**3GPP TSG-SA5 Meeting #144-e *S5-224042***

**Online, , 27th June 2022 – 1st July 2022**

**Source: Samsung**

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

**Document for: Approval**

**Agenda Item: 6.9.6.3**

# 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** |

## 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]).
3. 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.
7. MnS Producer may interact with CAPIF Core for authentication, authorization and charging.
8. MnS Producer provides appropriate response.

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

## 7.10.1 Using ServiceAPIDescription to describe MnS.

As per CAPIF framework the service API is described using ServiceAPIDescription datatype defined in [19]. This data type is used to facilitate service API description in various CAPIF APIs e.g CAPIF\_Discovery\_Service\_API, CAPIF\_Discovery\_Publish\_API etc. When using CAPIF framework to expose MnS to the consumers, the MnS need to be described using same ServiceAPIDescription datatype.

The access authorizations for a particular consumer or the group of consumer may differ for each MnS e.g OAM\_External consumers may not be authorized to access Discovery MnS. When the access is provided it may be restricted only to a particular IOC(s). The access can be further (readonly or writable) restricted to an attribute(s) within the IOC. Similarly, consumers may be restricted to only a set of measurements, KPI and notifications. The existing ServiceAPIDescription does not provide means to define this granular level of exposure details to MnS for various type of MnS Consumers.

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

Editors Note: The complete list of attributes is FFS.

|  |  |  |  |
| --- | --- | --- | --- |
| **Attribute name** | **Support** | **Cardinality** | **Description** |
| ExposureDetails | M | 1 | Defining the granular access authorization, based on Exposure Governance rules defined in 7.1.2, for details for exposure for all three type of MnS Consumer:NOPExternal: Consumer which are external to operator trust domain e.g vertical customers, enterprise. OAM External: Consumer which are external to OAM domain e.g NWDAF, RICOAMInternal: Consumer which are internal to OAM domain e.g Performance MnS Producer |
| ServiceLocation | O | 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 | O | 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 | O | 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 | O | 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. |

7.10.2 Exposure Governance Rules

The following structure defines the exposure governance rules for a particular MnS to be exposed to various consumers. This will facilitate the granular MnS access authorization. This type of granular access is not specified as part of CAPIF Framework[14]. These rules shall be implemented by a management function (e.g EGMF) implementing CCF functionalities.

|  |  |  |
| --- | --- | --- |
| **Attributes** | **Support** | **Description** |
| ConsumerID | M | The identification of the consumer provided at the time of registration. |
| ConsumerType | O | The type of consumer (OAM-Internal, OAM-External{gNB, CU-CP, NWDAF}, NOP-External{ASP, ECSP} ) |
| authorizedMnS <<dataType>> | M | List of management services and its capabilities the consumer is authorized to access. This will include the followings:1. MnS Type, Label and Version: Type of MnS (PROVISIONING, FAULT\_SUPERVISION, PERFORMANCE\_ASSURANCE), Label: human readable description, Version: version of the MnS.
2. allowedComponentA: The list of operation of the MnS, consumer is authorized to access. This will be the {MnSRoot} in case of OpenAPI implementations.
3. allowedComponentB: The list of IOC the consumer can access. This will include:
	1. Uri: The URI of the NRM fragment (IOC)
	2. Attribute Permission: List of attributes in the IOC and the associated permission for each attribute. The type of permission can be Readonly or Writeable
4. allowedComponentC: The list of performance measurement/KPI and Alarm info, the consumer is authorized to collect.
5. allowedNotifications: The notifications which consumer is authorized to subscribe for.
 |

7.10.3 OAuth Access Token Claims indicating granular MnS access authorization

The authorization mechanisms defined in [14] are based on OAuth 2.0. The API Invoker need to send Access Token Request message to the CAPIF core function as per the OAuth 2.0 [x] specification. The CAPIF core function successfully verifies the Access Token Request message, the CAPIF core function shall generate an access token specific to the API invoker and return it in an Access Token Response message. The token claims, clause C.2 of [20], provides token expiration time, client ID and the list of service APIs the client is authorized to access.

Using CAPIF framework to expose MnS requires token claims to be extended in order to support granular access to MnS for several MnS Consumers.

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.  |
| client\_id | REQUIRED. The identifier of the consumer making the API request |
| scope | REQUIRED. A structure containing granular access authorization per authorized 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>* |