**3GPP TSG-SA5 Meeting #143-e *S5-223208***

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

**Source: Samsung**

**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”.

|  |
| --- |
| **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 publishes the MnS in a service catalog or service directory.

4. NSC discovers the available MnSes and request for authorization to access a particular MnS.

5. NSC access the MnS with proper authorization.

6. 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 support CAPIF alternative 2 and 3 as defined in 7.9.2.

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 operator trust domain. Three types of consumer are considered here; NOP-External: the consumer external to operator trust domain, OAM-External: the consumers external to 3GPP management domain e.g (5GC NFs, trusted AF and application layer entities e.g SEAL) and OAM-Internal: consumer internal to 3GPP management domain.



1. MnS consumer (acting as API Invoker) registers to consume management services with EGMF (acting as CAPIF Core Functions). Consumer will include ConsumerType (OAM Internal, OAM External, NOP External) in APIInvokerEnrolmentDetails. The APIInvokerEnrolmentDetails (clause 8.4.4.2.2 of [15]) need to be extended with ConsumerType.
2. MnS producer publishing the available management services with EGMF. Producer describes the exposed management services with ServiceAPIDescription as extended with this solution.
3. MnS consumer discovering the available management services using the CAPIF discovery mechanisms. EGMF authenticate the MnS Consumer and reports the available management service described by the ServiceAPIDescription.
4. The secure TLS session is established between MnS Consumer and EGMF as defined in (clause 6.5 of [16]). MnS consumer request for OAuth based authorization, from EGMF, to access the management services. EGMF provides OAuth token with the token claims defined in this solution. The OAuth token claims will be created based on exposure governance rule as decided by the MnS Producer for each MnS to be exposed. MnS consumer tries to access the management service. Producer checks the validity of the token including checking the granular consumer’s authorizations. Producer will then decide whether to allow the access or not.

Note: The solution supports having a CAPIF Core function as an independent, not related with EGMF, entity available with the operator.

## 7.1.1 Extensions required for ServiceAPIDescription

The attributes of ServiceAPIDescription [15] data type need to be extended with the following set of attributes (not exhaustive).

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Attribute name** | **Data Type** | **P** | **Cardinality** | **Description** |
| ExposureDetails |  | M | 1 | Defining the details for exposure for all three type of MnS Consumer |
| >NOPExternal | Exposure Governance Rules | M | 1..\* | It defines the granular access authorization for consumer which are external to operator trust domain e.g vertical customers, enterprise. |
| >OAMExternal | Exposure Governance Rules | M |  | It defines the granular access authorization for consumer which are external to OAM domain e.g NWDAF, RIC. |
| >OAMInternal | Exposure Governance Rules | M |  | It defines the granular access authorization for consumer which are internal to OAM domain e.g Performance MnS Producer. |
| ServiceLocation |  | M | 1…\* | The location this MnS is serving i.e the serving location for the related NRMs or Managed Functions. This can be Geographical coordinates, TAIList, Civic address.  The consumer may be interested in the management of a node at a particular location only. Hence, it may interested in the MnS capable of managing the node in the same location |
| ServiceAvailability |  | M | 1…\* | The availability of the service. This will be “to” and “from” timestamp defining the service availability for the external consumers.  The consumer may require to use the MnS at a particular point of time because of the time bound services. |
| ServiceReliability |  | M | 1 | The reliability of the service in terms of success rate of the invoked Operations.  The consumer (e.g MC, V2X) may be interested in the MnS with 99.99% reliability only. |
| ServiceLatency |  | M | 1 | The minimum latency supported by the service. Latency will be determined by the average time taken to respond to an invoked operations.  The consumer of URLLC service may be interested in the MnS with minimum latency. |
| MnS Type, Label, Version, Address |  | M | 1 | Type of MnS (PROVISIONING, FAULT\_SUPERVISION, PERFORMANCE\_ASSURANCE), Label: human readable description, Version: version of the MnS. |

7.1.2 OAuth Access Token Claims indicating granular MnS access authorization

The OAuth token claim for CAPIF defined in [16] may need to be extended with the following scope parameter.

|  |  |
| --- | --- |
| Parameter | Description |
| exp | REQUIRED. The expiration time of the access token. Implementers MAY provide for some small leeway, usually no more than a few minutes, to account for clock skew (not to exceed 30 seconds). |
| client\_id | REQUIRED. The identifier of the consumer making the API request |
| scope | REQUIRED. A structure containing granular access authorization per allowed MnS.  *<MnS>*  *<Component A></Component A>*  *<Component B>*  *<uri></uri>*  *<permission>*  *<attName></attName>*  *<attPermission></attPermission>*  *</permission>*  *</Component B>*  *<Component C>*  *<allowedMeasurement></allowedMeasurement>*  *<managedEntity></managedEntity>*  *<perfMeasurement></perfMeasurement>*  *<allowedKPI></<allowedKPI>*  *<allowedAlarmInfo></allowedAlarmInfo>*  *</Component C>*  *<allowedNotifications></allowedNotifications>*  *</MnS>* |

7.1.3 Exposure Governance Rules

The following structure defines the exposure governance rules for a particular MnS to be exposed. This will facilitate the granular MnS access authorization.

|  |  |  |
| --- | --- | --- |
| **Attributes** | **Support** | **Description** |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
| allowedComponentA | M | The list of operation of the MnS, consumer is authorized to access. This will be the {MnSRoot} in case of OpenAPI implementations. |
| allowedComponentB <<dataType>> | M | The list of IOC the consumer can access. |
| >uri | M | The URI of the NRM fragment (IOC) |
| >permission <<dataType>> | M | The list of attributes permission present in the IOC |
| >>attName | M | Attribute name present in the IOC |
| >>attPermission | M | The type of permission (Readonly, Writeable |
| allowedComponentC <<dataType>> | O | The list of performance measurement and the KPI, the consumer is authorized to collect. |
| >allowedMeasurement <<dataType>> | M | List of authorized measurements |
| >>managedEntity | M | Managed entity producing the measurement |
| >>perfMeasurement | M | Measurement the consumer is authorized to collect. |
| >allowedKPI <<dataType>> | M | List of authorized KPI |
| >allowedAlarmInfo | O | List of alarm info the consumer is authorized to receive |
| >>managedEntityAlarmInfo | M | Alarm info |
| >allowedNotifications | M | The notifications which consumer is authorized to subscribe for. |