**3GPP TSG-SA5 Meeting #143-e *S5-223624***

**Online, , 9th May 2022 - 17th May 2022**

**Source: Samsung, AsiaInfo, Alibaba**

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

**Document for: Approval**

**Agenda Item: 6.5.22.3**

# 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 and propose a possible solution for the same.

# 4 Detailed proposal

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

# 2 References

The following documents contain provisions which, through reference in this text, constitute provisions of the present document.

- References are either specific (identified by date of publication, edition number, version number, etc.) or non‑specific.

- For a specific reference, subsequent revisions do not apply.

- For a non-specific reference, the latest version applies. In the case of a reference to a 3GPP document (including a GSM document), a non-specific reference implicitly refers to the latest version of that document *in the same Release as the present document*.

[1] 3GPP TR 21.905: "Vocabulary for 3GPP Specifications".

[2] TM Forum TMF622 Product Order API REST Specification

[3] TM Forum TMF641 Service Ordering API

[4] TM Forum TMF652 Resource Order Management API

[5] 3GPP TS 28.531: "Management and orchestration; Concepts, use cases and requirements"

[6] 3GPP TS 28.202: "Charging management; Network slice management charging in the 5G System (5GS); Stage 2"

[7] 3GPP TR23.700-99 “Study on Network Slice Capability Exposure for Application Layer Enablement (NSCALE)”

[8] 3GPP TS23.434 “Service Enabler Architecture Layer for Verticals (SEAL); Functional architecture and information flows.”

[9] 3GPP TS 28.541: "Management and orchestration; 5G Network Resource Model (NRM); Stage 2 and stage 3"

[10] 3GPP TS 28.537: "Management and orchestration; Management capabilities"

[11] 3GPP TS 28.533: "Management and orchestration; Architecture framework"

[12] TM Forum TMF633 Service Catalogue Management API

[13] TM Forum TMF620 Product Catalogue Management API

[14] 3GPP TS 23.222: “Common API Framework for 3GPP Northbound APIs; Stage 2”

[15] 3GPP TS 29.222: “Common API Framework for 3GPP Northbound APIs”.

[16] 3GPP TS 31.222: “Security aspects of Common API Framework (CAPIF) for 3GPP northbound APIs”.

|  |
| --- |
| **Next 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 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. NSP implements and deploys a Management Function which consumes the MnS. The MnS can be exposed directly or NSP applies any constraints, and exposes the resulting functionality as an MnS.

4. NSP publishes the MnS in a service catalog or service directory.

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

6. NSC accesses the MnS with proper authorization.

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

### 5.1.2 Issue and gaps

The following gaps are identified:

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

|  |
| --- |
| **Next modification** |

## 7.1 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 [15]) 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 [15].
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 [15]).

Editor’s Note 1: Whether the APIInvokerEnrolmentDetails (clause 8.4.4.2.2 of [15]) 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. MnS Producer will then decide whether to allow the access or not. This may also involve interaction with CAPIF Core for authentication, authorization and charging.
7. MnS Producer provides appropriate response.

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

Editor Notes 2: The solution requires MnS to be described as Service API. How the description is done is FFS. This will also include asserting whether the existing mechanism (e.g ServiceAPIDefinition datatype in [15]) need to be extended or not.

Editor Notes 3: Whether the authorization mechanism as defined in [14] need to be extended is FFS.