**3GPP TSG-SA5 Meeting #130e *S5-202273***

**e-meeting, April 20-24 2020** *Revision of S5-202xxx*

**Source: Orange, Telefonica**

**Title: Additional considerations on NPN**

**Document for: Approval**

**Agenda Item: 6.6.2**

# 1 Decision/action requested

***The group is asked to discuss and agree on the proposal.***

# 2 References

[1] TS 28.807 1.0.0: Study on management aspects of non-public networks

# 3 Rationale

# 4 Detailed proposal

This document proposes the following changes in TS 28.807 [1].

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

## 3.3 Abbreviations

For the purposes of the present document, the abbreviations given in 3GPP TR 21.905 [1] and the following apply. An abbreviation defined in the present document takes precedence over the definition of the same abbreviation, if any, in 3GPP TR 21.905 [1].

NPN Non-Public Network

SNPN Stand-alone NPN

PNI-NPN Public Network Integrated NPN

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

# 4 Concepts and background

## 4.1 General

A Non-Public Network (NPN) is a 5GS deployed for non-public use, see TS 23.501 [3]. In contrast to public networks that offer mobile network services to the general public, non-public networks are intended for the sole use of a private entity such as a college or an enterprise. Non-public networks may be deployed on the entity’s defined premises such as a campus or a factory to provide coverage within a specific geographic area.

Non-public networks may be deployed in a variety of configurations, utilising both virtual and physical network functions, see TS 22.261 [2]. Specifically, see TS 23.501 [3], an NPN may be deployed as:

- a Stand-alone Non-Public Network (SNPN), i.e. operated by an NPN operator and not relying on network functions provided by a PLMN, or

- a Public network integrated NPN, i.e. a non-public network deployed with the support of a PLMN.

From the view of 5G-ACIA, non-public networks can be desirable for several reasons, see clause 4 of [4]:

- High quality-of-service requirements

- High security requirements, met by dedicated security credentials

- Isolation from other networks, as a form of protection against malfunctions in the public mobile network. Also, isolation may be desirable for reasons of performance, security, privacy, and safety

- Accountability. A non-public network makes it easier to identify responsibility for availability, maintenance, and operation

## 4.1a Model of roles

In the context of NPNs, responsibilities regarding operations have to be clearly defined and assigned to roles. The roles related to NPNs include:

- NPN operator: designs, builds and operates an NPN providing all the required network services and resources.

- NPN service provider: provides non-public communication services using an NPN. Designs, builds and operates these services, which are supported by the NPN operator provided network services.

- NPN service customer: consumes services offered by an NPN service provider.

There is a direct mapping between these roles and the ones defined in clause 4.8 of TS 28.530 [7], when network and services under consideration are non-public. The NPN operator role is a particularization of the Network Operator (NOP) role, the NPN service provider role is a particularization of the Communication Service Provider (CSP) role and the NPN service customer role is a particularization of the Communication Service Customer (CSC) role.

Depending on actual scenarios and the type of NPN under consideration, i.e. standalone NPN or public network integrated NPN, different relationships can be found between NPN related roles and potential stakeholders. This means:

- each role can be played by one or more organizations simultaneously. For example, in PNI-NPN deployments the NPN operator role can be shared between a MNO and a vertical (or a private company acting on behalf of it). In the same way, in SNPN deployments the NPN operator role can be played by either a vertical (or a private company on behalf of it) or a MNO which manages the SNPN;

- an organization can play one or several roles simultaneously. For example, a company can play both NPN operator and NPN service provider roles.

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

## 4.2 Management of Stand-alone Non-Public Networks

An SNPN is deployed as an independent, isolated network. As shown in figure 4.2-1, all SNPN network functions are located inside the logical perimeter of the defined premises (e.g. factory) and the SNPN is separate from the public network. The SNPN operator has full management control over the exclusive SNPN network functions, e.g. the non-public 5G Core Network and/or 5G Access Network part of SNPN.

**SNPN**

Public Network Management

SNPN Management

**PLMN**

**Figure 4.2-1: SNPN deployment and SNPN management**

To manage a SNPN, which is based on 3GPP-defined technologies, 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 support two assignment models, see clause 5.30.2 of TS 23.501 [3]:

- Locally managed NIDs are assumed to be self-managed by SNPNs (i.e. chosen individually by SNPNs) at deployment time (and may therefore not be unique) but use a different numbering space than the universally managed NIDs as defined in TS 23.003 [5].

- Universally managed NIDs are assumed to be globally unique.

Additional considerations:

- With respect to the management of the NG-RAN segment of the SNPN:

- The following roles are involved:

- NPN Service Provider: played by the Vertical

- NPN Operator: played by the Vertical, for the NG-RAN segment

- NPN Service Customer: can be played by Vertical’s employees, Vertical’s applications, Vertical’s customers, etc.

- Virtualization Infrastructure Service Provider (VISP): played by a 3rd-party cloud service provider.

- The NG-RAN segment of the NPN is operated by the Vertical (see NOTE 1, NOTE 2, NOTE 3);

- The NG-RAN segment of the NPN is deployed in well-defined areas (e.g. within Vertical’s premises, factory, along railroad tracks, etc.) to meet the Vertical’s requirements. In case of virtualization of some NG-RAN network functions, the Vertical may rely on one or more VISPs (cf. TS 28.530 – clause 4.8) to host its virtualized NG-RAN network functions;

- Only the Vertical’s UEs are authorized to gain access to the NPN;

- The following variants may exist:

- Fully isolated SNPN (see [4] clause 5.2– Figure 1 with the optional connection not being deployed), or

- SNPN partly integrated with a PLMN (see [4] clause 5.2– Figure 1 with the optional connection being deployed from SNPN to PLMN only). In such a case, the management of the connection between the SNPN and the PLMN is shared between proponents.

- With respect to the management of the 5GC segment of the SNPN:

- The following roles are involved:

- NPN Service Provider: played by the Vertical

- NPN Operator: played by the Vertical, for the 5GC segment (see NOTE 1)

- NPN Service Customer: can be played by Vertical’s employees, Vertical’s applications, Vertical’s customers, etc.

- Virtualization Infrastructure Service Provider (VISP): played by a 3rd-party cloud service provider.

- The 5GC segment of the NPN is deployed in Vertical’s premises. Alternatively, in case of virtualization of some 5GC network functions, the Vertical may rely on one or more VISPs (cf. TS 28.530 – clause 4.8) to host its virtualized 5GC network functions, out of the Vertical’s premises;

- In the 5GC segment, the Vertical may utilize ‘Network Slice as NOP Internals’ model (cf. TS 28.530 – clause 4.1.7) to accommodate services to be provided to its own customers.

NOTE 1: Whether the Vertical outsources (part of) its network management tasks to other stakeholder(s) is out of scope of the present document.

NOTE 2: The focus is put here on who operates the NPN segments, not on who deploys them. Whether a NPN segment is deployed by the Vertical, or by a Network Operator or by anyone else on behalf of them, is out of scope of the present document

NOTE 3: How dedicated licensed spectrum is obtained by the Vertical to operate its NPN is out of the scope of the present document.

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

## 4.3 Management of Public Network Integrated NPN

### 4.3.1 NPN supported by network slice instance of a PLMN

A Public Network Integrated NPN (PNI-NPN) can be made available by PLMNs e.g. using one (or more) network slice instance(s). The existing network slicing functionalities apply as described in clause 5.15 of TS 23.501 [3].

A Closed Access Group identifies a group of subscribers who are permitted to access one or more CAG cells associated to the CAG. A CAG is identified by a CAG Identifier which is unique within the scope of a PLMN ID, see clause 5.30.3.2 of TS 23.501 [3]. The management system of the PNI-NPN takes charge of the management of CAG Identifiers.

From a management viewpoint, the provision of a network slice instance can follow the Network Slice as a Service (NSaaS) principles as described in clause 4.1.6 of TS 28.530 [7]. Figure 4.3.1-1, as an example, illustrates how a PLMN operator can rely on NSaaS capabilities (e.g. OAM, exposure) for the provisioning of a PNI-NPN to a vertical. This PNI-NPN, which is deployed across one PLMN and the vertical’s premises (e.g. factory), can be seen as an end-to-end network composed of two differentiated segments: one public, consisting of a (R)AN and network functions built upon public 5G network resources; and one private, consisting of network functions deployed using private 5G network resources. Using the NSaaS approach:

* The public segment is made available by the PLMN in the form of a network slice instance, and provisioned by the PLMN operator using NSaaS. In this service provisioning, the PLMN operator and the vertical play the roles of NSaaS provider and NSaaS customer, respectively.
* The PLMN operator can offer possibilities (e.g. exposed MnS to manage the network slice instance) for the vertical to manage the provided network slice instance according to TS 28.531 [6].
* The vertical adds the private segment to the network slice instance obtained from the PLMN operator. The resulting combination, i.e. PNI-NPN, is a new network slice instance. Following 3GPP 5G Network Resource Model (NRM) [10], the PNI-NPN’s public segment can be modelled as a network slice subnet.
* The vertical uses the PNI-NPN to provide non-public communication services to his customer(s). In this case, the vertical plays the role of NPN service provider, and his customer(s) play the role of NPN service customer(s). For more information on these NPN related roles, see clause 4.4.

A screenshot of a cell phone

Description automatically generated

**Figure 4.3.1-1: PNI-NPN provisioning with NSaaS**

Additional considerations:

- With respect to the management of the NG-RAN segment of the PNI-NPN:

- The Network Operator grants access to the Vertical to the whole Network Operator NG-RAN, or only to a part of it;

- Whatever the part of the NG-RAN of the Network Operator which access is granted to the Vertical, this part of the NPN is operated by the Network Operator;

- A roaming agreement or, alternatively, a RAN sharing agreement between the Vertical and the Network Operator may be required;

- One (or more) Closed Access Group(s) (CAG), identifying which Vertical’s UEs are permitted to access Network Operator NG-RAN cells may have to de defined. Since only the Network Operator has management access to the NG-RAN, the Vertical and the Network Operator may have to interact (Vertical requests the network Operator to add, delete, modify the list of Vertical’s UEs allowed to access the Network Operator cells);

- The same as above applies to CAG cells;

- There may be more than one Network Operator involved in this scenario (e.g. for coverage requirements)

- With respect to the management of the 5GC segment of the PNI-NPN:

- The 5GC segment of the NPN is operated by a Network Operator, whether the 5GC is i) wholly deployed in Vertical’s premises (see [4] clause 5.3.1 – Figure 2); or ii) partly in Vertical’s premises (e.g. UPFs) and partly in the Network Operator’s domain (e.g. 5GC control plane network functions); or iii) wholly in the Network Operator’s domain;

- In the 5GC segment, the Network Operator may utilize ‘Network Slice as a Service’ model (cf. TS 28.530 – clause 4.1.7) and/or ‘Network Slice as NOP internals’ model (cf. TS 28.530 – clause 4.1.7).

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

## 4.4 Roles related to non-public networks management

See clause 4.1a.

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