**3GPP TSG-SA5 Meeting #144-e *S5-224043***

**Online, , 27th June 2022 – 1st July 2022**

**Source: Samsung, Ericsson**

**Title: pCR 28.824 Updating use case for Network slice management capability exposure**

**Document for: Approval**

**Agenda Item: 6.9.6.3**

# 1 Decision/action requested

***The group is asked to discuss and approve the proposals.***

# 2 References

None

# 3 Rationale

This contribution updates the use case of network slice management capability exposure.

# 4 Detailed proposal

|  |
| --- |
| **First modification** |

## 5.1 Network slice management capability exposure

### 5.1.1 Description

A use case of network slice management capability exposure can be described as follows:

1. NSP selects the MnS that can be exposed externally.

2. NSP decides on constraints that shall be applied to the MnS when it is exposed externally. For example, NSP may decide to disallow certain operations, limit the Managed Object Instances that may be managed, or aggregate/anonymize sensitive data.

3. The MnS can be exposed directly, or NSP applies constraints before exposing the MnS.

4. NSP publishes the MnS in a service directory.

5. NSC authenticates itself, discovers the available MnSs and request for authorization to access a particular MnS.

6. , NSC request to access the MnS.

7. NSP validates the authorization and decides to allow or not to allow access.

### 5.1.2 Issue and gaps

5.1.2.1 Issues

How to publish MnS which can be exposed to BSS to a suitable MnS producer for network management capability exposure is not specified in existing 3GPP management system

5.1.2.1 Gaps

Editor’s Note: FFS