**3GPP TSG-SA5 Meeting #145-e *S5-225158rev1***

**e-meeting, 15 - 24 August 2022**

**Source: Huawei**

**Title: Rapporteur proposal**

**Document for: Approval**

**Agenda Item: 6.9.1.1**

# 1 Decision/action requested

***Discuss and approve on the proposal.***

# 2 References

[1] TR 28.907 Study on enhancement of management of non-public networks v0.3.0

# 3 Rationale

Some clean-up proposals for the draft TR 28.907 [1] are proposed from Rapporteur point of view.

# 4 Detailed proposal

This document proposes the following changes in TR 28.907 [1].

|  |
| --- |
| **1st Change** |

## 3.2 Symbols

Void.

|  |
| --- |
| **Next Change** |

### 5.1.2 Potential solutions

#### 5.1.2.1 Potential solution #1: fault management of NPN and 5G industry terminals

##### 5.1.2.1.1 Introduction

This clause provides a potential solution for fault management capabilities scoping NPN and 5G industry terminals.

##### 5.1.2.1.2 Description

In order to provide fault management capabilities scoping NPN and UEs representing 5G industry terminals, an NPN management system should monitor the fault of NPN and large quantity of 5G industry terminals which may be deployed in an enterprise.

* For the fault management of NPN, the network alarm can be discovered by analyzing performance data or network alarm event reporting. In this case, the generic fault supervision management service and performance assurance management service in section 11 of [7] can be re-used to collect the network performance data and alarm data.
* For the fault management of 5G industry terminals deployed in an enterprise, the NPN management system should support to performance monitoring and fault diagnosis for 5G industry terminals. NPN management system can collect the performance data and then execute data analysis for alarm detection, localization and/or resolution. The performance data collected from industry terminal may include DL/UL throughput, end to end latency, packet loss, etc. The trace control and configuration of MDT in clause 4.1, 4.2 and 6 of [9] can be reused for trace/UE measurements activation/deactivation and MDT report to collect MDT data from 5G industry terminals.

Editor's note 2: Whether the data analysis is based on 3GPP management capabilities, and which these capabilities are, is FFS.

### 5.1.3 Conclusion

Editor's Note: This clause provides the conclusion from the aspect of impact on normative work.

|  |
| --- |
| **Next Change** |

### 5.2.2 Potential solutions

#### 5.2.2.1 Potential solution #1: Management of the related information for NPN service customer

##### 5.2.2.1.1 Introduction

This clause describes briefly the potential solution for management of the related information for NPN service customer.

##### 5.2.2.1.2 Description

An NPN is provided to a vertical (playing the role of NPN-SC) for private use. Before an NPN is created, an MNO (playing the role of NPN-SP/NPN-OP) needs to authenticate the vertical. If the authentication is passed, the MNO management system should manage the related information for NPN service customer, for example, allocating a new identity of the vertical which can be used in MNO management system and creating the context of the vertical to keep the new identity, authorized available management capabilities, required coverage area and so on.

The procedure of management of the related information for NPN service customer is following. The pre-condition of the procedure is the business agreements between MNO and NPN-SC is reached.



Figure 5.2.2.1.2-1: Procedure of management of the related information for NPN service customer

1. NPN-SC provides the vertical information (e.g. human readable name of vertical, subscribed management capabilities exposed to vertical, etc.) to register a vertical to NPN-SP/NPN-OP through an NPN-SC registration request message. This message may be interacted with BSS layer. But the BSS layer should forward the subscription data to OSS layer to authorize the exposure of management capabilities and corresponding managed resources to NPN-SC.
2. NPN-SP/NPN-OP receives the vertical information from NPN-SC and executes the authentication and authorization for a vertical. The NPN-SP/NPN-OP allocates a new identity which is associated with the vertical identity and creates the context information of the vertical in local. The context information can be managed in form of NRM IOCs. The NPN-SP/NPN-OP uses the allocated new identity in MNO management system to identify the corresponding vertical.

Editor's note: The details of the context information of the vertical in NPN management system is FFS.

1. The NPN-SP/NPN-OP sends NPN-SC registration response message to the NPN-SC including the authentication result (e.g. success or failure), the new identity, authorized available management capabilities information and other attributes which are part of the context information of the vertical.

Editor's note: The outcome of management capability exposure governance in FS\_NSCE study item will be taken into consideration for identifying the authorized available management capabilities information in step 3).

### 5.2.3 Conclusion

Editor's Note: This clause provides the conclusion from the aspect of impact on normative work.

|  |
| --- |
| **Next Change** |

### 5.3.2 Potential solutions

Editor's Note: This clause provides the potential solutions.

### 5.3.3 Conclusion

Editor's Note: This clause provides the conclusion from the aspect of impact on normative work.

|  |
| --- |
| **Next Change** |

### 5.4.2 Potential solutions

#### 5.4.2.1 Potential solution #1: high level process for NPN SLA management

#### 5.4.2.1.1 Introduction

This clause describes briefly the potential solution for SLA monitoring and evaluation.

##### 5.4.2.1.2 Description

The high-level process for NPN SLA management in figure 5.4.2-1.



Figure 5.4.2.1.2-1: high level process for NPN SLA management

In figure 5.4.2.1.2-1, step 1-3 describes the workflows of NPN creation or update which is specified as NPN provisioning procedures in [2] in detail. The step 4, 5 and 3 are the NPN network monitoring and SLA assurance loop.

The NPN management system (e.g. NPN-SP/NPN-OP/NEP) collects performance data (e.g. packet delay in [10] and reliability in [11]) to monitor the NPN status through performance assurance MnS. Based on the network KPIs, the NPN management system evaluates the network availability and reliability to assurance the SLA fulfilment. If the SLA is not fulfilled, the NPN management system adopts some optimization methods to promote the network performance, such as SLA parameter coordination among RAN NEs, RAN resource and priority scheduling adjustment.

### 5.4.3 Conclusion

Editor's Note: This clause provides the conclusion from the aspect of impact on normative work.

|  |
| --- |
| **Next Change** |

Annex A (informative):
Plant UML source code

## A.1 Procedure for management of the related information for NPN service customer

The following PlantUML source code is used to describe the procedure for management of the related information for NPN service customer, as depicted by Figure 5.2.2.1.2-1:

@startuml

"NPN-SC" -> "NPN-SP/OP": 1. NPN-SC registration request

"NPN-SP/OP" -> "NPN-SP/OP":2. NPN-SC information\ncreation, e.g. allocating ID.

skinparam responseMessageUpArrow true

"NPN-SP/OP" -> "NPN-SC":3.NPN-SC registration response

 skinparam sequenceMessageAlign center

@enduml

## A.2 Procedure for high level process for NPN SLA management

The following PlantUML source code is used to describe the high level process for NPN SLA management, as depicted by Figure 5.4.2.1.2-1:

@startuml

"NPN-SC" --> [ 1. SLA Requirement mapping] "NPN-SP"

--> [ 2. SLS Requirement decomposition] "NPN-OP/NEP"

--> [ 3. Network creation\n/update]" NPN Network"

--> [ 4. Network monitoring\nand assurance]"NPN-OP/NEP"

--> [ 5. Network\nmonitoring]"NPN-SP"

@enduml

|  |
| --- |
| **End of change** |