**3GPP TSG-SA5 Meeting #145-eS5-225218rev4**

**e-meeting, 15 - 24 August 2022**

**Source: Alibaba group**

**Title: pCR 28.824 Update Solution for Network slice management capability**

**Document for: Approval**

**Agenda Item: 6.9.6.3**

# 1 Decision/action requested

***For approval***

# 2 References

[1] 3GPP TR 28.824 V0.8.0 Study on network slice management capability exposure

# 3 Rationale

This contribution is to resolve the position and functionality of exposure governace. Solution#10 suggests that the MnS consumer needs to firstl conduct authentication and authorization with CAPIF core function. If successfully authorized by the CCF, the MnS consumer can obtain access token from CCF.The access token can support the MnS consumer to consume the allowed element information of MnS once the access token is verified from MnS producer.

For the management domain, network operator may want to enforce exposure governace, i.e. to perform access control, filtering and simplification for MnS. For example, an subset of MnS can be derived from MnS A following exposure goverance. The exposure goverance functionality within the API domain can support the validation of access token from each MnS customer and allow the MnS consumer to consume a proper subset of MnS that matches the access permission from access token.

This contribution proposes to update the solution#10 in order to relect the functionality of exposure goverance within the service API domain.

# 4 Detailed proposal

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

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

## 7.10 Possible solution for network slice management capability exposure

This solutions supports exposure via CAPIF alternative 2and exposure via CAPIF alternative 3 as defined in 7.9.2 and 7.9.3.

This solution proposes to use CAPIF framework [14] to expose network slice management capabilities to external entities. The solution requires extending the existing CAPIF mechanism to support MnS exposure and authorization. This includes extending the ServiceAPIDescription (see clause 8.2.4.2.2 of [19]) to support the description of the 3GPP management services required for exposure. This also includes defining mechanism to build exposure governance rules for allowing granular access to MnS from external entities.

In addition to external entities, the same solution can be used to provide access to entities inside PLMN trust domain (see clause 3.1 of [14]). Three types of consumer are considered here;

* NOP-External: the consumer is external to PLMN trust domain,
* OAM-External: the consumers is external to 3GPP management domain e.g (5GC NFs, trusted AF and application layer entities e.g SEAL)
* OAM-Internal: consumer is internal to 3GPP management domain.



1. MnS Producer (acting as API Provider Domain Function) registers with CCF using Register\_API\_Provider operation as defined in 5.11.2.2.2 of [19].
2. MnS consumer (acting as API Invoker) registers with CCF. The registration request will include related MnS Consumer details as part of APIInvokerEnrolmentDetails (8.4.4.2.2 of [19]).

Editor’s Note 1: Whether the APIInvokerEnrolmentDetails (clause 8.4.4.2.2 of [19]) need to be extended with provided consumer details in FFS.

1. MnS producer publishing the available management services with CCF. MnS Producer can optionally perform transformation of MnS into service API(s) before publishing. In absence of this transformation MnS are considered to be service APIs being exposed to MnS Consumer.

Note: Whether this optional transformation is needed or not, and its implementation details, is out-of-scope of SA5.

Editor’s Note: Initiatives such as CAMARA are working on this kind of transformation.

1. MnS consumer gets authenticated with CCF as per the procedures defined in clause 8.10 of [14].
2. MnS consumer discovers the available service APIs using the CAPIF discovery mechanisms. CCF authenticates the MnS Consumer and reports the available management service described by the ServiceAPIDescription.
3. MnS consumer gets authorization to access available service APIs as per the procedures defined in clause 8.11 of [14].
4. MnS consumer gets authenticated with AEF as per the procedures defined in clause 8.14 of [14].
5. MnS consumer tries to access the service API.
6. MnS Producer checks the validity of the token including checking the granular consumer’s authorizations.

NOTE: When checking the granular consumer’s authorizations, the MnS producer may be able to provide original MnS following exposure goverance which includes filtering. As a result, MnS consumer may be able to access only a subset of original MnS via the response from the MnS producer. The exposure governance can be implemented by a dedicated MnS producer/MnF (e.g. EGMF) for exposure governance.

1. MnS Producer may interact with CAPIF Core for authentication, authorization and charging.
2. MnS Producer provides appropriate response.

NOTE: When this solution applies to alternative 3, the CAPIF core function becomes part of MnS Producer.

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