**3GPP TSG-SA5 Meeting #135e *S5-212361***

**e-meeting, 1March – 9 March 2021 Revision of S5-212090**

**Source: Telefónica S.A.**

**Title: pCR 28.557 Applicability of management modes considering the deployment options of individual NPN functions.**

**Document for: Approval**

**Agenda Item: 6.4.1**

# 1 Decision/action requested

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

# 2 References

[1] TS 28.557 Management of non-public networks; Stage 1 and stage 2 v0.2.0

[2] TS 23.501 System architecture for the 5G System (5GS); Stage 2 v16.7.0

# 3 Rationale

This contribution aims to discuss the applicability of management models defined in Section 3.3 considering the deployment options of individual NPN functions. This discussion is captured in an informative annex.

# 4 Detailed proposal

This document proposes the following changes in TS 28.557 [1].

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

## 4.4 Management of SNPNs

An SNPN is deployed as an isolated network from PLMN. An optional connection to the public network services via the firewall, can be employed to enable NPN customers to access to public network services, such as voice, while within NPN coverage, see figure 1 in clause 5.2 of [5].

To manage a SNPN which is a 5GS (i.e. NG-RAN and 5GC) that can be optionally complemented with other access networks based on non-3GPP technologies (i.e. IEEE Wi-Fi), the standalone SNPN management system needs a dedicated NPN identifier. The combination of a PLMN ID and Network identifier (NID) is used to identify an SNPN.

The NID shall consist of an assignment mode and an NID value, see figure 4.4-1.



Figure 4.4-1: Network Identifier (NID)

The NID can be assigned using the following assignment models, see clause 5.30.2.1 of TS 23.501 [3] and clause 12.7.1 of TS 23.003 [6]:

- Self-assignment: NIDs are chosen individually by NPN-OP for SNPNs at deployment time (and may therefore not be unique) but use a different numbering space than the coordinated assignment NIDs as defined in TS 23.003 [6]. This assignment model is encoded by setting the assignment mode to value 1.

- Coordinated assignment: NIDs are assigned using one of the following two options:

1. Option 1: The NID is assigned such that it is globally unique independent of the PLMN ID used. Option 1 of this assignment model is encoded by setting the assignment mode to value 0;

2. Option 2: The NID is assigned such that the combination of the NID and the PLMN ID is globally unique. Option 2 of this assignment model is encoded by setting the assignment mode to value 2.

NOTE: The details of NID are defined in clause 12.7 of TS 23.003 [6].

An SNPN, which includes 3GPP and non-3GPP segments, may be created for use of an NPN-SC. From management viewpoint, this means that the 3GPP and non-3GPP segments of this NPN are completely independent and separated from PLMN provided network functions. The NPN operator has full management control over the exclusive SNPN network functions, i.e., 3GPP segment which includes non-public 5GC and/or non-public NG-RAN, and non-3GPP segment.

An SNPN, which includes 3GPP segments only, may be created for use of an NPN-SC. From management viewpoint, this means that the 3GPP segments of this NPN are completely independent and separated from PLMN provided network functions. The NPN-OP has full management control over the exclusive SNPN network functions, i.e., 3GPP segments which includes non-public 5GC and non-public NG-RAN.

|  |
| --- |
| **2nd Change** |

## 4.5 Management of PNI-NPNs

A PNI-NPN is a NPN made available via a PLMN, by means of dedicated DNNs, or by one (or more) network slice instances allocated for the NPN [2]. In order to access PNI-NPN, the UE shall have a subscription for the PLMN.

PNI-NPN operation may optionally make use of the concept of Closed Access Group (CAG) [2], which enables the control of UE’s access to PNI-NPN on a per cell basis (CAG cells). The CAG concept is used to prevent UEs which are not allowed to access the PNI-NPN from automatically selecting and accessing the associated cell(s). The CAG cell broadcasts information such that only UEs supporting CAG are accessing the cell. This is not possible with the sole use of network slicing unless an operator specific barring is used. That is why CAG concept is needed for access control.

The PLMN ID identifies the network and the CAG ID identifies the CAG cells. Network selection and reselection is performed based on PLMN ID. Cell selection and reselection, and access control are done based on the CAG ID.

In a PNI-NPN scenario, the CAG management aspects include:

* Assignment and maintenance of CAG IDs.
* Managing the actual list of UEs that are allowed on the CAG. The information contained on this list must be shared between the NPN-SP and the NPN-SC.
* Access rights of individual CAG cells. The NPN-SC shall have the capability to configure access rights to CAG cells (e.g., allowed days / time slots for UEs provided to contractors of a company).

|  |
| --- |
| **3rd Change** |

Annex A (informative): Deployment considerations on NPN management modes.

The applicability of management modes (cf. clause 4.3) depends on the NPN scenarios under consideration. Different scenarios may exist, depending on the deployment considerations of individual NPN functions. Table A.x-1 and Table A.x.2 capture this variety for SNPN and PNI-NPN scenarios, respectively.

Table A.x-1 Applicability of management modes in different SNPN scenarios

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| NPN functions | | Mode 2a | Mode 2b | Mode 2c |
| NG-RAN | | indoor; outdoor | indoor; outdoor | indoor; outdoor |
| 5GC | Packet core (AMF, SMF, NRF, ...) | on-premise;  off-premise (deployed on MNO footprint) | on-premise | on-premise;  off-premise (deployed on hyperscaler footprint) |
| Subscription and data-storage manager (UDM, UDR, AUSF, …) | on-premise | on-premise | on-premise |
| UPF | on-premise;  off-premise (deployed on MNO footprint) | on-premise | on-premise |
| NOTE 1: In case of virtualization of 5GC functions, the VISP role is relevant. The VISP is in charge of managing the virtual resources which support the execution of those VNFs, each hosted by one or more VDUs.  NOTE 2: The vertical may play the VISP role for the virtualization of on-premise 5GC functions.  NOTE 3: The MNO may play the VISP role for the virtualization of off-premise 5GC functions in Mode 2a. These 5GC functions are dedicated to the NPN, and therefore are separated from PLMN functions (used for public use).  NOTE 4: An hyperscaler may play the VISP role for the virtualization of off-premise 5GC functions in Mode 2c.  NOTE 5: Off-premise UPF may need to be deployed at the Telco Edge Cloud, typically due to performance constraints. | | | | |

Table A.x-2 Applicability of management modes in different PNI-NPN scenarios

|  |  |  |  |
| --- | --- | --- | --- |
| NPN functions | | Mode 1a | Mode 1b |
| NG-RAN | | indoor; outdoor | indoor; outdoor |
| 5GC | Packet core (AMF, SMF, NRF, ...) | off-premise (deployed on MNO footprint) | off-premise (deployed on MNO footprint) |
| Subscription and data-storage manager (UDM, UDR, AUSF, …) | off-premise (deployed on MNO footprint) | on-premise;  off-premise (deployed on MNO footprint) |
| UPF | off-premise (deployed on MNO footprint) | on-premise; off-premise (deployed on MNO footprint) |
| NOTE 1: In case of virtualization of 5GC functions, the VISP role is relevant. The VISP is in charge of managing the virtual resources which support the execution of those VNFs, each hosted by one or more VDUs.  NOTE 2: The vertical may play the VISP role for the virtualization of on-premise 5GC functions.  NOTE 3: The MNO may play the VISP role for the virtualization of off-premise 5GC functions in Modes 1a and 1b.  NOTE 4: Off-premise UPF may need to be deployed at the Telco Edge Cloud, typically due to performance constraints. | | | |

|  |
| --- |
| **End of changes** |