**3GPP TSG-SA5 Meeting #141-e** ***S5-221434rev2***

**e-meeting, 17 -26 January 2022**

**Source: Lenovo, Motorola Mobility**

**Title: Update position and add solution for direct MnS exposure**

**Document for: Approval**

**Agenda Item: 6.5.2**

# 1 Decision/action requested

***Please approve***

# 2 References

[1] 3GPP TR 28.824 v0.4.0 Study on network slice management capability exposure (Release 17)

# 3 Rationale

This contribution addresses the EN and provides a possible solution to direct exposure to MnS scenario

# 4 Detailed proposal

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

Start of changes

Second Change

## 5.x Exposure to application servers and application functions

Editor’s note: Section to be updated based on result of S5-221089

### 5.x.1 Description

### 5.x.2 Issue and gaps

Issues:

The external entities need to be aware of the existence of the operator and its MnS. This issue depends on the dynamism supported by the system. In a highly dynamic and changing system the issue is equivalent to Section 5.4 eMnS support to discovery systems

The external entities need to gain credentials to access the exposed MnS.

Third change

# 7 Possible solutions for network management capability exposure

### 7.x Possible solution for “Exposure to application servers and application functions” – Section 5.x

For consumer entities internal to the operator the access details to MnS are directly configured by the operator.

For consumer entities (AS or AF) external to the operator, the assumption is that the appropriate business relation exists between the entity owner and the operator. Given such an assumption, the following steps recommend how the consumer entities can access the exposed MnS. The steps assume that the entity is aware of the MnS (this can be done via an MnS discovery service producer specified in 28.537

1. The entity approaches an access controlling entity (which may be the EGMF) requesting access to the MnS. Which MnS and how this access is provided is implementation and business agreement dependent and is completely controllable by the operator.
2. If authorized, and in accordance with the business agreement the access controlling entity provides access tokens (which may be limited in some way) to the consumer entity
3. These access tokens are then used by the consumer entity to access the exposed MnS

End of changes