**3GPP TSG-SA5 Meeting #141-eS5-221432rev1**

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

**Source: Lenovo, Motorola Mobility, CMCC**

**Title: Resolve EN in 5.4**

**Document for: Approval**

**Agenda Item: 6.5.2**

# 1 Decision/action requested

***Please approve***

# 2 References

[1] 3GPP TR 28.824 V0.4.0

# 3 Rationale

This contribution proposes the remove the EN in 5.4.

# 4 Detailed proposal

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

Start of changes

## 5.4 eMnS support to discovery systems

### 5.4.1 Description

An eMnS should be allowed to register to an authorized supported discovery system such that interested authorized consumers (within or external to the operator) are able to discover it. This implies that the eMnS is only exposed to a discovery system where a pre-existing contract allows for such an exposure.

1. An operator would like to register its eMnS to a trusted discovery system. The operator configures the eMnS with the discovery system’s address and the appropriate level of exposure for the registration. The eMnS is registered at the discovery system with the appropriate level of exposure.

2. The operator performs changes in its management system that impacts the information exposed by the eMnS. The changed information is automatically updated in the discovery system.

3. In case the relationship between the operator and a discovery system ends, which implies the system is no longer trusted, then the eMnS automatically requests deletion of its registration in the discovery system.

Editor’s Note: How the “is no longer trusted” would be handled by the authentication and authorization and system is FFS, since it is not clear how a non-trust party can be trusted to delete a registration entry.

### 5.4.2 Issue and gaps

There are several issues that need to be resolved.

Issues:

There is a difference if the discovery system is external or internal to the operator. A discovery system for internal use may still exist outside the scope of management.

There is an issue with managing which consumers have access to the discovery system and could theoretically consume the management service.

There is an issue with the trust (i.e., authentication and authorization) between the three parties (MnS producer/operator, MnS consumer/customer and discovery system owner) in this use case

Gap:

To limit issues the exposure from a discovery system of the operator may only provide “read” permissions (w.r.t the eMnS) without authentication and authorization. To execute the discovered eMnS the consumer still needs to be authenticated and authorized by the management system. Therefore, there is a gap in the difference in exposure for consumption, and exposure for discovery which needs to be solved.Second Change

# 7 Possible solutions for network management capability exposure

Editors note: reallocate section according to agreement in S5-221089,

### 7.1 Possible solution for “exposed MnS support to discovery systems” – Scenario 5.4

The steps of the solution are as follows:

1. A MnS consumer configures using the appropriate MnS (for example the generic provisioning service) the details of the external discovery service location and other supporting details (for e.g., authentication and authorization). Further, the detail on which parts of which MnS (component A) IOCs and which instances of the corresponding MOI (component B) and corresponding data (component C) can be registered with the discovery service/system. As an example, the operator may want to register her the ability to provision (Management object A) a particular slice type (NSSAI-ID) at a certain coverage area (coverageArea item 6.3.3 TS28.541) with some additional details (example: supported latency or maxNumberofUEs or delayTolerance) to an external discovery service or system.
2. In addition to the information of what is externally registered, information relating to the address of the exposed MnS needs to be provided. This could be default information based on the operator in the external discovery system or in case of a trusted discovery the address of the actual exposed management service.
3. The 3GPP Management System registers the exposed management component A, B and C as configured in step 1 to the appropriate external discovery service/system.
4. Eventually, if any of the exposure details change – for example the same slice type can now be supported in a new coverageArea – the registration to the external discovery system may now need to be updated.

Editor’s note: provide a picture explain the operator and JV relationship below

The solution for the trust issue between the three MnS discovery system owner, MnS consumer and the MnS producer is scenario dependent. Let’s take for example a multi-operator network scenario. In this scenario let’s take operator A as an MnS producer, a joint venture of multiple operators as a MnS discovery system owner and operator B as an MnS consumer. Both Operator A and Operator B have business relations with the joint venture thereby creating a trust relationship between Operator A and the joint venture (JV) AND operator B and the joint venture. The JV provides the authorization and authentication details for each of the operator to use the discovery service. Operator A may then expose aspects of its MnS that it considers ok to expose with the JV. Operator B can then discover the MnS offered by operator A and contact operator A to access them. If operator B requires a higher level of access than operator A provides in the JV by default, then they need to form a new business relationship.

End of Changes