**3GPP TSG- Meeting #4 *3***

**, , –**

**Source: Samsung**

**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 exposure policies 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 any constraints before exposing the resulting functionality as an MnS.

4. NSP publishes the MnS in a service directory.

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

6. , NSC request to accesses the MnS.

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

### 5.1.2 Issue and gaps

5.1.2.1 Issues

The MnS need to be published so that it can be discovered by the consumers. The related exposure policies need to be applied before exposing the MnS to the authorized consumers.

5.1.2.1 Gaps

1. How to publish a MnS.
2. How an external consumer can discover the available MnS;
3. And, how to define exposure policies that shall be applied when an MnS is accessed by an external consumer is not specified in existing 3GPP management standards.