ETSI TS 128 557 V17.1.0 (2023-04)

5G;
Management and orchestration;
Management of Non-Public Networks (NPN);
Stage 1 and stage 2
(3GPP TS 28.557 version 17.1.0 Release 17)

Reference
RTS/TSGS-0528557vh10

Keywords
5G

ETSI

650 Route des Lucioles
F-06921 Sophia Antipolis Cedex - FRANCE

Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Siret N° 348 623 562 00017 - APE 7112B
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° w061004871

Intellectual Property Rights

Essential patents

IPRs essential or potentially essential to normative deliverables may have been declared to ETSI. The declarations pertaining to these essential IPRs, if any, are publicly available for **ETSI members and non-members**, and can be found in ETSI SR 000 314: *"Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards"*, which is available from the ETSI Secretariat. Latest updates are available on the ETSI Web server (https://ipr.etsi.org/).

Pursuant to the ETSI Directives including the ETSI IPR Policy, no investigation regarding the essentiality of IPRs, including IPR searches, has been carried out by ETSI. No guarantee can be given as to the existence of other IPRs not referenced in ETSI SR 000 314 (or the updates on the ETSI Web server) which are, or may be, or may become, essential to the present document.

Trademarks

The present document may include trademarks and/or tradenames which are asserted and/or registered by their owners. ETSI claims no ownership of these except for any which are indicated as being the property of ETSI, and conveys no right to use or reproduce any trademark and/or tradename. Mention of those trademarks in the present document does not constitute an endorsement by ETSI of products, services or organizations associated with those trademarks.

DECT™, **PLUGTESTS™**, **UMTS™** and the ETSI logo are trademarks of ETSI registered for the benefit of its Members. **3GPP™** and **LTE™** are trademarks of ETSI registered for the benefit of its Members and of the 3GPP Organizational Partners. **oneM2M™** logo is a trademark of ETSI registered for the benefit of its Members and of the oneM2M Partners. **GSM**® and the GSM logo are trademarks registered and owned by the GSM Association.

Legal Notice

This Technical Specification (TS) has been produced by ETSI 3rd Generation Partnership Project (3GPP).

The present document may refer to technical specifications or reports using their 3GPP identities. These shall be interpreted as being references to the corresponding ETSI deliverables.

The cross reference between 3GPP and ETSI identities can be found under https://webapp.etsi.org/key/queryform.asp.

Modal verbs terminology

In the present document "**shall**", "**shall not**", "**should**", "**should not**", "**may**", "**need not**", "**will**", "**will not**", "**can**" and "**cannot**" are to be interpreted as described in clause 3.2 of the ETSI Drafting Rules (Verbal forms for the expression of provisions).

"**must**" and "**must not**" are **NOT** allowed in ETSI deliverables except when used in direct citation.

Contents

Foreword

This Technical Specification has been produced by the 3rd Generation Partnership Project (3GPP).

The contents of the present document are subject to continuing work within the TSG and may change following formal TSG approval. Should the TSG modify the contents of the present document, it will be re-released by the TSG with an identifying change of release date and an increase in version number as follows:

Version x.y.z

where:

- x the first digit:
  - 1 presented to TSG for information;
  - 2 presented to TSG for approval;
  - 3 or greater indicates TSG approved document under change control.
- y the second digit is incremented for all changes of substance, i.e. technical enhancements, corrections, updates, etc.
- z the third digit is incremented when editorial only changes have been incorporated in the document.

In the present document, modal verbs have the following meanings:

shall indicates a mandatory requirement to do something

shall not indicates an interdiction (prohibition) to do something

The constructions "shall" and "shall not" are confined to the context of normative provisions, and do not appear in Technical Reports.

The constructions "must" and "must not" are not used as substitutes for "shall" and "shall not". Their use is avoided insofar as possible, and they are not used in a normative context except in a direct citation from an external, referenced, non-3GPP document, or so as to maintain continuity of style when extending or modifying the provisions of such a referenced document.

should indicates a recommendation to do something

should not indicates a recommendation not to do something

may indicates permission to do something

need not indicates permission not to do something

The construction "may not" is ambiguous and is not used in normative elements. The unambiguous constructions "might not" or "shall not" are used instead, depending upon the meaning intended.

can indicates that something is possible

cannot indicates that something is impossible

The constructions "can" and "cannot" are not substitutes for "may" and "need not".

will indicates that something is certain or expected to happen as a result of action taken by an agency the behaviour of which is outside the scope of the present document

will not indicates that something is certain or expected not to happen as a result of action taken by an agency the behaviour of which is outside the scope of the present document

might indicates a likelihood that something will happen as a result of action taken by some agency the behaviour of which is outside the scope of the present document

might not indicates a likelihood that something will not happen as a result of action taken by some agency the behaviour of which is outside the scope of the present document

In addition:

is (or any other verb in the indicative mood) indicates a statement of fact

is not (or any other negative verb in the indicative mood) indicates a statement of fact

The constructions "is" and "is not" do not indicate requirements.

Introduction

A non-public network is a network that is intended for non-public use. Deployments of non-public networks in private environments (e.g. factories, enterprises) to provide coverage within a specific geographic area for non-public use is a key demand of emerging 5G applications and verticals. An NPN can be deployed as SNPN or as PNI-NPN.

1 Scope

The present document specifies concepts, use cases, requirements and solutions for management of non-public networks.

2 References

The following documents contain provisions which, through reference in this text, constitute provisions of the present document.

- References are either specific (identified by date of publication, edition number, version number, etc.) or non-specific.
- For a specific reference, subsequent revisions do not apply.
- For a non-specific reference, the latest version applies. In the case of a reference to a 3GPP document (including a GSM document), a non-specific reference implicitly refers to the latest version of that document *in the same Release as the present document*.

[1] 3GPP TR 21.905: "Vocabulary for 3GPP Specifications".

[2] 3GPP TS 28.530: "Management and orchestration; Concepts, use cases and requirements".

[3] 3GPP TS 23.501: "System architecture for the 5G System (5GS)".

[4] 3GPP TS 22.261: "Service requirements for the 5G system".

[5] 5G-ACIA White paper: "5G Non-Public Networks for Industrial Scenarios", July 31, 2019.

[6] 3GPP TS 23.003: "Numbering, addressing and identification".

[7] 3GPP TS 28.541: "Management and orchestration; 5G Network Resource Model (NRM); Stage 2 and stage 3".

[8] 3GPP TS 28.531: "Management and orchestration; Provisioning".

[9] 3GPP TS 38.413: "NG-RAN; NG Application Protocol (NGAP)".

[10] 3GPP TS 38.473: "NG-RAN; F1 Application Protocol (F1AP)".

[11] 3GPP TS 38.331: "NR; Radio Resource Control (RRC); Protocol specification".

[12] 3GPP TS 28.552: "Management and orchestration; 5G performance measurements".

[13] 3GPP TS 28.554: "Management and orchestration; 5G end to end Key Performance Indicators (KPI)".

[14] 3GPP TS 28.532: "Management and orchestration; Generic management services".

[15] 3GPP TS 28.622: "Telecommunication management; Generic Network Resource Model (NRM); Integration Reference Point (IRP); Information Service (IS)".

[16] 3GPP TS 32.422: "Telecommunication management; Subscriber and equipment trace; Trace control and configuration management".

[17] 3GPP TS 28.537: "Management and orchestration; Management capabilities".

3 Definitions of terms, symbols and abbreviations

3.1 Terms

For the purposes of the present document, the terms given in TR 21.905 [1] and the following apply. A term defined in the present document takes precedence over the definition of the same term, if any, in TR 21.905 [1].

Non-Public Network: See definition in TS 22.261 [4].

Public network integrated NPN: See definition in TS 23.501 [3].

Stand-alone Non-Public Network: See definition in TS 23.501 [3].

3.2 Symbols

Void.

3.3 Abbreviations

For the purposes of the present document, the abbreviations given in 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 TR 21.905 [1].

CSC	Communication Service Customer
CSP	Communication Service Provider
MNO	Mobile Network Operator
NPN	Non-Public Network
PNI-NPN	Public Network Integrated NPN
SNPN	Stand-alone NPN

4 Concepts and overview

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.

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 (PNI-NPN), i.e. a non-public network deployed with the support of a PLMN.

4.2 Roles related to NPN management

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

In clause 4.8 of TS 28.530 [2], the roles related to 5G networks and network slicing management are presented. An NPN represents a 5G network with a delimited scope in its use (i.e. non-public use). This means that NPN management can be built upon the roles related to 5G networks management, as long as the scope of these roles is limited to acting on network and services for non-public use.

According to the above rationale, the roles related to NPN management include:

- NPN Service Customer (NPN-SC): a Communication Service Customer (CSC) which consumes communication services for non-public use, i.e. communication services offered over NPNs. An NPN-SC is the realization of the CSC role (see definition in TS 28.530 [2], clause 4.8) in NPN environments.

- NPN Service Provider (NPN-SP): a Communication Service Provider (CSP) which provides communication services for non-public use, i.e. communication services offered over NPNs. An NPN-SP is the realization of the CSP role (see definition in TS 28.530 [2], clause 4.8) in NPN environments.

- NPN Operator (NPN-OP): a Network Operator (NOP) whose management scope is limited to 5G networks for non-public use, i.e. NPNs. An NPN operator is the realization of the NOP role (see definition in TS 28.530 [2], clause 4.8) in NPN environments.

- Network Equipment Provider (NEP), including VNF supplier: see definition in TS 28.530 [2], clause 4.8.

- Virtualization Infrastructure Service Provider (VISP): see definition in TS 28.530 [2], clause 4.8.

- Data Centre Service Provider (DCSP): see definition in TS 28.530 [2], clause 4.8.

- NFVI Supplier: see definition in TS 28.530 [2], clause 4.8.

- Hardware Supplier: see definition in TS 28.530 [2], clause 4.8.

Note that NEP, VISP, DCSP, NFVI supplier and Hardware Supplier roles are the same as defined for 5G networks and network slicing management. This is because their managed/provided assets are unaware of the public or non-public nature of 5G network and services running atop.

Depending on actual scenarios and the type of NPNs under consideration, i.e. SNPN or PNI-NPN, different relationships can be found between NPN management roles and potential stakeholders, see annex A Deployment considerations on NPN management modes.

4.3 NPN management aspects

4.3.1 Drivers

Vertical industries have a very wide range of use cases with very diverse requirements comparing with management of traditional PLMN. Management of NPN has the following specific aspects:

- Assurance for diversified SLA requirements: The diversified SLA requirements from different kinds of vertical industries need to be guaranteed, e.g. manufacturing industry and medical care need ultra-reliable low-latency wireless connectivity and indoor, outdoor or hybrid coverage NPN deployments. Other than performance requirements (e.g. ultra-low latency, ultra-high reliability), functional and operational requirements should also be guaranteed in SLA, e.g. high-precision positioning, real-time monitoring, etc.

- Support of different O&M models: an O&M model allows specifying who is responsible for managing what part of the network. The various NPN scenarios, with a number of vertical use cases and a plenty of deployment variants, in some cases may lead to the definition of different O&M models. For example, many Small and Medium-sized Enterprises (SMEs) do not have sufficient technical expertise for their NPNs' deployment and operation. Therefore, cooperation with PLMN Operators to obtain O&M of NPNs from PLMN Operators might be the most cost-effective way for such customers. On the other hand, large enterprises like electric utility companies might want to have their own O&M for their NPNs to fulfil specific requirements.

- Management capability exposure: this expresses the ability of an NPN-SP to expose some management capabilities, such as performance and KPIs monitoring, fault supervision and provisioning management capabilities, to the corresponding NPN-SC. The NPN-SP makes the selected NPN management capabilities available through well-defined APIs to allow the NPN-SC to consume these capabilities, as well as extending them with their own operation and maintenance systems, if needed. NPN-SC may provide their business objectives by intents and policies management to NPN-SP and no need to focus on detailed configuration parameters of NPNs. The mobile management capabilities exposed to the enterprise are as follows.

- Management capability of configuration: The vertical may request to mobile network operator for a limited management capability which would enable the enterprise to dynamically change the configuration parameters (e.g. CAG configuration).

- Management capability of performance assurance: The performance assurance capabilities that may be provided to the enterprise may include creation of certain measurement jobs which collects the value of one or multiple measurement types which are the performance measurements and assurance data defined in TS 28.552 [12] or collects the value of one or multiple KPIs defined in TS 28.554 [13].

- Management capability of fault supervision: The fault supervision capabilities that may be provided to the enterprise may include get NSI/NSSI/NF alarm data and control NSI/NSSI/NF alarm data.

4.3.2 Management modes

4.3.2.1 General

Different management modes of NPN are listed in table 4.3-1.

4.3.2.2 PNI-NPN

- **MNO Managed Mode**: The NPN operator role is entirely played by a mobile network operator, which also plays the Network Operator (NOP) role (see definition in TS 28.530 [2], clause 4.8) for PLMN. In this case, no specific spectrum resources are required and service continuity (e.g. roaming) with PLMN is ensured by the mobile network operator who manages both PNI-NPN and PLMN.

- **MNO-Vertical Managed Mode**: The NPN operator role is played by two parties: a mobile network operator, which also plays the NOP role for PLMN, and a vertical customer. The mobile network operator performs the main management tasks related to the PNI-NPN, while allowing the vertical to retain some control over this PNI-NPN. To that end, the vertical consumes the management capabilities exposed by the mobile network operator, being this exposure regulated according to the business agreement between the two parties. The mobile network operator shall restrict the types (e.g. provisioning, fault supervision, performance assurance) of management capabilities and corresponding managed network resource (e.g. NRM fragments) exposed to a vertical. In this case, no specific spectrum resources are required and service continuity (e.g. roaming) with PLMN is ensured by the mobile network operator who manages both PNI-NPN and PLMN. The vertical can also outsource its PNI-NPN management tasks to other third party OAM service provider.

4.3.2.3 SNPN

- **MNO Managed Mode:** The NPN operator role is entirely played by a mobile network operator, which also plays the NOP role for PLMN In this case, specific spectrum resources (e.g. unlicensed spectrums) are required, and cooperation with PLMN Operator may be needed if there is requested NPN connectivity to external PLMN resources (e.g. to allow UEs registered into the SNPN to access public network services).

- **MNO-Vertical Managed Mode:** The NPN operator role is played by two parties: a mobile network operator, which also plays the NOP role for PLMN, and a vertical customer. The mobile network operator performs the main management tasks related to the SNPN, while allowing the vertical to retain some control over this SNPN. To that end, the vertical consumes the management capabilities exposed by the mobile network operator, being this exposure regulated according to the business agreement between the two parties. The mobile network operator shall restrict the types (e.g. provisioning, fault supervision, performance assurance) of management capabilities and corresponding managed network resource (e.g. NRM fragments) exposed to a vertical. In this case, specific spectrum resources (e.g. unlicensed spectrums) are required, and cooperation with PLMN Operator may be needed if there is requested NPN connectivity to external PLMN resources (e.g. to allow UEs registered into the SNPN to access public network services). The management tasks for the SNPN are performed mainly by the mobile network operator and the vertical with some management capabilities. The vertical can also outsource its SNPN management tasks to other third party OAM service provider.

- **Vertical Managed Mode:** The NPN operator role is entirely played by a vertical. In this case, specific spectrum resources (e.g. unlicensed spectrums) are required, and cooperation with PLMN Operator may be needed if there is requested NPN connectivity to external PLMN resources (e.g. to allow UEs registered into the SNPN to access public network services). The vertical can also outsource its SNPN management tasks to other third party OAM service provider.

Table 4.3-1: Different management modes of NPN

Management mode	NPN type	Management of NPN	NPN Operator	Use case
MNO Managed Mode	PNI-NPN	An NPN is fully managed by a mobile network operator which also manages PLMN.	Mobile network operator	5.1.2
MNO-Vertical Managed Mode	PNI-NPN	An NPN is managed by a mobile network operator which also manages PLMN and a vertical who gets some management capabilities exposed from the mobile network operator according to business agreement between the two parties.	Mobile network operator and vertical (Note 1) (Note 2)	5.1.2
MNO Managed Mode	SNPN	An NPN is fully managed by a mobile network operator.	Mobile network operator	5.1.1.1
MNO-Vertical Managed Mode	SNPN	An NPN is managed by a mobile network operator and a vertical who gets some management capabilities exposed from the mobile network operator according to business agreement between the two parties.	Mobile network operator and vertical (Note 1) (Note 2)	5.1.1.1
Vertical Managed Mode	SNPN	An NPN is fully managed by a vertical.	Vertical (Note 1)	5.1.1.1
NOTE 1: The vertical can outsource its NPN management tasks to other third party OAM service provider to manage the NPN based on the management capabilities exposed from the mobile network operator. NOTE 2: The mobile network operator shall restrict the exposure of management capabilities and corresponding managed resources to vertical.				

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 an 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.

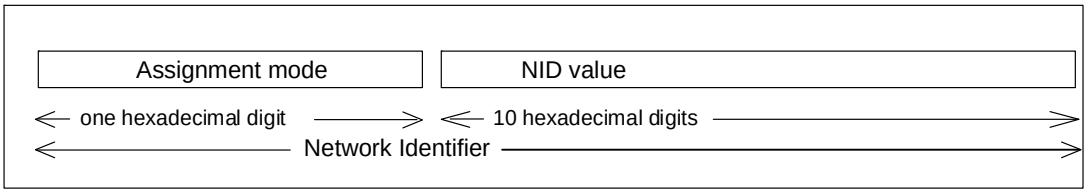

Figure 4.4-1: Network Identifier (NID)

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.

4.5 Management of PNI-NPNs

A PNI-NPN is an 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) [3], 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 should 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).

4.6 Impact of NPNs on 5G system management

4.6.1 UE related management aspects

4.6.1.1 Collecting UE related data and providing to authorized NPN service customer

UEs under service of NPN may have various forms, such as phones or PCs or IoT terminals, some of them are assets of the NPN service customer. UE related data including UE locations, measurements, etc. is required by the NPN service customer to help their own business in some cases. Such UE related data is easier or more cost-efficient to be acquired by NPN UEs compared with being acquired by other methods e.g. by add-on devices or applications. For example, healthcare industry NPN customers require location information of their NPN UEs applied in mobile medical machines for asset management; enterprise NPN customers require location information of the NPN UEs of their employees for attendance management.

In this case, 3GPP management system may need to collect UE related data and provide them to authorized NPN service customer. Such collected UE related data are generated by management services which are defined and implemented in 3GPP system, such as:

- MDT data, including immediate MDT, logged MDT, RLF reports, accessibility measurements.
- Trace data, to track traffic process of UEs and locate possible causes of traffic problems for example.

Furthermore, according to pre-defined agreements among the NPN stakeholders, some specific UE related data can be provided to authorized NPN customer, e.g. to promote their positioning ability or evaluate QoE. Such data may be processed or masked based on collected data such as MDT or trace. For example, GNSS information can be extracted from MDT data to locate assets in NPN.

4.6.1.2 5G VN group management

A 5G Virtual Network (VN) group is a set of UEs using private communication for 5G LAN-type service [3]. The definition of 5G VN groups is required by the NPN-SC to help their own business in some cases. For example, an NPN-SC might request that certain UEs be members of one or more 5G VN groups.

Based on the above rationale, 3GPP management system may need to allow for the 5G VN group management support in NPNs, following up the needs of the NPN-SC. This includes:

- Creation, modification and removal of 5G VN groups, including definition of group communication services and other attributes (e.g. the service area).
- Addition/removal of individual UEs to/from a 5G VN group.
- Notification of 5G VN group related information (e.g. status, events), following up NPN-SC subscription preferences.

4.6.2 NG-RAN related management aspects

An NG-RAN node can serve multiple NPNs, including SNPNs and PNI-NPNs. To that end, the NPN-OP shall configure the NG-RAN node accordingly, using 3GPP management system.

For NG-RAN non-split deployments, the gNB needs to be configured (via 3GPP management system) with lists of NID(s) and CAG(s) it supports, for SNPN and PNI-NPN, respectively. In the NG Application Protocol (NGAP), this information is used as follows.

- The gNB communicates supported NID(s) to AMF in the following NGAP messages: NG SETUP REQUEST (see clause 9.2.6.1 of TS 38.413 [9]) and RAN CONFIGURATION UPDATE (see clause 9.2.6.4 of TS 38.413 [9]).
- The gNB does not communicate supported CAG(s) to the AMF; instead, it keeps this cell-level information internally. The gNB uses information on supported CAG(s) to accept/reject handover requests from AMF in the following NGAP message: HANDOVER REQUEST (see clause 9.2.3.4 of TS 38.413 [9])

For NG-RAN split deployments, individual gNB-DU needs to be configured (via 3GPP management system) with lists of NID(s) and CAG(s) it supports, for SNPN and PNI-NPN, respectively. In the F1 Application Protocol (F1AP), this information is used as follows:

- Each gNB-DU communicates supported NID(s) to the gNB-CU in the following F1AP messages: F1 SETUP REQUEST (see clause 9.2.1.4 of TS 38.473 [10]) and gNB-DU CONFIGURATION UPDATE (see clause 9.2.1.7 of TS 38.473 [10]). With this information, the gNB-CU knows NPN support information about the cells configured in this gNB-DU.
- Upon receiving the above information from individual gNB-DUs, the gNB-CU knows which NID(s) are available for use. The reason is that not all distributed gNB-DUs under the same gNB-CU may necessarily support the same NIDs.
- Based on this information, the gNB-CU can decide on which specific cells need to be activated on individual gNB-DUs. The gNB-CU communicates this information in the following F1AP messages: F1 SETUP RESPONSE (see clause 9.2.1.5 of TS 38.473 [10]) and gNB-DU CONFIGURATION ACKNOWLEDGE (see clause 9.2.1.8 of TS 38.473 [10]).
- gNB-DUs do not communicate supported CAG(s) to the gNB-CU; instead, they keep this cell-level information internally.

There could be scenarios where the NG-RAN node supporting NPNs is shared using 5G MOCN. In all these NPN sharing scenarios, each Cell Identity as specified in TS 38.331 [11] is associated with one of the following configuration options:

- one or multiple SNPNs;
- one or multiple PNI-NPNs (with CAG);
- one or multiple PLMNs only.

For more details on these configuration options, see clause 5.18 of TS 23.501 [3].

4.6.3 5GC related management aspects

As described in clause 5.30.3.1 of TS 23.501[3], the architecture of 5G Core is capable to support SNPN and PNI-NPN.

For SNPN, the architecture depicted in clause 4.2.3 of TS 23.501 [3] is extended with the additional features as described in clause 5.30.2 of TS 23.501 [3].

The 5GC NRM shall support the network resource model for SNPN:

- N3IWF and service access point of Untrusted Non-3GPP access for UE to access PLMN services via SNPN.

3GPP management system shall support configuration of 5GC NFs (e.g., AMF, SMF, UPF etc.) as network nodes in SNPN. The NID shall be configured to 5GC NFs when 5GC NFs are part of SNPN, in case of both self-assignment and coordinated assignment.

For PNI-NPN, there are no further specific 5GC related management aspects apart from those captured in clause 4.5.

5 Specification level requirements

5.1 Use cases

5.1.0 Generic use cases

5.1.0.1 Collecting UE related data

In some NPN scenarios, the NPN-SC may need to deploy a new vertical service or supervise NPN service SLA based on the UE related data (e.g. UE measurement, etc). In this situation, the 3GPP management system may collect UE related data and provide them to authorized NPN-SC. To obtain the UE related data, the NPN-SC may consume the corresponding capability exposed by the NPN-SP.

5.1.1 Use cases related to SNPN management

5.1.1.1 Create a SNPN

This use case describes a scenario where an NPN-SP decides to provision an NPN for use by an NPN-SC in the form of SNPN. It is either an MNO or an enterprise can be playing a role of NPN-SP, and it is an enterprise (the different or same if the enterprise is also NPN-SP) be playing a role of NPN-SC. This SNPN consists of network resources decoupled from PLMN resources, including:

- RAN NE(s)
- 5GC network functions
- Transport network

In this scenario, the NPN-SC sends to the NPN-SP a request for the provision of an NPN. This request contains the NPN related SLS requirements. To fulfil the SLS of requested NPN, the NPN-SP decides to create a new SNPN.

The NPN-SP maps SLS of requested NPN into 3GPP 5G system related requirements. These requirements allow the NPN operator to decide on the constituent network resources and the topology of the 3GPP 5G network to be created for the SNPN, as follows:

- For the AN and CN related parts, the NPN operator takes all the actions needed to set up and configure required network resources, including RAN NE(s) and 5GC network functions. For more details, refer to TS 28.531 [8], clauses 5.1.17 "Creation of 3GPP NF" and 5.1.18 "Configuration of a 3GPP NF instance". Some of these actions can require setting up a new 3GPP sub-network. For more details, refer to TS 28.531 [8], clause 5.1.19 "Creation of a 3GPP sub-network".

- For the TN related part, the NPN operator takes all the actions needed to set up the required connectivity along the RAN and CN, configuring the underlying transport network. When taking these actions, information on SNPN topology (e.g. external connection points of AN and CN) and performance (e.g. latency, bandwidth) should be considered.

If the requested NPN requires connectivity to external PLMN resources (e.g. to allow UEs registered into the SNPN to access public network services), the NPN-SP derives the requirements for such a connectivity. These requirements allow the NPN operator to configure the transport network connecting the SNPN and the PLMN accordingly.

NOTE 1: To allow UEs to access public network services from the SNPN, the UEs also have to be registered in the PLMN UDM.

NOTE 2: For the derivation of connectivity requirements between SNPN and the PLMN, the NPN-SP makes use of two sources of information:

1) the SLS of requested NPN, received from the NPN-SC; and

2) connectivity information of the created 3GPP 5G network, received from the NPN operator.

In this use case, depending on different situations, the NPN operator role can be played by:

- the mobile network operator only. In such MNO Managed Mode case, the mobile network operator takes the entire responsibility of operating the SNPN and managing SNPN-PLMN connectivity, if required; or

- the mobile network operator and the enterprise. In such MNO-Vertical Mode case, the mobile network operator can expose some management capabilities to the enterprise, according to business agreement between the two parties. SNPN-PLMN connectivity, if required, is always managed by the mobile network operator; or

- the vertical only. In such Vertical Managed Mode case, the enterprise takes the entire responsibility of operating the SNPN. The SNPN-PLMN connectivity, if required, is always managed by the mobile network operator who takes the entire responsibility of operating the PLMN.

In this use case depending on the different NID assignment models as described in clause 4.4, the NPN operator role can configure the NID to related AN nodes and 5GC NFs. The management of NID is described in clause 4.4 in the present document.

5.1.2 PNI-NPN provisioning by network slice (NSaaS) of PLMN

A mobile network operator (playing the role of NPN-SP) decides to provision a PNI-NPN for use by an enterprise (playing the role of NPN-SC) in the form of a network slice of a PLMN. This network slice may include PLMN network functions / network function services for non-public use. Depending on NPN-SC, the slice can span one or more network domains, e.g.:

- Network slice corresponding to a RAN-only network slice subnet.

- Network slice corresponding to CN-only network slice subnet.

- Network slice corresponding to a network slice subnet composed of RAN slice subnet + Transport network slice subnet + CN slice subnet.

In this scenario, the NPN-SC provides the NPN related SLA requirements to the NPN-SP. These requirements specify NPN related SLS (i.e. NPN desired performance and required functionality) together with other business related information (i.e. NPN lifetime, NPN slice charging / accounting, etc.). To fulfil the SLS of requested NPN, the NPN-SP decides to use network slicing.

The NPN-SP maps SLS of requested PNI-NPN into ServiceProfile attributes. For details on these attributes, see TS 28.541 [7]. Based on these attributes, the NPN-SP determines to reuse an existing network slice or create a new network slice for the PNI-NPN. If an existing network slice can be reused, the operator may reconfigure the existing network slice.

In this use case, the NPN operator role is played by:

- The mobile network operator only. In such MNO Managed Mode case, the mobile network operator takes the entire responsibility of operating the network slice of the PLMN.
- The mobile network operator and the enterprise. In such MNO-Vertical Managed Mode, according to business agreement between both parties, the mobile network operator can expose some management capabilities to the enterprise.

NOTE: The scope of the NPN operator in this use case does not include the management of enterprise owned 5G network resources (i.e. on-premise physical equipment and on-premise NFVI).

5.2 Requirements

5.2.1 Generic requirements for management of NPN

REQ-NPN-FUN-01 The 3GPP management system shall have the capability to monitor the performance measurements and KPIs associated with an NPN.

REQ-NPN-FUN-02 The 3GPP management system shall have the capability to provide the performance measurements and KPIs associated with an NPN to authorized entity, either NPN-SC (when NPN-SP and NPN-OP are both played by the same actor) or NPN-SP (when NPN-SP and NPN-OP are played by different actors).

REQ-NPN-FUN-03 The 3GPP management system shall have the capability to receive SLA requirements from authorized NPN-SC and then translating the SLA requirements into service and network resources related requirements.

REQ-NPN-FUN-04 The 3GPP management system shall have the capability to evaluate SLS assurance related to an NPN.

REQ-NPN-FUN-05 The 3GPP management system shall have the capability to restrict the exposure of management capabilities and corresponding managed resources to NPN-SC.

REQ-NPN-FUN-06 The 3GPP management system shall have the capability to support management capabilities exposure, which includes management capabilities of network provisioning, fault supervision and performance assurance to the authorized NPN-SC.

REQ-NPN-FUN-07 The 3GPP management system shall have the capability to provision both physical and virtual NPNs.

REQ-NPN-FUN-08 The 3GPP management system shall have the capability to provision different NPNs intended to different NPN-SCs.

REQ-NPN-FUN-09 The 3GPP management system shall have the capability to provision an NPN which serves different NPN-SCs.

REQ-NPN-FUN-10 The 3GPP management system shall offer the NPN-SC the ability to manage its own NPN(s) and its private slice(s) in the PLMN in a combined manner.

5.2.2 Requirements for management of SNPN

REQ-SNPN-FUN-01 The 3GPP management system shall have the capability to support standalone operation of an SNPN.

REQ-SNPN-FUN-02 The 3GPP management system shall have the capability to support management of dedicated NPN identifier (i.e. combination of a PLMN ID and a Network Identifier (NID) which is used to identify an SNPN.

REQ-SNPN-FUN-03 The 3GPP management system shall have the capability to configure NID which consists of an assignment mode and an NID value.

REQ-SNPN-FUN-04 The 3GPP management system shall have the capability to configure an NR cell for the support of SNPN, by configuring a gNB (gNB-DU in NG-RAN split deployment scenarios) with a list of served NIDs per PLMN Identity.

REQ-SNPN-FUN-05 The 3GPP management system shall have the capability to interwork with one or more non-3GPP management systems to support the operation of a SNPN which includes 3GPP and non-3GPP segments.

5.2.3 Requirements for management of PNI-NPN

REQ-PNIN-FUN-01 The 3GPP management system shall have the capability to collect NPN UE related data which may include MDT data and trace data.

REQ-PNIN-FUN-02 The 3GPP management system shall have the capability to provide NPN UE related data to authorized NPN-SC according to pre-defined agreements.

REQ-PNIN-FUN-03 The 3GPP management system should have the capability to support assignment and maintenance of CAG ID which identifies the CAG cells.

REQ-PNIN-FUN-04 The 3GPP management system shall have the capability to configure a NR cell to support PNI-NPN, by configuring a gNB (gNB-DU in NG-RAN split deployment scenarios) with a list of serving CAGs per PLMN Identity.

REQ-PNIN-FUN-05 The 3GPP management system should have the capability to manage the list of UEs that are allowed on the corresponding CAG.

REQ-PNIN-FUN-06 The 3GPP management system should have the capability to configure access policy of CAG cells.

NOTE: The access policy of CAG cells includes such as allowed days/time slots for NPN UEs that are allowed on the corresponding CAG cells.

REQ-PNIN-FUN-07 The 3GPP management system shall have the capability to provision a PNI-NPN by means of dedicated DNN, or by one (or more) network slice instance(s). For the latter, the network slice instance is made available for the NPN-SC by means of Network Slice as a Service (NSaaS) model (see clause 4.1.6 from TS 28.530 [2]).

6 Solutions

6.1 Generic solutions for management of NPN

6.1.1 Solution for collecting UE related data

The NPN-SP/OP follows the mechanisms used for the control and configuration of the Trace and MDT as described in TS 32.422 [16], including:

- the MDT/trace activation procedures in clause 4.1 of TS 32.422 [16] for MDT/trace configuration, and,
- the MDT/trace reporting procedures in clause 4.6 and 4.7 of TS 32.422 [16] for UE related data reporting.

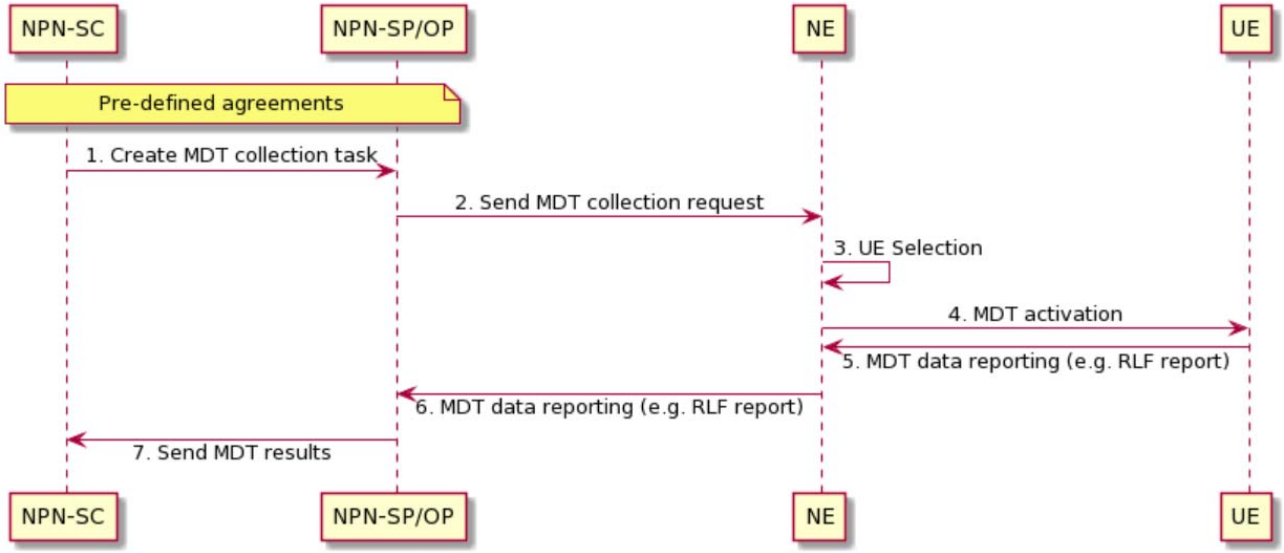

Figure 6.1.1-1: Procedures of UE related data collection

Figure 6.1.1-1 shows the procedure of UE related data collection.

It is assumed that the NPN-SP and NPN-OP roles are played by the same actor in figure 6.1.1-1. The work flow between NPN-SP and NPN-SC for the pre-defined agreements is out of scope of the present document.

1) Based on the pre-defined agreements, NPN-SC sends "Create MDT collection task" request to NPN-SP/OP.

2) The NPN-SP/OP sends a Trace Session activation request to the NE. This request includes the parameters for configuring MDT data collection such as area, job type and list of measurements.

3) After receiving the MDT collection request, NE performs the UE selection based on the input information derived from NPN-SP/OP, such as device capability information and area scope.

4) NE shall activate the MDT functionality and send configuration information to the selected UEs (see clause 4.1 of clause of TS 32.422 [16]).

5) When UE receives the MDT activation, it shall start the MDT functionality based on the received configuration parameters. The MDT related measurements are then reported to NE.

6) Then NE reports the related data to NPN-SP/OP (see clauses 4.6 and 4.7 of TS 32.422 [16]).

7) According to pre-defined agreements among the NPN roles, some specific UE related data can be provided to authorized NPN customer (see clause 7.2 of TS 28.537 [17]) such data may be processed or masked based on collected data such as MDT or trace. For example, GNSS information can be extracted from MDT to locate assets in NPN.

6.2 Solutions for management of SNPN

6.2.1 Solution for SNPN provisioning with 3GPP segments only

An SNPN, which includes 3GPP segment only, may need to be created for use of an NPN-SC. It is illustrated as provisioning a SNPN in figure 6.2.1-1 which can be used for create SNPN in the MNO Managed Mode and Vertical Managed Mode (see clause 4.3.2).

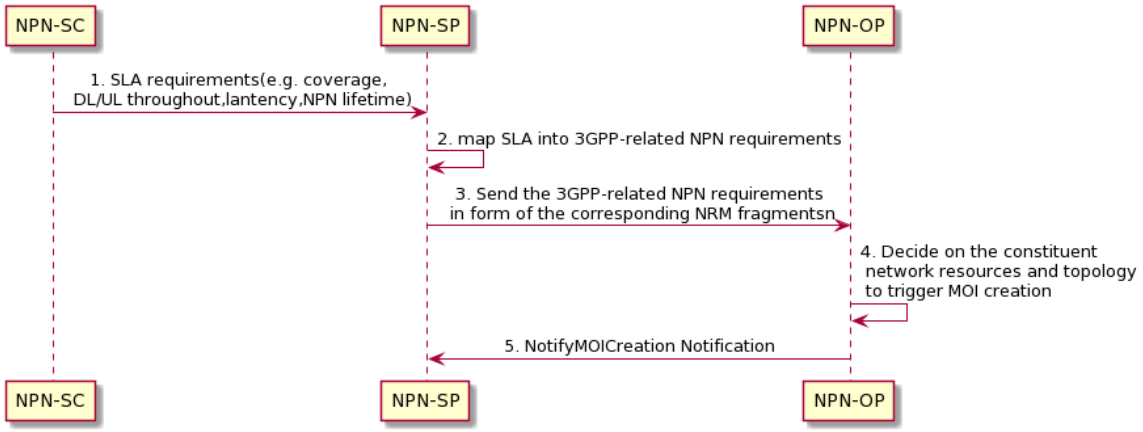

Figure 6.2.1-1: Procedure of SNPN provisioning with 3GPP segments only

1) NPN-SP receives SLA requirements of the requested SNPN from NPN-SC. The SLA requirements specifies NPN related SLA according to different vertical industry requirements (e.g. coverage requirement within a specific geographic area, downlink/uplink throughput requirements, latency requirement, etc.) together with other business related information (e.g. NPN lifetime, etc.). The work flow between NPN-SP and NPN-SC is out of scope of present specification.

2) Based on the requirements from NPN-SC, NPN-SP maps SLS into 3GPP-related NPN requirements including RAN/CN/TN part-related requirements.

3) The NPN-SP sends the 3GPP-related NPN requirements in form of NRM fragments (e.g. `ServiceProfile <dataType>`) to NPN-OP.

4) The NPN-OP determines the constituent network resources and topology needed for the SNPN creation. The related Managed Object instance (reference to related information models for NR, 5GC in TS 28.541 [7] and generic NRM in TS 28.622 [15], e.g., `GNBCUCPFunction` IOC, `GNBDUFunction` IOC, `GNBCUUPFunction` IOC, `SubNetwork` IOC, `Top` IOC and etc.) would be created for the requested SNPN using the operations (e.g. createMOI operations) of generic provisioning MnS in TS 28.532 [14].

   The NPN-OP determines to reuse an existing 3GPP segment or create a new 3GPP segment for the requested NPN. If a 3GPP segment from an existing stand-alone NPN can be reused, the NPN-OP may reconfigure that SNPN:

   a) In case of creating a new 3GPP segment for the SNPN:

      - Based on RAN part-related requirements, the 3GPP network management system determines to utilize new RAN NE(s).

      - Based on CN part-related requirements, the 3GPP network management system determines to utilize new CN NF(s) or CN NF service(s).

      - Based on TN part-related requirements, the NPN operator configures the underlying transport network, considering the information on SNPN topology (e.g. external connection points of AN and CN) and performance (e.g. latency, bandwidth).

5) The NPN-OP notifies the created 3GPP segment information (e.g. the DN of created MOI) to the NPN-SP which subscribes the provisioning notification by re-using the notifications (e.g. NotifyMOICreation notifications) of generic provisioning MnS in TS 28.532 [14].

6.3 Solutions for management of PNI-NPN

6.3.1 Solution for NPN provisioning by a network slice of a PLMN

A mobile network operator (playing the role of NPN-SP) decides to provision a PNI-NPN for private use by an enterprise (playing the role of NPN-SC) in the form of a network slice of a PLMN. NPN-SP and NPN-OP are assumed to be same in this case for simplicity in understanding.

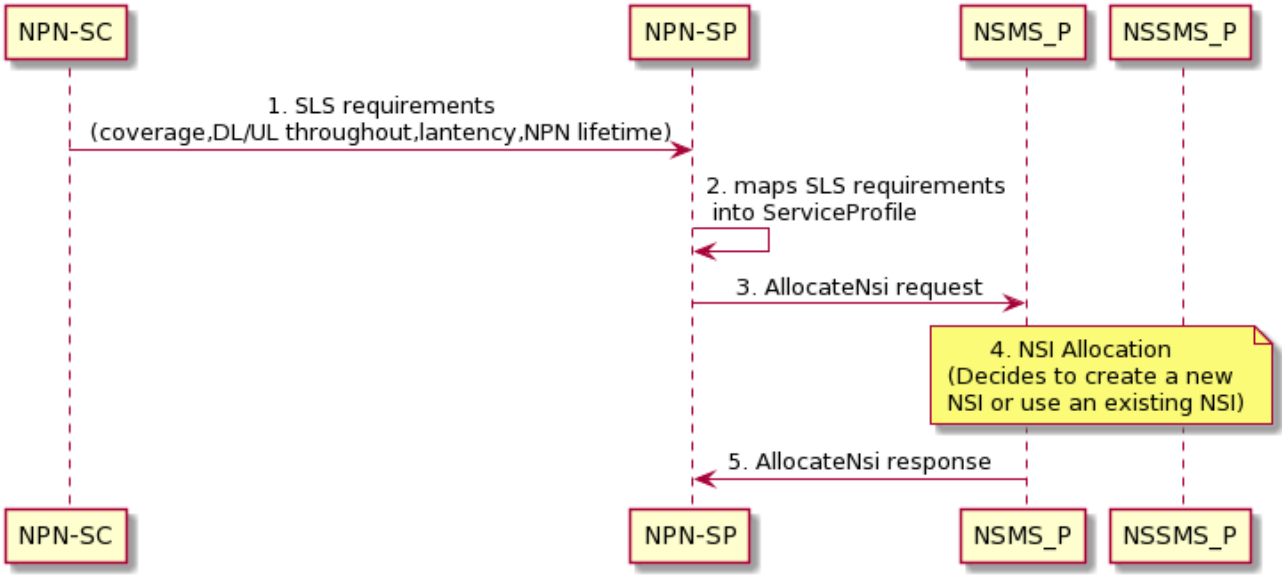

Figure 6.3.1-1: Procedure for NPN provisioning by a network slice of a PLMN

The main aspects of NPN provisioning by a network slice of a PLMN illustrated in Figure 6.3.1-1 include:

1) The NPN-SC provides the NPN related SLA requirements to NPN-SP. These requirements specify NPN related SLS according to different vertical industry requirements (e.g. coverage requirement within a specific geographic area, downlink/uplink throughput requirements, latency requirement, etc.) together with other business related information (e.g. NPN lifetime, NPN slice charging / accounting, etc.). The work flow between NPN-SP and NPN-SC is out of scope of the present document.

2) The NPN-SP maps these SLS requirements into ServiceProfile attributes (see TS 28.541 [7]).

3) The NPN-SP sends ServiceProfile in "AllocateNSI" request to NSMS_P.

4) Then the NSMS_P follows the NSI allocation procedure as described in clause 7.2 in TS 28.531 (this implicitly follows sub-steps like deriving slice profile requirements for subnets from service profile, checking possibility of reusing existing or creating new slice, allocation of NSSI etc. as per procedure defined in TS 28.531 [8]).

   - The NG-RAN domain NSSMS_P determines to utilize the existing NG-RAN NE(s) or new NG-RAN NEs that are deployed in the PLMN network or deployed locally at the enterprise's premise or in the factory.

     Based on the access policy from operator, from which the NSSMS_P can derive rules like days/time slots/occasions etc. for which an NPN UE can access a CAG cell, the NSSMF assigns the CAG ID identifying the CAG cells which enables the control of UE's access to related PNI-NPN. The `NRCellDU` should be configured with the CAG ID to support access control for PNI-NPN UEs. The details of `NRCellDU` see TS 28.541 [7].

   - The 5GC domain NSSMS_P determines to utilize new or existing 5GC NF(s) of the 5GC part that are deployed in the PLMN network.

   - If any, the TN domain related requirements are provided to the management system of TN domain.

5) The NSMS_P sends NSI allocation result in AllocateNsi response to the NPN-SP including the relevant network slice instance information.

6.3.2 Solution for exposure of management capability of PNI-NPN

The MNO (playing the role of NPN-SP) provides a PNI-NPN for a vertical (playing the role of NPN-SC) in the form of a network slice of a PLMN. This solution can be used by a vertical to obtain certain management capabilities (e.g., provisioning, performance monitoring) exposed by MNO in MNO-Vertical Managed Mode. The vertical consumes the exposed management capabilities to manage the PNI-NPN, including:

- Using the Network Slice Provisioning exposure management services and Network Slice Provisioning data report exposure management service (see clause 6.1 of TS 28.531 [8]), NPN-SC can request allocating, deallocating modifying an NSI, or obtain notifications about NSI Information model data.

- Using exposure of generic fault supervision management service (see clause 11.2 of TS 28.532 [14]) and generic performance assurance management service (see clause 11.3 of TS 28.532 [14]), NPN-SCs can create certain measurement jobs and select the type of data analytics and performance to be monitored, e.g., performance related to various traffic types, geographical areas, different device types, for a specific group of devices, for certain traffic congestion situation and analytical KPIs related to performance predictions.

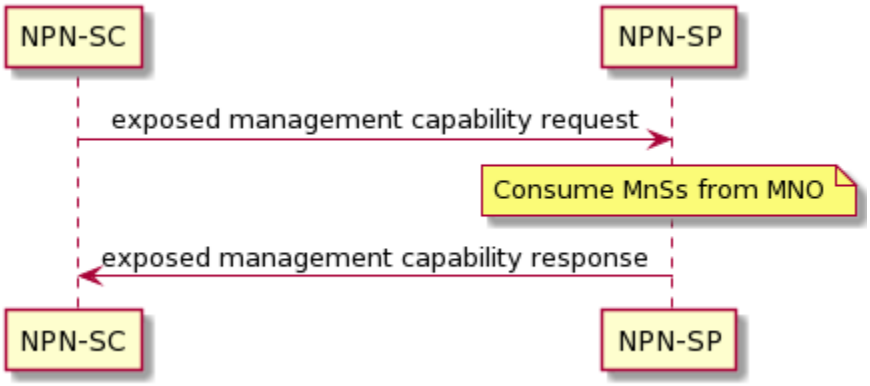

Figure 6.3.2-1: Exposure of management capability of PNI-NPN in MNO-Vertical Managed Mode

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

The applicability of management modes (see clause 4.3.2) depends on the NPN scenarios under consideration. Different scenarios may exist, depending on the deployment considerations of individual NPN functions. Table A-1 and Table A-2 capture this variety for SNPN and PNI-NPN scenarios, respectively.

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

NPN functions		MNO Managed Mode	MNO-Vertical Managed Mode	Vertical Managed Mode
NG-RAN		indoor; outdoor	indoor; outdoor	indoor; outdoor
5GC	Packet core (AMF, SMF, NRF, ...)	on-premise; off-premise (deployed on MNO footprint)	on-premise; off-premise (deployed on MNO footprint)	on-premise; off-premise (deployed on hyperscaler footprint)
	Subscription and data-storage manager (UDM, UDR, AUSF, …)	on-premise; off-premise (deployed on MNO footprint)	on-premise; off-premise (deployed on MNO footprint)	on-premise
	UPF	on-premise; off-premise (deployed on MNO footprint)	on-premise; off-premise (deployed on MNO footprint)	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 MNO Managed Mode and MNO-Vertical Managed Mode. These 5GC functions are dedicated to the NPN, and therefore are separated from PLMN functions (used for public use).
NOTE 4: A hyperscaler may play the VISP role for the virtualization of off-premise 5GC functions in Vertical Managed Mode.
NOTE 5: Off-premise UPF may need to be deployed at the Telco Edge Cloud, typically due to performance constraints.

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

NPN functions		MNO Managed Mode	MNO-Vertical Managed Mode
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 MNO Managed Mode and MNO-Vertical Managed Mode.
NOTE 4: Off-premise UPF may need to be deployed at the Telco Edge Cloud, typically due to performance constraints.

Annex B (informative): Plant UML source code

B.1 Procedure for UE related data collection

```
@startuml

note over "NPN-SC", "NPN-SP/OP": Pre-defined agreements
"NPN-SC" -> "NPN-SP/OP": 1. Create MDT collection task
"NPN-SP/OP" -> "NE":2. Send MDT collection request
"NE" -> "NE":3. UE Selection

skinparam responseMessageBelowArrow true
"NE" -> "UE":4. MDT activation
"UE" -> "NE":5. MDT data reporting (e.g. RLF report)
"NE" -> "NPN-SP/OP":6. MDT data reporting (e.g. RLF report)
"NPN-SP/OP" -> "NPN-SC":7. Send MDT results

skinparam sequenceMessageAlign center

@enduml
```

B.2 Procedure for SNPN provisioning with 3GPP segments only

The following PlantUML source code is used to describe the procedure for SNPN provisioning with 3GPP segments only, as depicted by Figure 6.2.1-1:

```
@startuml

   "NPN-SC" -> "NPN-SP":1. SLA requirements(e.g. coverage, \n DL/UL throughout,lantency,NPN
      lifetime)

   "NPN-SP" -> "NPN-SP": 2. map SLA into 3GPP-related NPN requirements

   "NPN-SP" -> "NPN-OP": 3. Send the 3GPP-related NPN requirements\n in form of the corresponding
      NRM fragmentsn

   "NPN-OP" -> "NPN-OP": 4. Decide on the constituent\n network resources and topology\n to trigger
      MOI creation

   "NPN-OP"-> "NPN-SP": 5. NotifyMOICreation Notification

   skinparam sequenceMessageAlign center

@enduml
```

B.3 Procedure for NPN provisioning by a network slice of a PLMN

The following PlantUML source code is used to describe the procedure for NPN provisioning by a network slice of a PLMN, as depicted by Figure 6.3.1-1:

```
@startuml

"NPN-SC" -> "NPN-SP": 1. SLS requirements\n(coverage,DL/UL throughout,lantency,NPN lifetime)
"NPN-SP" -> "NPN-SP": 2. maps SLS requirements \n into ServiceProfile
"NPN-SP" -> "NSMS_P":3. AllocateNsi request

note over NSMS_P, NSSMS_P: 4. NSI Allocation \n (Decides to create a new NSI \n or use an existing
NSI)
"NSMS_P" -> "NPN-SP":5. AllocateNsi response

skinparam sequenceMessageAlign center

@enduml
```

B.4 Procedure for exposure of management capability of PNI-NPN in MNO-Vertical Managed Mode

The following PlantUML source code is used to describe the procedure for exposure of management capability of PNI-NPN in MNO-Vertical Managed Mode, as depicted by figure 6.3.2-1:

```
@startuml


"NPN-SC" -> "NPN-SP": exposed management capability request

note over "NPN-SP": Consume MnSs from MNO

"NPN-SP" -> "NPN-SC":exposed management capability response

skinparam sequenceMessageAlign center


@enduml
```

Annex C (informative): Change history

Change history							
Date	**Meeting**	**TDoc**	**CR**	**Rev**	**Cat**	**Subject/Comment**	**New version**
2022-03	SA#95e	SP-220125				Presented for approval	2.0.0
2022-03	SA#95e					Upgrade to change control version	17.0.0
2023-03	SA#99	SP-230196	0001	-	F	Correct wrong abbreviation for Data Centre Service Provider	17.1.0

History

Document history		
V17.0.0	May 2022	Publication
V17.1.0	April 2023	Publication