, Huawei**

**Title: pCR 28.824 Add scenario of management exposure**

**Document for: Approval**

**Agenda Item: 6.5.22.1**

# 1 Decision/action requested

***For approval***

# 2 References

[1] 3GPP TR 28.824 V0.5.0 Study on network slice management capability exposure

# 3 Rationale

This contribution is to add the scenario of management exposure.

# 4 Detailed proposal

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

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

##### 4.1.1.3.2 Exposure scenarios

Scenario 1: 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 4.1.1.3.2-1. 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 consumed 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 function may also access exposed MnS.

In Figure 4.1.1.3.2-1 AS1 and AS2 may or may not be aware that they use exposed MnSs from the operator. The respective enabler servers 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 4.1.1.3.2-1 Exposure to application server within and outside operator network

Scenario 2: Consumption of exposed MnS by vertical management system

In this scenario, network operator is capable to provide a dedicated MnS for vertical management system (e.g., power grid supporting system), to consume the management services provided to vertical MnS consumer. The the access to the MnS can be provided by network operator to external MnS consumer, or vertical end user owned management system which behaves as an external MnS consumer.

For example, the access to the MnS provided to this vertical end user can be the access to management entity in charging of management to a SNPN. So, the dedicated MnS is only to provide the management capabilities to vertical end user. Another example is that the network operator may provide dedicated management capabilities for a non-shared slice to a power grid company.

The connection and consumption of management service provided by management system, is very likely required to be after authortication and authorization provided by the network operator. The process of authortication and authorization functionality can be part of BSS in this scenario.

In addition, the network operator may provide a dedicated management service to this external MnS consumer, which may resident in a management function.

The use of dedicated management services provided to external MnS consumer for vertical can be,

* The connection monitoring, e.g., QoS monitoring, network status.
* The alarm notification of the network slice and network slice subnet
* Other modification operation related to application in vertical IT system.

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