**3GPP TSG-SA5 Meeting #136e *S5-212033rev2***

**e-meeting, 01 – 09 March 2021** (revision of S5-211205)

**Source: Alibaba Group**

**Title: New SID on management aspects of network slice management capability exposure**

**Document for: Approval**

**Agenda Item: 6.2**

3GPP™ Work Item Description

Information on Work Items can be found at <http://www.3gpp.org/Work-Items>   
See also the [3GPP Working Procedures](http://www.3gpp.org/specifications-groups/working-procedures), article 39 and the TSG Working Methods in [3GPP TR 21.900](http://www.3gpp.org/ftp/Specs/html-info/21900.htm)

# Title: Study on management aspects of network slice management capability exposure

## Acronym: FS\_NSCE

## 1 Impacts

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Affects:** | UICC apps | ME | AN | CN | Others (specify) |
| **Yes** |  |  |  | X |  |
| **No** | X | X | X |  |  |
| **Don't know** |  |  |  |  | X |

## 2 Classification of the Work Item and linked work items

### 2.1 Primary classification

|  |  |
| --- | --- |
|  | Feature |
|  | Building Block |
|  | *Work Task* |
| X | Study Item |

### 2.2 Parent Work Item

|  |  |
| --- | --- |
| Parent Work Items | |
| Unique ID | Title |
|  |  |

### 2.3 Other related Work Items and dependencies

|  |  |  |
| --- | --- | --- |
| Other related Work Items (if any) | | |
| Unique ID | Title | Nature of relationship |
| 760065 | Management and Orchestration; Provisioning | SA5 work item |
| 720048 | Study on Management and Orchestration of Network Slicing for next generation network | SA5 study item |
| 900023 | Study on Charging Aspects for Network Slicing Phase 2 | SA5 study item |
| 860022 | Management and Orchestration; Network Slice Management Enhancement | SA5 study item |

## 3 Justification

Network slice management has been studied and standardized in SA5, see TS 28.531. The network slice related management functions (e.g. CSMF, NSMF and NSSMF) can coordinate with NFV MANO and instantiate network slice when needed. To simplify the instantiation procedure, ServiceProfile (or network slice template derived from GSMA GST) are used during the NetworkSlice instance lifecycle phases.

In current specification, CSMF within the network slice related management functions can make the requirement for ServiceProfile, and related network slice instance for applications. However, since the requirement of applications are changed dramatically over time, third parties within different verticals (e.g. online conferencing, high resolution video) may also have their unique requirements set on the network slices that are needed for satisfying to the network KPIs for certain services. Without the network slice management capability exposure functionalities, the manual configuration of ServiceProfile between the platform and the Operator’s network slice management system causes redundant resources in terms of personnel and time. How does the 3GPP management system conditionally expose MnSs to enable vertical to manage (e.g. monitor, optionally provision) the service need to be studied. So far, there is no study in SA5 for this purpose.

To solve the aforementioned issue, network slice related management functions, which belong to the Operator’s telecom management system, can have a series of exposure services that can be used by the third parties in order to make request for specific network slice based service for certain application level service. This is especially applied in the case that a giant service provider wishes to establish dedicated connection with the Operator’s OAM system under a big contract. The network slice management exposure functionalities can help Operator to efficiently obtain network slice requirement from verticals, which can also be cloud service provider, and to provision ServiceProfiles based on which more vertical customers will request for network slice instantiation.

Existing specification (i.e. TS 28.533) has defined a NF known as EGMF which can expose Operator management related capability to the communication service customer.

TR 28.811 clause 7.2 identifies certain types of network slice management capabilities that may be exposed by EGMF, but there is no identified method to formally describe the agreement between MnS producer and consumers which can have different types that produces different use cases, and how this agreement should be used to configure EGMF.

MnS consumers may have different types, for example, application provider, enterprise, vertical, etc, different types of MnS consumers may have different agreements with their MnS producer based on their use cases. For example, MnS consumer A which is an application provider may have an agreement with NOP-B to read partial attributes of the managed object NetworkSlice, for example, via the getMOIAttributes operation, defined in 28.532. This will allow MnS consumer A from vertical to read the operationalState and administrativeState of the NetworkSlice instance. MnS consumer B which is a large enterprise may have an agreement with NOP-B for controlling the adminstrativeState of the NetworkSlice instance. NOP-B may allow MnS consumer B to have write access to the managed object NetworkSlice via the modifyMOIAttributes operation. MnS consumer C which is a vertical from vertical may have an agreement with NOP-B for creating a new ServiceProfile through createMOI operation. Since different types of MnS consumer may have different use case and agreement with the producer, the policy for agreement needs to be decoupled with different types and should be flexible and generic enough to fit in different types of MnS consumer and their related use case. So far there is no such study on this aspect.

SA3 has studied the access control mechanism for the protection of management interface, for example the authroization of management service consumer’s request. However, SA3 only addressed access control enforcement when MnS consumer accessing MnS provided by MnS producer, it does not specify what kind of MnSs can be exposed for different types of MnS consumers in different use cases.

Therefore, this study will focus on the method that formally describes the above agreement between MnS producer and consumers with different types (e.g. application provider, enterprise, vertical, etc) and how this agreement should be used to configure EGMF to enable flexible network slice management capability exposure. The rule of agreement should be generic and can be applied in different use cases.

## 4 Objective

The study item will be conducted with the following objectives:

- Investigate the Use cases (e.g. NSaaS mode where the CSP might be a different entity from the network Operator) and requirements for enablement of network slice management capability exposure.

- Study the method to formally describe the policy filter between MnS producer and consumer with different types e.g. in NSaaS mode where a CSC/NOP can have the policy filter access with or without passing BSS, and study how this agreement can be used for network slice management capability exposure.

- Study the aggregation of attributes for policy filter based on different type of MnS consumers (e.g. the outermost CSC in NSaaS mode) and their use cases.

NOTE1: The network slice management capability exposure for Non-standardized attribute for ServiceProfile can be studied in this SID.

NOTE2: The charging aspects of the management of network slice management capability is out of the scope of this SID.

NOTE3: Whether the policy filter can be used to configure EGMF is FFS.

## 5 Expected Output and Time scale

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **New specifications** | | | | | |
| Type | TS/TR number | Title | For info  at TSG# | For approval at TSG# | Remarks |
| TR | 28.YYY | Management aspects of network slice management capability exposure | SA#91  Mar 2021 | SA#92  Jun 2021 |  |

|  |  |  |  |
| --- | --- | --- | --- |
| **Impacted existing TS/TR** *{One line per specification. Create/delete lines as needed}* | | | |
| TS/TR No. | Description of change | Target completion plenary# | Remarks |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

## 6 Work item Rapporteur(s)

Xiaobo Yu, Alibaba Group (shibo.yxb@alibaba-inc.com)

## 7 Work item leadership

SA5

## 8 Aspects that involve other WGs

SA3 for security aspects. Coordination with SA and RAN WGs may be needed.

## 9 Supporting Individual Members

|  |
| --- |
| Supporting IM name |
| Alibaba |
| China Mobile |
| Intel |
| Huawei |
| Xiaomi |
| Lenovo |
| Matrixx |
| Motorola Mobility |
|  |
|  |
|  |
|  |