**3GPP TSG-SA5 Meeting #141-e *S5-221230r01***

**e-meeting, 17 – 26 January 2022** (revision of S5-XXXXXX)

**Source: Alibaba Group**

**Title: WID Revised Study on network slice management capability exposure**

**Document for: Approval**

**Agenda Item: 6.2**

**TSG SA Meeting #91E SP-210131**

**18 - 29 March 2021, Electronic meeting**

**Source: SA WG5**

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

**Document for: Approval**

**Agenda Item: 6.3**

**3GPP TSG-SA5 Meeting #136e *S5-212368***

**e-meeting, 01 – 09 March 2021** (revision of S5-212033rev5)

**Source: Alibaba Group**

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

## Acronym: FS\_NSCE

## Unique identifier: 910026

Potential target Release: {Rel-18}.

## 1 Impacts

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Affects:** | UICC apps | ME | AN | CN | Others (specify) |
| **Yes** |  |  | X | X |  |
| **No** | 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 |
| 860022 | Management and Orchestration; Network Slice Management Enhancement | SA5 study item |
| 890016 | Study on access control for management service | 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.

Network Slice Provider (e.g. Verticals) can have contract with Operator for the usage of network slice for communication service. Besides simply having contract for communication service, the users within different verticals (e.g. online conferencing, high resolution video) may further have their own requirements on certain management capabilities (e.g. information retrieval for network performance statistics and characteristics, and control functionalities) of the network slices that are needed for certain application services. How does the 3GPP management system conditionally expose MnSs to enable certain types of externals, e.g. verticals and service providers, to manage (e.g. monitor, optionally provision) the service need to be studied.

This may include two aspects:

1) What: What MnS, under what condition is suitable to expose to what types of MnS consumers (verticals and service providers). For example, certain MnS may not be suitable to be exposed to certain types of users while certain MnS may be suitable to be exposed and others may be suitable to be exposed with certain conditions and limitations. These can form a guideline, e.g. set of rules, principles, for the operator to open the network slice management capability exposure properly based on different types of MnS consumers.

2) How: How to expose those MnSs in a flexible way that can fulfil the requirement. This includes the mechanisms that are used to express the set of rules from the study result of 1).

So far, there is no study in SA5 for this purpose.

Current study of FS\_MNSAC focuses on the enforcement of the access policy of MnS. While this study focuses on the mechanisms needed for specifying and handling rules for exposure of management capabilities and management services to external MnS consumer, if not covered by existing specification and studies such as FS\_MNSAC. The enforcement of the rule will not be studied in this SID.

## 4 Objective

The study item will be conducted with the following objectives:

- Identify use cases and requirements regarding exposure of management capabilities and management services to externals, e.g. verticals and service providers.

- Conduct an analysis to determine gaps in existing specifications and studies (such as FS\_MNSAC) based on the identified requirements (see bullet point one).

- Propose mechanisms needed for specifying and handling rules for exposure of management capabilities and management services to external MnS consumer, if not covered by existing specification and studies such as FS\_MNSAC.

- Use case and requirements based on different types of NSCs;

- The study of EGMF/MCEG considering the following question:

* + what NSC related information (e.g., NSC id, NSC granted capabilities) does the NSP send to the NOP?
  + how does the NOP manage this information in relation to the existing NetworkSlice and NetworkSliceSubnet IOCs?

- Support network slice capability exposure without going through BSS.

- Support for external entities discovery eMnS of an Operator.

- Support of one single exposure layer to make all the exposure capabilities (e.g. exposure via NSC-NSP service interaction) available for NSCs.

- Relation to other SA5 work/study items.

- Derive recommendations for a normative work.

NOTE1: The charging aspects of the management of network slice management capability is out of the scope of this SID.

NOTE2: The enforcement of the mechanism that used to express the set of rules for network slice management capability exposure can be studied in FS\_MNSAC.

## 5 Expected Output and Time scale

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **New specifications** | | | | | |
| Type | TS/TR number | Title | For info  at TSG# | For approval at TSG# | Rapporteur |
| TR | 28.824 | Network slice management capability exposure | SA#97  Sept 2022 | SA#99  March 2023 | shibo.yxb@alibaba-inc.com |

|  |  |  |  |
| --- | --- | --- | --- |
| **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 |
| AsiaInfo |
| China Mobile |
| Intel |
| Huawei |
| Xiaomi |
| Lenovo |
| Matrixx |
| Motorola Mobility |
| NEC |
|  |
|  |