Deployment and Operational Requirements of 5G Non-Public Networks

ATIS-I-0000091 | June 2022

Abstract

Support for Non-Public Networks (NPN) is a valuable addition to 5G in 3GPP Release 16. This white paper surveys and identifies services and capabilities inherent in public mobile networks that are not currently specified in detail by 3GPP for NPNs. Many of these services and capabilities relate to:

- Providing service continuity outside the NPN footprint, such as roaming.
- Interworking with other public and NPNs, such as robocalling protection for voice calls.

This white paper identifies enhancements that may be developed for NPNs to provide similar services and capabilities to those available in public networks.

Foreword

As a leading technology and solutions development organization, the Alliance for Telecommunications Industry Solutions (ATIS) brings together the top global ICT companies to advance the industry's most pressing business priorities. ATIS' nearly 200 member companies are currently working to address the all-Internet Protocol (IP) transition, 5G, network functions virtualization, big data analytics, cloud services, device solutions, emergency services, M2M, cyber security, network evolution, quality of service, billing support, operations, and much more. These priorities follow a fast-track development lifecycle — from design and innovation through standards, specifications, requirements, business use cases, software toolkits, open-source solutions, and interoperability testing.

ATIS is accredited by the American National Standards Institute (ANSI). The organization is the North American Organizational Partner for the 3rd Generation Partnership Project (3GPP), a founding Partner of the oneM2M global initiative, a member of and major U.S. contributor to the International Telecommunication Union (ITU), as well as a member of the Inter-American Telecommunication Commission (CITEL). For more information, visit www.atis.org.

Notice of Disclaimer and Limitation of Liability

The information provided in this document is directed solely to professionals who have the appropriate degree of experience to understand and interpret its contents in accordance with generally accepted engineering or other professional standards and applicable regulations. No recommendation as to products or vendors is made or should be implied.

NO REPRESENTATION OR WARRANTY IS MADE THAT THE INFORMATION IS TECHNICALLY ACCURATE OR SUFFICIENT OR CONFORMS TO ANY STATUTE, GOVERNMENTAL RULE, OR REGULATION, AND FURTHER, NO REPRESENTATION OR WARRANTY IS MADE OFMERCHANTABILITY OR FITNESS FOR ANY PARTICULAR PURPOSE OR AGAINST INFRINGEMENT OF INTELLECTUAL PROPERTY RIGHTS. ATIS SHALL NOT BE LIABLE, BEYOND THE AMOUNT OF ANY SUM RECEIVED IN PAYMENT BY ATIS FOR THIS DOCUMENT, AND IN NO EVENT SHALL ATIS BE LIABLE FOR LOST PROFITS OR OTHER INCIDENTAL OR CONSEQUENTIAL DAMAGES. ATIS EXPRESSLY ADVISES THAT ANY AND ALL USE OF OR RELIANCE UPON THE INFORMATION PROVIDED IN THIS DOCUMENT IS AT THE RISK OF THE USER.

NOTE - The user's attention is called to the possibility that compliance with this standard may require use of an invention covered by patent rights. By publication of this standard, no position is taken with respect to whether use of an invention covered by patent rights will be required, and if any such use is required no position is taken regarding the validity of this claim or any patent rights in connection therewith. Please refer to [http://www.atis.org/legal/patentinfo.asp] to determine if any statement has been filed by a patent holder indicating a willingness to grant a license either without compensation or on reasonable and non-discriminatory terms and conditions to applicants desiring to obtain a license.

Copyright Information

ATIS-I-0000091

Alliance for Telecommunications Industry Solutions
1200 G Street, NW, Suite 500
Washington, DC 20005

Contents

1. Introduction

NPN support is arguably the most significant feature added to 5G in 3GPP Release 16 [1]. Prior to 5G, 3GPP networks were developed primarily for public communication services by commercial service providers. 3GPP expanded 5G utility by adding support for NPNs, which are intended for use in many private network settings and vertical sectors.

The impetus for this white paper is to collect information from vertical sectors that are considering 5G NPN deployments.

To understand the NPN use cases, this white paper also assesses technical solutions based on 3GPP specifications, which have developed extensive supporting services and activities to meet public network deployment and operational requirements. This information is meant to be useful in identifying:

- Possible requirements for inclusion in solution roadmaps for operators and vendors.
- Possible topics for future specification in 3GPP or other organizations.

2. 5G Non-Public Network Use Case

Initial support for 5G NPNs was added to 3GPP Release 16 and is being extended in Release 17 [2] and beyond. 5G NPNs essentially extend 5G technologies for deployment and use in private (enterprise) environments. 5G NPN development is being driven mainly by two use cases:

- **Industrial settings employing advanced automation (variously referred to as the 4th Industrial Revolution, Industry 4.0, or Industrial Internet of Things (IIoT).** For these scenarios, the 5G NPN is likely to serve a single or cluster of industrial facilities such as factory, warehouse, logistics center, or port in a flexible and low cost manner. Examples of Industry 4.0 use cases that 5G NPN will be used to support include IIOT factory automation, inventory management and tracking, asset management and tracking, and process control.
- **Campus settings providing enterprise voice and data services.** 5G NPN will be used for combined enterprise voice and data services providing mobility within and beyond the campus setting. 5G NPN will provide additional flexibility and cost-effectiveness over the current use of Wi-Fi and softswitch Private Branch Exchanges (PBXs) with their attendant wiring for the Wi-Fi access points.

3GPP TS 22.261 [3] introduces NPNs as follows:

"Non-public networks are intended for the sole use of a private entity such as an enterprise, and may be deployed in a variety of configurations, utilizing both virtual and physical elements. Specifically, they may be deployed as completely standalone networks, they may be hosted by a PLMN, or they may be offered as a slice of a PLMN."

The Standalone Non-Public Network (SNPN) has no dependency on functions provided by a public 3GPP network. A 5G NPN integrated into a public network is referred to as a Public Network Integrated Non-Public Networks (PNI-NPN) and is hosted as a network slice of a Public Land Mobile Network (PLMN). The PNI-NPN requires a PLMN subscription by the 5G NPN subscriber, enabling access to public network services with the same User Equipment (UE).

5G NPN devices can be set up to access only specific 5G NPNs or to access both public networks (PLMNs) and specific 5G NPNs. Some of these PLMN/NPN combination devices will be able to connect to both types of networks simultaneously.

3. NPN Features

3.1 911 Support

3.1.1 Introduction

In 2019, the Federal Communications Commission (FCC) in its continuing oversight of citizen-to-authority emergency communication (E911) adopted the *Report and Order* implementing Kari's Law and Section 506 of RAY BAUM'S Act [4]. The focus of this rulemaking is the enhancement of 911 handling by enterprises and Multi-Line Telephone Systems (MLTS), also known as PBXs.

The main features of this regulation pertinent to the focus of this white paper are:

- **Direct dialing of 911.** The regulation specifies that no prefixes or special dialing can be required by a user to call 911 through the MLTS. An example is dialing 9 to gain an outside line by a hotel guest; this can't be required for 911 calls.
- **Notification of a 911 MLTS call to designated enterprise staff or MLTS terminal.** The regulation specifies that a MLTS must provide a notification to a central location or person that a 911 call has been placed, along with a valid callback number and the caller's location, which was provided to the Public Safety Answering Point (PSAP). This is to inform the enterprise's security or other responsible staff of the emergency. Additional notifications, such as to a facilities manager, are allowed.
- **Caller location.** The MLTS must provide this information to the PSAP.

3.1.2 Location Reporting

Public safety needs each 911 caller's exact location in order to dispatch emergency services there in a timely manner — a requirement that receives significant FCC attention. In the case of this regulation, the FCC extended its recent work on wireless location reporting accuracy to MLTS deployments.

The FCC's goal is for MLTS 911 location reporting accuracy to use the same accuracy definition as for wireless 911 – Dispatchable Location. The FCC recognized that providing Dispatchable Location in the near term of the regulations may be unattainable, so it provided Dispatchable Location alternatives depending on FCC-defined conditions such as fixed/wireless, on/off premise phone location, and phone types (e.g., Session Initiation Protocol (SIP) softphones, or wireless phones).

The FCC allows the use of Alternative Location and Registered Location (e.g., when the user manually enters their location into a database or profile) when Dispatchable Location is unattainable.

The FCC also specified that street addresses must be validated, as is done for public network 911 call location reporting.

The FCC did not adopt reporting requirements or require demonstration or proof of MLTS 911 Dispatchable Location Accuracy performance, as is required for PLMNs.

3.2 WEA/CMAS/PWS

Wireless Emergency Alert (WEA), also known as Public Warning System (PWS), is a public safety system that allows compatible mobile devices to receive geographically targeted, text-like messages alerting them of imminent threats to safety. These alerts include specified auditory (e.g., alert cadence) and sensory (e.g., vibration cadence) presentation in addition to the visual display. Since its launch in 2012, WEA has evolved from only Network-Based Geo-Targeting, where specific cell/sectors are selected to broadcast an alert, to also utilizing Device-Based Geo-Fencing. This allows WEA-capable mobile devices to perform a location comparison of an alert area defined by coordinates included in the broadcast from the network before presenting the alert to the user. WEA utilizes cellular broadcast technology, so it is currently not supported on Wi-Fi or other access technologies, even if owned or operated as part of the carrier's network.

In the United States, Commercial Mobile Service Providers (CMSPs) voluntarily participate in WEA, which involves a unique public/private partnership between the Federal Emergency Management Agency, the FCC, and the U.S. wireless industry to enhance public safety.

To support WEA, CMSPs must be connected to the Federal Emergency Management Agency's (FEMA) Integrated Public Alert and Warning System (IPAWS) via the "C"

interface. A "C-1" interface has also been specified that would allow delivery of the WEA emergency messages to participating CMSPs via free, over-the-air TV signals on participating Public Broadcasting Service (PBS) networks.

3.3 Stolen Handset Tracking

One 3GPP feature from 2G through 5G is that a mobile device can be easily switched to another subscriber or another network simply by swapping the existing Universal Subscriber Identity Module (USIM) with a USIM provisioned for a different user and possibly a different CMSP. The CMSP change is based on the mobile device's support of radio spectrum used by the new CMSP.

There is a downside for this: Each subscriber and CMSP switched in that mobile device can be stolen from their owners and the owner's USIM removed. The stolen mobile device can be re-sold, and the new user can install a USIM provided by their CMSP. The new user may or may not be aware of the stolen status of the mobile phone.

3GPP networks have a function, Equipment Identity Register (EIR), that can store lost and stolen handset identities. The CMSP network can validate device identities during network attach attempts against this list in the EIR. If the mobile device is identified as lost or stolen, the CMSP network can take remedial action such as blocking network use and services.

Through the normal course of customer service, CMSPs can take reports of lost or stolen mobile devices from their subscribers and add the International Mobile Equipment Identity (IMEI) into their EIR.

If CMSP A provisioned its EIR only with its own subscriber's reported lost and stolen mobile device identities, mobile devices stolen from a CMSP B's subscriber, and a CMSP A subscriber USIM installed, CMSP A's network will be unable to identify and block the stolen mobile device.

GSM Association (GSMA) provides CMSPs with an optional service to share stolen mobile device identities between operators. Periodically a CMSP's EIR can upload any new or changed reported stolen or recovered handset identities to the Central EIR (CEIR). Other CMSPs can then selectively download to their EIR this new or changed reported stolen or recovered handset identities. With this shared stolen device identity information, a CMSP

can provide the same treatment to a mobile device reported stolen to another operator when it is attempting to connect to the CMSPs network with the other CMSP's USIM.

For an NPN, an EIR can be deployed for storing lost or stolen NPN mobile device identification local to the NPN. Currently, at the time of this white paper, the GSMA does not allow or accommodate NPNs to directly participate in the GSMA CEIR. The NPN may be able to utilize the GSMA CEIR indirectly through a business arrangement with a CMSP that does have access to the GSMA CEIR.

Indirect use of the CEIR through a CMSP could be realized, for example, by the NPN sharing use of or accessing the CMSP's EIR as for PNI-NPN. Alternatively, for NPN mobile devices that also have PLMN subscriptions, reporting these lost or stolen devices could be done through the subscribed CMSP's reporting process (which could include use of GSMA's CEIR).

The decision whether to use only a local EIR can depend on the threat modelling and security risk level of an attacker being able to obtain a valid NPN subscription USIM to use in a stolen NPN mobile device.

Using the GSMA CEIR indirectly can depend on both establishing a business arrangement with a CMSP covering reporting and handling of lost and stolen NPN mobile devices, as well as the threat modelling and fraud risk level of stolen NPN mobile devices being used in other CMSP networks as described above.

3.4 Roaming

3GPP standards currently do not support NPN roaming. This was a deliberate consensus agreement based on a number of issues, including:

1) Security concerns about the use of non-3GPP credentials supported by NPNs preclude roaming between NPNs and PLMNs.
2) Use of a NPN network identification scheme that differs from the PLMN network identification scheme. NPN identifiers are not required to be globally unique, but PLMN identifiers are required to be globally unique.
3) Lack of a supporting infrastructure and NPN roaming ecosystem to create, manage, service, and enforce roaming agreements between NPNs or between NPNs and PLMNs.

Even though 3GPP does not currently support roaming, service continuity is supported by 3GPP standards, which is enabled by operator agreements. Service continuity allows for continuation of a call/session when a UE moves between coverage of an NPN and PLMN, as well as continuous coverage within an NPN comprised of both standalone and PNI-NPN aspects. An example of the latter would be a factory covered by a standalone NPN with some buffer of additional coverage provided around the factory by a PNI-NPN hosted by the local PLMN operator.

3.5 Caller ID Spoofing

This clause describes Caller ID spoofing for voice service providers over IP networks. It also assesses enterprise voice service providers with 5G NPN deployment, which is interconnected with the Public Switched Telephone Networks (PSTNs) and furnishes voice services to an end user.

3.5.1 Mitigation Components STIR/SHAKEN

Signature-based Handling of Asserted information using toKENs (SHAKEN) framework and Secure Telephony Identity Revisited (STIR) use public key cryptography to provide assurances that certain information about the caller ID transmitted with a particular call is accurate. STIR/SHAKEN validates the phone call, specifically the number indicated on the caller ID passing through the PLMNs. Both standards establish a reliable authentication system that helps strengthen robocall-blocking services and mitigate caller ID spoofing.

The STIR/SHAKEN spoofed call detection is limited when a voice call routes through a voice service provider with a non-IP network (e.g., a legacy PSTN) or a SIP call over User Datagram Protocol (UDP). In those networks, the STIR/SHAKEN-signed token may be lost, along with the ability to verify the caller ID. The 5G NPN IP Multimedia Subsystem (IMS) may be expected to implement SIP over Transmission Control Protocol (TCP) and Stream Control Transmission Protocol (SCTP) instead when the voice service providers offer STIR/SHAKEN to the enterprise customers.

STIR/SHAKEN is designed for the Originating Service Provider (OSP) to indicate the authenticity of the caller ID through cryptographic signing. However, there are some enterprise networks (e.g., NPN IMS voice) that use scenarios where the OSP does not have complete caller information and is therefore unable to fully authenticate the caller information. The capability of delegating this caller information authentication by the

OSP to the enterprise NPN is supported within the STIR/SHAKEN framework. There are several different methods defined to support delegation to the enterprise network (NPN) and can be found in ATIS 1000089: *Study of Full Attestation Alternatives for Enterprises and Business Entities with Multi-Homing and Other Arrangements* [5]. The NPN and OSP will need to agree on which method to use.

3.5.2 Tools to Help Combat Robocalls

Carriers and supporting analytics services must carefully ensure consumer protection while also ensuring that legitimate businesses are not impeded from reaching their customers. The most successful methods are incorporating stringent know-your-customer vetting, onboarding, and analytics services.

Carriers offer websites and helplines for legitimate businesses to appeal telephone numbers they believe are being labelled or blocked erroneously.

Tools may be helpful to protect NPN enterprise voice service users.

3.5.3 Data Collection and Analysis

In addition to Do-Not-Originate lists, the data analytics services can be applied to lower the overall service error rate for both false negatives (e.g., missed spam calls) and false positives (e.g., wrongly flagged legitimate calls). The analytics service helps to distinguish fraudulent or nuisance calling behavior from legitimate call traffic.

3.5.4 Traceback

The Industry Traceback Group conducts tracebacks on behalf of the industry through a Secure Traceback Portal. The Industry Traceback Group team asks the originator to make efforts to mitigate the illegal traffic. When that traffic is not mitigated, the downstream carriers, as well as appropriate enforcement agencies, may be informed about the source of the illegal traffic.

3.5.5 Call Blocking

Call blocking capabilities can be implemented by a voice service provider or by a mobile device. They are available to both enterprises and consumers to mitigate the delivery of fraudulent or other nuisance calls.

3.5.6 Blocklist and Allow List

The telephone numbers in a blocklist are typically blocked. Telephone numbers in a Do-Not-Originate list are blocked by the service provider. Blocklists may be incorporated into customer provided equipment (CPE) or provided as a service feature.

The caller subscriber's allow list lets a telephone number bypass call analytics services or blocking.

3.5.7 Display to Called Party

The industry led Robocall Strike Force highlighted the need to provide called parties with a greater degree of identification and control over the calls they receive. The Strike Force recommended that the industry develop a framework for delivering information from the network to the called party's device. The information displayed to the user can empower consumers to make a better decision in handling the calls.

3.5.8 Call Authentication Framework

The FCC issued an order to mandate that voice service providers implement the STIR/SHAKEN caller ID framework in the IP portions of their network by June 30, 2021 [6]. The FCC adopted certain extensions to the STIR/SHAKEN mandate, including for small voice service providers and for non-IP networks requiring voice service provider to:

1) Completely upgrade their non-IP networks to IP and implement STIR/SHAKEN on their entire network.
2) Work to develop a non-IP authentication solution, either on their own or through a third-party representative

3.5.9 Traceback

The FCC is establishing a process to traceback reported calls to the sources of illegal robocalls in order to register the origin of suspected unlawful robocalls. The Industry Traceback Group is established to lead these efforts.

In the future, a provider of covered Voice over Internet Protocol (VoIP) service may be required to maintain current contact information on file at the FCC and retain records of

each call transmitted over the service that is sufficient to trace such calls back to the source.

For more detailed background on illegal robocalling, the tools to counteract them, such as STIR/SHAKEN, and related regulations refer to ATIS: *Robocalling and Communication ID Spoofing: Better Understanding Illicit and Unwanted Calls and How to Counter Them* [7].

3.6 Lawful Interception

Lawful Interception (LI) is a regulated feature that allows Law Enforcement Agencies (LEAs) to require Telecommunications Service Providers (TSPs) to capture (e.g., intercept) the communications that transit the TSP's network involving certain individuals, referred to as intercept subjects. The intercepted information is then provided to the authorizing LEA(s). Within the U.S., the LI-related requirements are governed by the Communications Assistance for Law Enforcement Act (CALEA) of 1994. Court orders may also hold legal requirements outside the purview of CALEA; however, these are outside the scope of this white paper.

Communications transiting to/from an SNPN from a public network may be lawfully intercepted, pursuant to a court order, by the public network.

3.7 NPN Credentials from an External Entity

3GPP 23.501 [8] chapter 5.30.2.9 specifies management of SNPN UE credentials owned by a credential's holder. The UE may obtain access using credentials provided by an entity other than the SNPN, called a credentials holder. The credentials holder can use an authentication, authorization, and accounting (AAA) Server (reference 23.501 [8] figure 5.30.2.9.2-1) or the authentication server function (AUSF) and unified data management (UDM) for primary authentication and authorization (reference 23.501 [8] figure 5.30.2.9.3-1).

When the AUSF in an SNPN authenticates/authorizes the UE using the credentials from an AAA Server in a credentials holder, the Subscription Permanent Identifier (SUPI) is used to identify the UE toward the AAA server. The AUSF is discovered and selected by the Access and Mobility Management Function (AMF) based on the home network identifier (e.g., realm part) and the routing indicator in the Subscription Concealed

Identifier (SUCI) provided by the UE. The UE subscription data is retrieved from the UDM using the SUPI.

When the UDM decides that the primary authentication is performed by the AAA Server in the credentials holder based on the UE subscription data and UE's SUPI, the UDM instructs the AUSF to discover and select the Network Slice Specific and SNPN Authentication and Authorization Function (NSSAAF), and then forward Extensible Authentication Protocol (EAP) messages to the NSSAAF. The NSSAAF selects the AAA Server based on the domain name corresponding to the realm part of the SUPI.

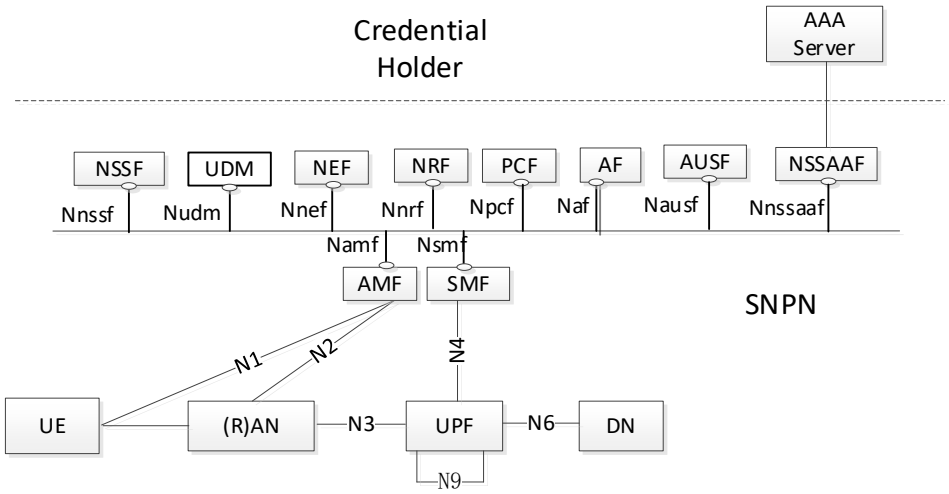

Figure 3.7-1: 5G System architecture with access to SNPN using credentials from Credentials Holder using AAA Server (from 3GPP TS 23.501 [8])

When a credentials holder uses AUSF and UDM for primary authentication and authorization for the SNPN UE, though the roaming architecture reference point N32 is used in the architecture, the UE is not considered to be roaming, and the architecture is a non-roaming reference architecture.

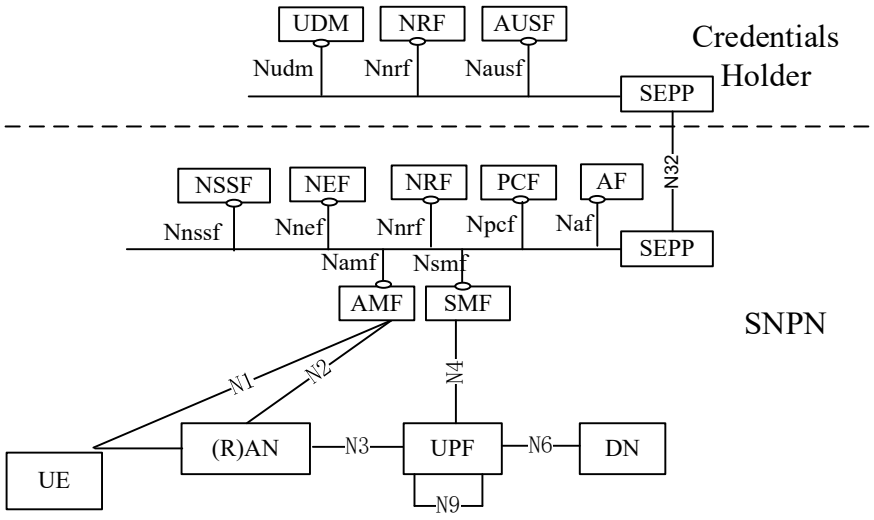

Figure 3.7-2: 5G System architecture with access to SNPN using credentials from Credentials Holder using AUSF and UDM (from 3GPP TS 23.501 [8])

3GPP 23.501 [8] chapter 5.39 specifies provisioning of third-party credentials for network slice selection and secondary authentication. Essentially, a connection is established between the UE and the server providing the credentials. These credentials themselves are out of scope for 3GPP.

There are no regulatory requirements for SNPN credentials.

3.8 National Security and Emergency Preparedness (NS/EP) Support

The U.S. government provides NS/EP priority communications to selected officials through the Next Generation Network Priority Services (NGN PS) program. The federal government has selected and contracted certain service providers to provide the service.

The NS/EP capability provides priority voice communication for the subscribed officials when the public voice communication network is overloaded, such as during widespread manmade or natural emergencies. NGN PS currently supports voice communication and is expanding to provide priority data and video services.

NGN PS provides this priority communication in one of two ways to individual designated officials. The first is through their mobile device subscribed to NS/EP (e.g., Wireless Priority Service (WPS)). The second is through calling-card-like features for

priority wireline calling (e.g., Government Emergency Telecommunications Service (GETS)).

NPN specifications in 3GPP currently do not define or support any NS/EP priority services. The Department of Homeland Security, Cybersecurity, and Infrastructure Security Agency (DHS CISA) is responsible for defining and extending NS/EP services and capabilities.

3.9 Voice Services

Voice services will allow SNPN users to communicate with other users using audio as the media (in principle, other media types, like video, can also be used). Voice sessions involving the SNPN users are established and maintained over the IP-based SNPN core network using the IMS-based session handling procedures as defined in 3GPP TS 24.229 [9]. Any voice services enjoyed by the SNPN users using IP-based Over the Top (OTT) networks are outside the scope of this white paper.

The other users who may be engaged in a voice communication with the SNPN users may be within the same SNPN (intra-SNPN) or outside the SNPN (e.g., other SNPN, PLMN, or fixed network). In the latter case, they may also be users without a VoIP-capable phone.

The scope of the features that go along with the voice services available to SNPN users may vary on an SNPN need basis. A few examples of such features are:

- Conferencing
- Call redirection
- Voicemail
- Abbreviated dialling plan (e.g., dialling extensions for intra-SNPN calls)

The network functions that handle the call-routing-related (e.g., SIP-based) signalling and the media transfer (e.g., Real-time Transport Protocol (RTP-based)) are considered to be part of an IMS domain that may be deployed within the SNPN or outside the SNPN. In the latter case, the IMS service provider can be in another SNPN, a PLMN, or a third party that the SNPN has an agreement with. These possible options are defined in 3GPP TS 23.228 [10].

When the IMS is deployed by the SNPN itself, IMS-based services may be limited to intra-SNPN sessions. SNPN users may have to connect to a PLMN or fixed network for outgoing PSTN voice calls. As yet another deployment option, the SNPN users may be allowed to use voice services only while connected to a PLMN. In this case, the SNPN user is treated like any other user within the PLMN with a suitable voice subscription in the PLMN.

A more detailed technical discussion of IMS in NPNs can be found in Appendix A of this white paper.

3.10 Messaging Services

Like any other mobile users, the SNPN users may also like to engage in message-based communications with the other users. Short Message Service (SMS), Multimedia Messaging Service (MMS), and Rich Communication Suite (RCS) are the three primary messaging services provided by 5G.

3.10.1 SMS

The 3GPP specifications do not explicitly mention the details of SMS handling in the context of SNPN. But based on how the SMS is defined in 3GPP TS 23.501 [8] for other users that access 3GPP-based networks, this clause assumes that SMS for SNPN users can operate in two modes:

1) SMS over IP
2) SMS over Non-Access Stratum (NAS)

SMS over IP is routed over the IMS through the Short Message Gateway (IP-SM-GW), whereas SMS over NAS is routed over the 5G Core (5GC) through Short Message Service Function (SMSF).

NOTE 1: SMS over NAS destined for an IMS-enabled UE is routed through the IP-SM-GW (part of the IMS) over SMSF (part of 5GC).

For SMS over IP, the IMS deployment options considered for voice services (see Annex A) will have to be considered for SMS, as well.

NOTE 2: The 3GPP TS 23.501 [8] defines that based on a home PLMN (HPLMN) operator's preferences, IMS-enabled UEs can be provisioned to use just the SMS over NAS, or SMS over IP as the preferred way.

This clause assumes that it will be an operator preference whether similar provisioning options should made available for SNPN UEs, as well.

Mobile devices usually have one preconfigured Short Message Service Center (SM-SC) address. Applying the same principle to the SNPN UEs, the operation of the SMS for SNPN UEs will have to have the following considerations:

- To support SMS over NAS, the SNPN shall be deployed with an SMSF. Otherwise, an SNPN UE that is not IMS-enabled will have to be connected to the PLMN in order to use SMS.
- An SNPN UE that is IMS-enabled will have to be preconfigured with the address of the SM-SC that resides in the IMS network domain used for that UE.
    - Some deployment options may necessitate the need to have two pre-configured SM-SC addresses in the SNPN UEs, along with two telephone numbers.
- If the SNPN also has an SM-SC, then unless that SM-SC has external connectivity, the SNPN UEs are required to be connected to the PLMN in order to use SMS. In this case, it should be possible to preconfigure two SM-SC addresses in the SNPN UEs.
- When the SM-SC present in the SNPN has external connectivity, and if two SM-SC addresses are pre-configured in the SNPN UEs, then such SNPN UEs should have two telephone numbers.

Home Subscriber Server (HSS) present in the PLMN or in the third-party IMS network shall be able to interact with the UDM present in the SNPN to support SMS over NAS for SNPN UEs. Such an interaction would be required with the third-party IMS even for SMS over IP.

The SMS over IP from/to SNPN UEs, without a telephone number, will be routed in the same way the voice calls are routed. In that case, the SM-SC or IP-SM-GW is not used.

For further details, see Annex B.

3.10.2 RCS

RCS is an IMS- and internet-based communication protocol that lets users engage in a variety of messaging services with the ability to know the capabilities of the other user's device. This clause provides an overview of RCS from an SNPN perspective.

The specifications for RCS were developed by GSMA and include the following services:

- **Standalone messaging.** This allows the transfer of a single message between two RCS users. There are two modes in this:
  - Messages that have less than 1300 bytes. Also referred to as pager mode standalone messaging, this mode can be without an IMS session (e.g., via SIP MESSAGE).
  - Messages that have more than 1300 bytes. Also referred to as large message mode standalone messaging, this mode is done with an IMS session.
- **1:1 chat.** After an IMS session is established (two RCS users), the SNPN RCS user can exchange more than one messages with another RCS user (SNPN or non-SNPN).
- **Group chat.** After an IMS session is established (multiple RCS users), the SNPN RCS user can exchange more than one message with multiple RCS users (SNPN or non-SNPN).
- **Capability discovery.** Using SIP OPTIONS or Presence method, an SNPN RCS user can discover the capabilities supported by the other RCS user's client (SNPN or non-SNPN).
- **File transfer.** This allows an RCS user (SNPN or non-SNPN) to send a file to another RCS user (SNPN or non-SNPN). There are two ways an RCS file transfer can be done:
  - An RCS user (SNPN or non-SNPN) can upload a large file to an internet server and then send just the URL to the other RCS users (SNPN or non-SNPN) via SIP MESSAGE. The other RCS users (SNPN or non-SNPN) can then download the file using that URL.
  - An RCS user (SNPN or non-SNPN) can establish an IMS session with another RCS user (SNPN or non-SNPN) and then transfer the file using MSRP. This method of file transfer can also be part of a chat session, a large message standalone messaging session, or as an in-call service.

- **Geolocation push.** An RCS user (SNPN or non-SNPN) can establish an IMS session with another IMS user (SNPN or non-SNPN) and then send their own geo-location information using MSRP.

As the above list shows, almost all the services defined so far focus on the various forms of messaging. However, earlier versions of GSMA specifications did support RCS voice and RCS video as a part of the overall suite of communications. In the later specifications, voice and video are no longer supported.

For the file upload/download procedures, the destination internet server for uploads is referred to as a Hypertext Transfer Protocol (HTTP) content server. The terminating RCS user's provider may deploy a localization function to retrieve the file from the HTTP content server.

Because RCS is an application of IMS, the different deployment options discussed in clause 3.10 for SNPN shall also be applicable to SNPN RCS services:

- The SNPN that has the IMS may have an RCS Server, as well.
- When partnering PLMN-based IMS is used, the RCS Server can be an Applications Server (AS) in that partnering PLMN.
- When third-party IMS is used, the RCS Server can be an AS in the third-party IMS provider.

The RCS Server can also be a third-party-provided AS of an IMS used to provide the voice services or of a third-party IMS used to provide just the RCS.

3.10.3 MMS

Using MMS, the users may exchange Multi-Media (MM) messages with other users. The details of MMS are defined in OMA-TS-MMS_ENC-V1_3-20110913-A [11] and the 3GPP TS 23.140 [12]. The recipient of an MM message may be addressed via either a Mobile Station International Subscriber Directory Number (MSISDN) (or E.164 number) or an email address.

The above specifications do not explicitly mention the details of MMS handling in the context of SNPN. But due to the fact that MMS is an internet-based service, this clause assumes that SNPN users may also send and receive MM messages using MMS.

The MM messages are routed to the MMS Proxy-Relay/Server present in the MMS service provider's network. For an MM message transfer between two users, two different MMS Proxy-Relay/Servers may be on the path (e.g., one in the originating network and one in the terminating network). Unlike SMS, an incoming MM message can also get forwarded. The MMS Proxy-Relay/Server may also be deployed as separate NFs. The MMS Proxy-Relay/Server will have connectivity to the other servers, such as those for email, SM-SC, etc.

All incoming and all submitted (e.g., sent) MM messages may be stored at the Multi-MediaBox (MMBox), a logical entity of the MMS Proxy-Relay/Server. The MMS users may also upload an MM message to the MMBox. They may also use the MMBox to review, retrieve and delete messages stored there.

Figures 3.10.3-1 and 3.10.3-2 illustrate overviews of MM message transfer from a perspective SNPN with two different deployment models.

Deployment Model 1 - The figure below shows the case where the MMS Proxy-Relay/Server of the partnering PLMN is used.

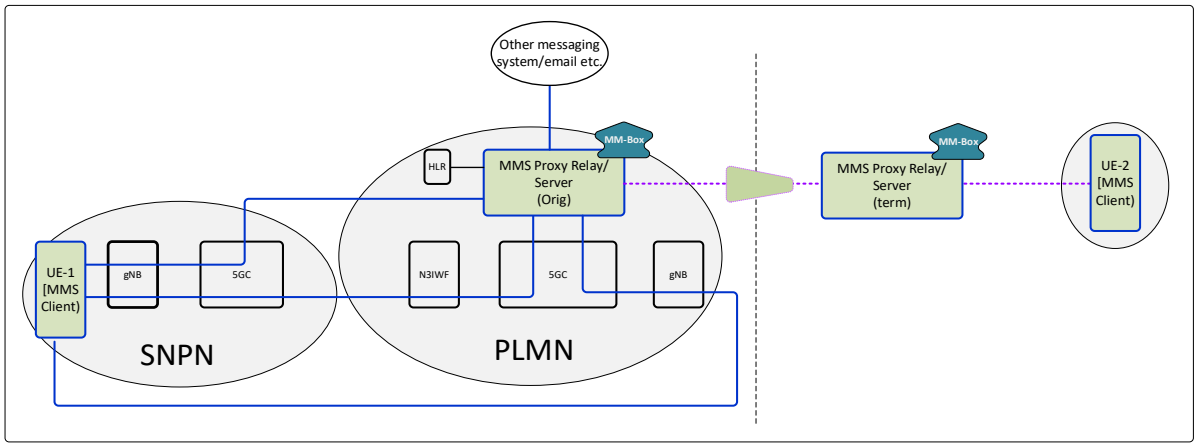

Figure 3.10.3-1: An overview of MM message transfer with a PLMN MMS Proxy-Relay/Server

Figure 3.10.3-1 illustrates three ways of UE-to-network connectivity from an SNPN UE's perspective that would allow an SNPN user to send or receive MM messages. In one of them, the SNPN users need not be connected to the PLMN in order to send or receive the MM messages. With this model, the SNPN UEs may have the same pre-configured MMS Proxy-Relay/Server independent of the serving network.

Deployment Model 2 - The figure below illustrates the case of MM transfer with an SNPN-hosted MMS Proxy-Relay/Server.

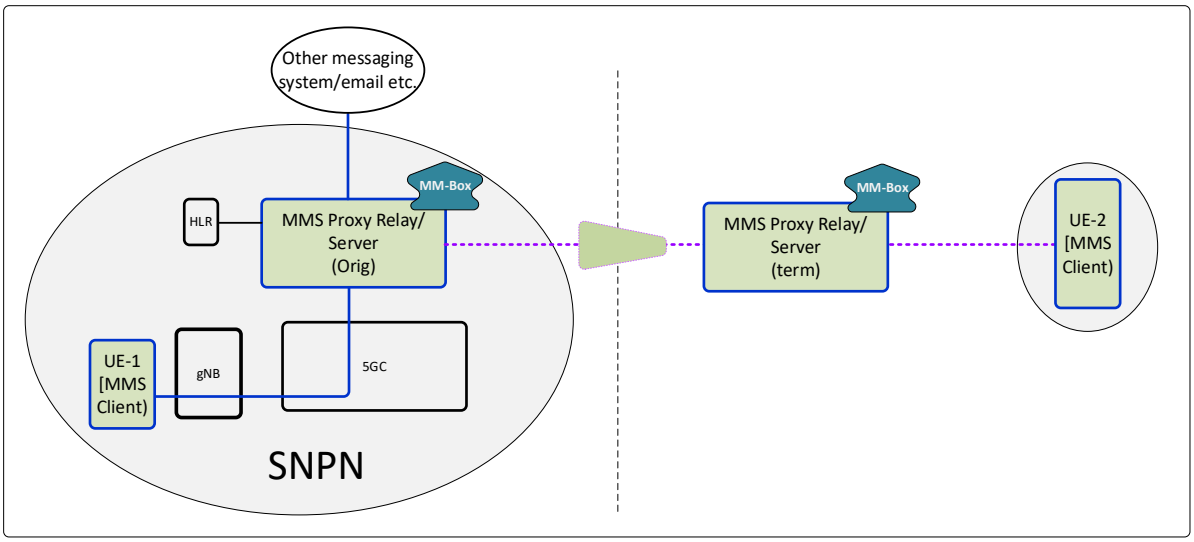

Figure 3.10.3-2: Overview of MM message transfer with SNPN MMS Proxy-Relay Server

Figure 3.10.3-2 illustrates a deployment model where the SNPN is deployed with its own MMS Proxy-Relay/Server, which would allow the SNPN users to send and receive MM messages without any dependency on the partnering PLMN. With this model, the SNPN UEs will be required to have two preconfigured MMS Proxy-Relay/Server addresses, with the ability to choose between the two. In addition, the SNPN UEs will have to have two separate telephone numbers to allow the network to properly route incoming MM messages.

3.11 Real-Time-Text (RTT)

RTT will allow the SNPN users to communicate with other users using real-time text messages.

The RTT sessions involving the SNPN users are established and maintained over the IP-based SNPN core network using the IMS-based session handling procedures as defined in 3GPP TS 24.229 [9] with a media type of text. A special payload type of text is used to transport the text characters over the IP network in the form of Real-Time Transport Protocol (RTP) streams [13] (RFC4103: RTP Payload for Text Conversation). Any RTT

services enjoyed by the SNPN users using IP-based OTT networks are outside the scope of this white paper.

Other than the media type being text instead of audio, deployment options are the same as described in Annex A for voice services with following RTT-specific considerations:

- When the SNPN user is involved in an RTT session with another user in the CS-domain, the MRFP provides the conversion from RTT to TTY (e.g., Baudot 45.45 baud codes that utilize the Frequency Shift Keying (FSK) method with 1400 Hz and 1800 Hz tones) and vice-versa.

The text appears at the destination device (either the terminating party or the originating party of an RTT call) when it is typed at the source device (either the originating party or the terminating party of an RTT call). The use of RTT as media in a communication can be unidirectional or bidirectional.

If RTT support is required in the SNPN, then the devices shall have the capabilities as defined in ATIS-0700029: Real-Time-Text Mobile Device Behavior [14].

3.12 National Suicide Prevention Lifeline Support

The federal government has established the National Suicide Prevention Lifeline (NSPL), or "Lifeline," and Veterans Crisis Line (VCL) to help Americans in crisis access suicide prevention and mental health support services. In the *988 Report and Order* [15] the FCC designates 988 as the three-digit number to reach the Lifeline. The FCC requires covered providers to make all changes necessary to support transmitting a call initiated by an end user dialing 988 to the current toll-free access number for Lifeline by July 16, 2022 [15]. The calls are then routed to the appropriate regional call center. The term "covered provider" means any telecommunications carrier, interconnected VoIP provider, or provider of one-way VoIP.

In a *Second Report and Order* [16], the FCC states that beginning July 16, 2022, all covered text providers must route a covered 988 text message to Lifeline.

4. Conclusions

NPN development, deployment, and use of NPNs by various vertical sectors are in the very early stages, with limited usage experienced so far. Examination by vertical sectors on how NPN services, covered in this white paper, could be useful to NPN deployments has been limited.

This white paper has presented some important topics related to the deployment and operation of 5G NPNs that may have interest by one or more vertical sectors utilizing NPNs. The body of the white paper shows the detailed analysis performed on each feature.

This analysis has shown that 3GPP specifications give sufficient technical guidance to enable support for the features considered for elements covered by 3GPP specifications. However, in some cases there are design decisions for support capabilities of significant size and complexity that are not specified by 3GPP.

This white paper does not make specific recommendations for future specifications in 3GPP.

It may be valuable for ATIS to revisit topic areas of this white paper, as well as applicable additional topics, as sector-specific interest and requirements emerge for NPNs.

A topic not covered in this white paper, but a potential future one for ATIS, is the NPN device lifecycle. This could examine how devices supporting NPNs are managed during their lifecycle, from initial availability from the device vendor to de-activating or de-commissioning. 3GPP has defined a standardized solution for NPNs, but the supporting service capabilities needed are currently not well-defined in the public commercial mobile communication services.

5. Glossary

Non-Public Network: A network that is intended for non-public use. [3]

Public Network Integrated NPN: A non-public network deployed with the support of a PLMN. [8]

Standalone Non-Public Network: A non-public network not relying on network functions provided by a PLMN. [8]

6. Acronyms

2G	Second generation
3GPP	Third Generation Partnership Project
5G	Fifth generation
5GC	5G Core
AAA	Authentication, Authorization, and Accounting
AMF	Access and Mobility Management Function
AS	Applications Server
AUSF	Authentication Server Function
CALEA	Communications Assistance for Law Enforcement Act
CEIR	Central EIR
CISA	Cybersecurity and Infrastructure Security Agency
CMSPs	Commercial Mobile Service Providers
CPE	Customer Provided Equipment
DHS	Department of Homeland Security
E911	Citizen-to-Authority Emergency Communication
EAP	Extensible Authentication Protocol
EIR	Equipment Identity Register
FCC	Federal Communications Commission
FEMA	Federal Emergency Management Agency
FSK	Frequency Shift Keying
GETS	Government Emergency Telecommunications Service
GSMA	GSM Association, aka Global System for Mobile Communications Association
HNPN	Home NPN[1]

[1] HNPN is not a 3GPP term because 3GPP has not yet addressed NPN roaming.

HPLMN	Home PLMN
HSS	Home Subscriber Server
HTTP	Hypertext Transfer Protocol
IIoT	Industrial Internet of Things
IMEI	International Mobile Equipment Identity
IMS	IP Multimedia Subsystem
IP	Internet Protocol
IPAWS	Integrated Public Alert and Warning System
IP-SM-GW	Short Message Gateway
LEAs	Law Enforcement Agencies
LI	Lawful Interception
MLTS	Multi-line Telephone Systems
MM	Multi-Media
MMBox	MultiMediaBox
MMS	Multimedia Messaging Service
MSISDN	Mobile Station International Subscriber Directory Number
MSRP	Messenger Service Remote Protocol
NAS	Non-Access Stratum
NGN PS	Next Generation Network Priority Services
NPN	Non-Public Network
NS/EP	National Security and Emergency Preparedness
NSPL	National Suicide Prevention Lifeline
NSSAAF	Network Slice-Specific and SNPN Authentication and Authorization Function
OSP	Originating Service Provider
OTT	Over the Top
PBX	Private Branch Exchanges
PLMN	Public Land Mobile Network, sometimes referred to as Public Network
PNI-NPN	Public Network Integrated NPN
PSAP	Public Safety Answering Points
PSTN	Public Switched Telephone Network
PWS	Public Warning System
RCS	Rich Communication Suite
RTP	Real-time Transport Protocol
RTT	Real-Time-Text
SCTP	Stream Control Transmission Protocol
SHAKEN	Signature-based Handling of Asserted information using toKENs
SIP	Session Initiation Protocol
SMS	Short Message Service

SM-SC	Short Message Service Center
SMSF	Short Message Service Function
SNPN	Standalone NPN
STIR	Secure Telephony Identity Revisited
SUCI	Subscription Concealed Identifier
SUPI	Subscription Permanent Identifier
TCP	Transmission Control Protocol
TSPs	Telecommunications Service Providers
TTY	Text Telephone
UDM	Unified Data Management
UDP	User Datagram Protocol
UE	User Equipment
USIM	Universal Subscriber Identity Module
VCL	Veterans Crisis Line
VNPN	Visited NPN[2]
VoIP	Voice over Internet Protocol
VPLMN	Visited PLMN
WEA	Wireless Emergency Alerts
WPS	Wireless Priority Service

[2] VNPN is not a 3GPP term because 3GPP has not yet addressed NPN roaming.

References

[1] https://www.3gpp.org/release-16

[2] https://www.3gpp.org/release-17

[3] 3GPP TS 22.261 Service requirements for the 5G system

[4] FCC 19-76 FCC *Report and Order*, PS Docket No. 18-261, PS Docket No. 17-239. GN Docket No. 11-117, released August 2, 2019

[5] ATIS 1000089. v002: *Study of Full Attestation Alternatives for Enterprises and Business Entities with Multi-Homing and Other Arrangements*, released May 2021

[6] https://www.fcc.gov/document/fcc-mandates-stirshaken-combat-spoofed-robocalls

[7] ATIS-I-0000081: *Robocalling and Communication ID Spoofing: Better Understanding Illicit and Unwanted Calls and How To Counter Them*, released February 2021

[8] 3GPP TS 23.501 System Architecture for the 5G System, V17.2.0 (2021-09).

[9] 3GPP TS 24.229 IP multimedia call control protocol based on Session Initiation Protocol (SIP) and Session Description Protocol (SDP); Stage 3

[10] 3GPP TS 23.228 IP Multimedia Subsystem (IMS); Stage 2

[11] OMA-TS-MMS_ENC-V1_3-20110913-A Multimedia Messaging Service Encapsulation Protocol

[12] 3GPP TS 23.140 Multimedia Messaging Service (MMS); Functional description; Stage 2

[13] RFC4103: *RTP Payload for Text Conversation,* released June 2005, https://www.rfc-editor.org/rfc/pdfrfc/rfc4103.txt.pdf

[14] ATIS-0700029: *Real-Time-Text Mobile Device Behavior*, released January 2017

[15] FCC 20-100 *FCC Report and Order,* WC Docket No. 18-336, released July 17, 2020

[16] FCC21-119 FCC *Second Report and Order,* WC Docket No. 18-336, released November 19, 2021, https://www.federalregister.gov/documents/2022/01/05/2021-27878/implementation-of-the-national-suicide-hotline-improvement-act-of-2018; https://docs.fcc.gov/public/attachments/FCC-21-119A1.pdf

Annex A: Voice Service Network Topologies

A.1 Overview

This annex illustrates a few network topologies that may apply to SNPN-related voice services.

A.2 PLMN-Based Voice Services

In this option, from a PLMN's perspective, the user's device is either camping on the PLMN or, if camping on the SNPN, then connected to the PLMN via non-3GPP access.

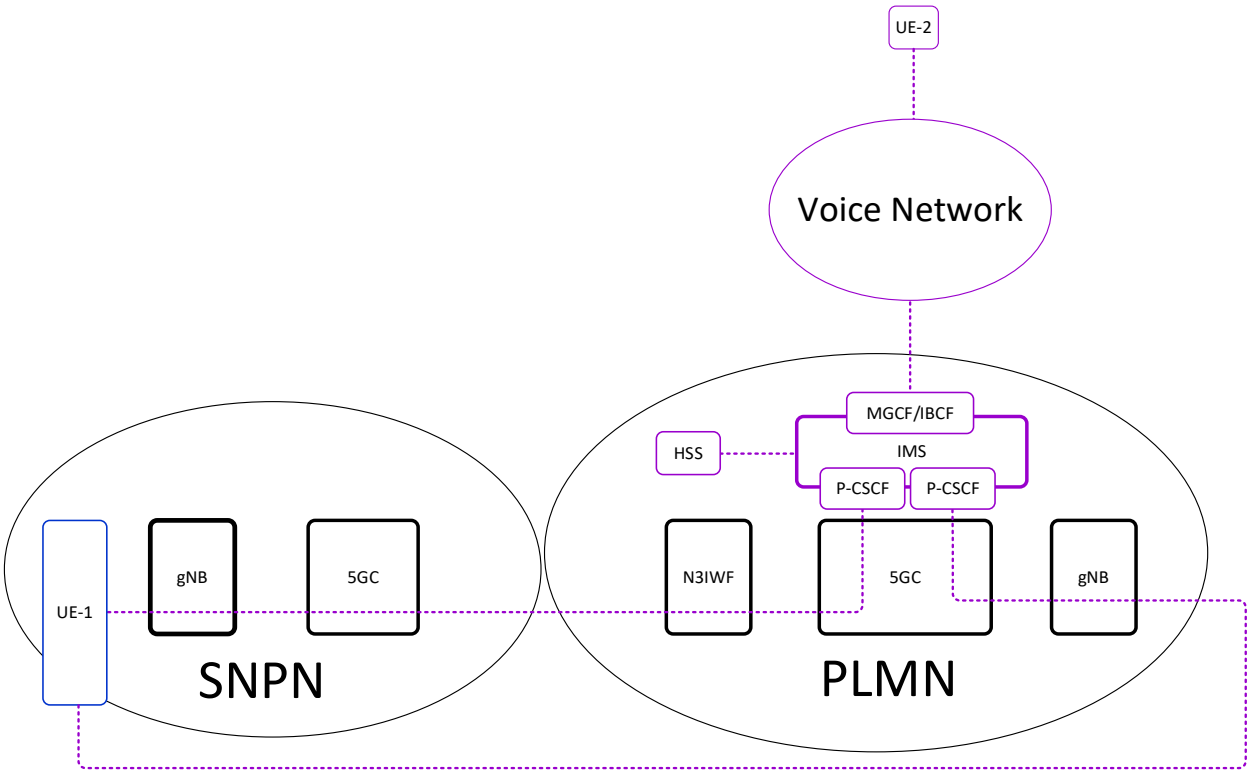

Figure A.2-1: PLMN-based voice services

Figure A.2-1 shows two ways the UE-1 can be connected to a PLMN-based IMS:

1) Camping on the SNPN but connected to PLMN via N3IWF Gateway located in the PLMN (which is called non-3GPP access from a PLMN perspective).
2) Camping directly on the PLMN network.

To allow for such a scenario, the SNPN user needs a PLMN subscription. Support of abbreviated dialling between SNPN users depends on the agreement between the SNPN and PLMN and IMS capabilities.

A.3 SNPN-Based IMS with Limited Capabilities

With this option, an SNPN user while connected to access SNPN services will be allowed to engage in voice services only with another SNPN user within the same SNPN. For outgoing voice calls, the SNPN user will have to connect to PLMN-based voice services, as covered in clause A.2. This option is illustrated below:

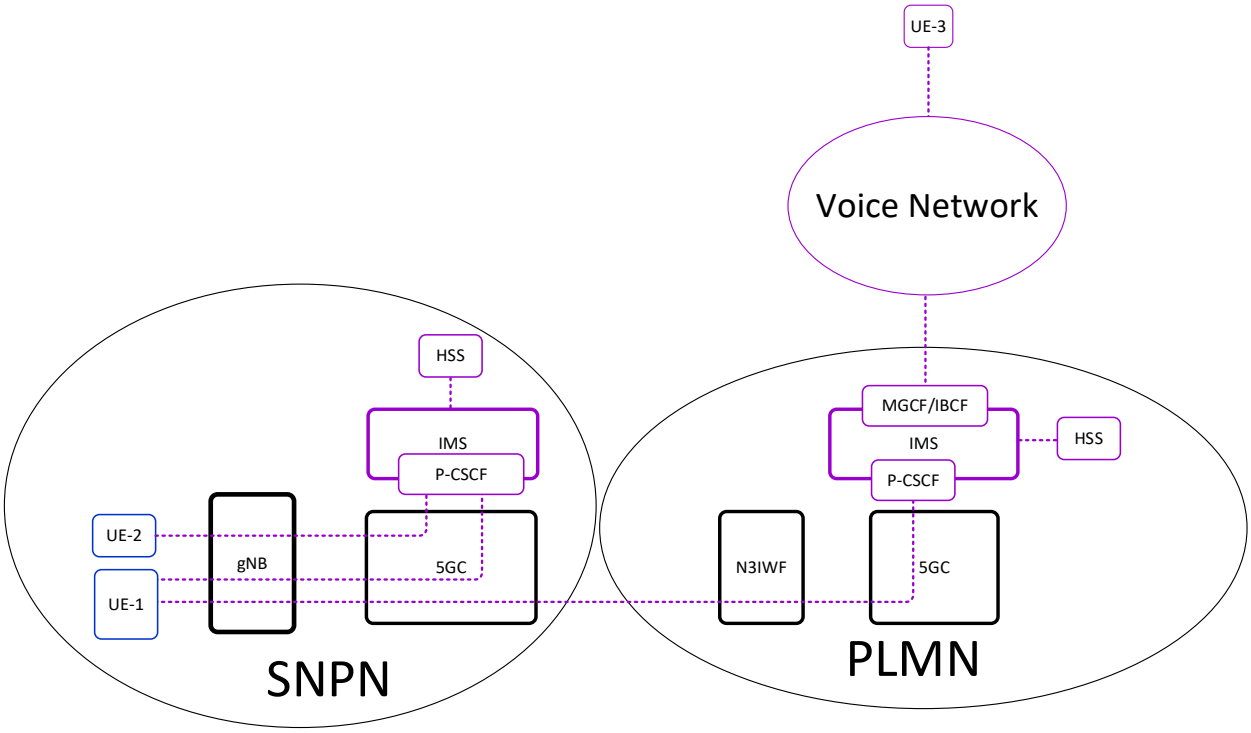

Figure A.3-1: SNPN-based voice services with limited capabilities

Figure A.3-1 shows two ways the UE-1 can get voice services:

1) While camping on the SNPN and connected to the SNPN-provided IMS.
2) While camping on the SNPN but connected to a PLMN via a N3IWF Gateway located in the PLMN (called non-3GPP access from a PLMN perspective).

Note that the second method shown in figure A.2-1 is also possible but not relevant to Figure A.3-1.

The SNPN-based IMS does not have any connectivity to the external voice network. Therefore, it can be used to provide only limited capabilities such as intra-SNPN calls. The SNPN user may have just one telephone number with this approach (e.g., 561 555 9432 for external calls and 9432 for internal calls).

A.4 SNPN-Based IMS with Full Capabilities

With this option, an SNPN user while connected to access SNPN services will be allowed to engage in voice services with another SNPN user within the same SNPN or with another user outside the SNPN. This option is illustrated below:

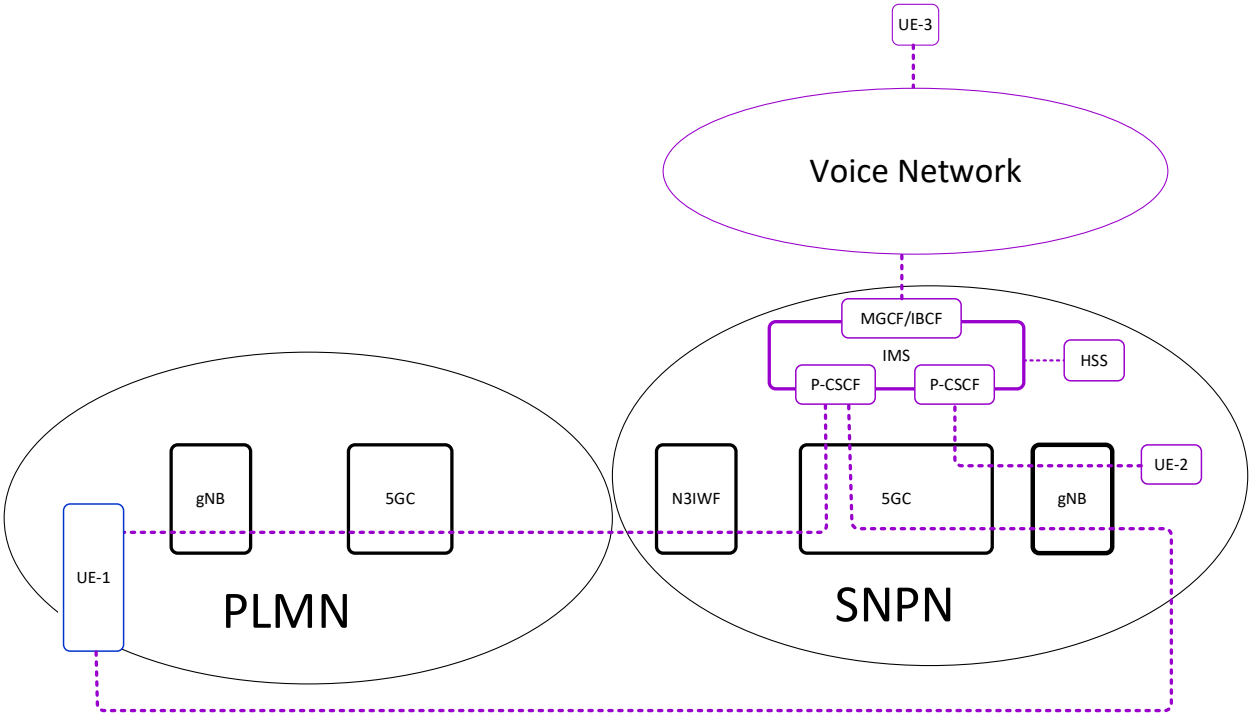

Figure A.4-1: SNPN-based voice services with full capabilities

Figure A.4-1 shows SNPN-based IMS that has connectivity to the external voice network. The SNPN-based IMS will allow the SNPN users (UE-1, UE-2) to engage in intra-SNPN and inter-SNPN or PLMN voice calls. An SNPN user (UE-1) camping on a PLMN can be connected to the SNPN via non-3GPP access (from SNPN perspective) to get the same

voice services provided by the SNPN-based IMS. Note that the two methods shown in Figure A.2-1 are also possible but not relevant to this illustration.

As in the case shown in Figure A.3-1, the abbreviated dialling plan may be also used for intra-SNPN sessions. If the SNPN user is allowed to use a PLMN-based voice service, as shown in Figure A.2-1, then that SNPN user will be assigned two separate telephone numbers.

A.5 Third Party-Based IMS

With this option, an SNPN user while connected to access SNPN services will be allowed to engage in voice services with another SNPN user within the same SNPN or with another user outside the SNPN. The difference between this option and the option shown in clause A.4 is that here the IMS is provided by a third party. This option is illustrated below:

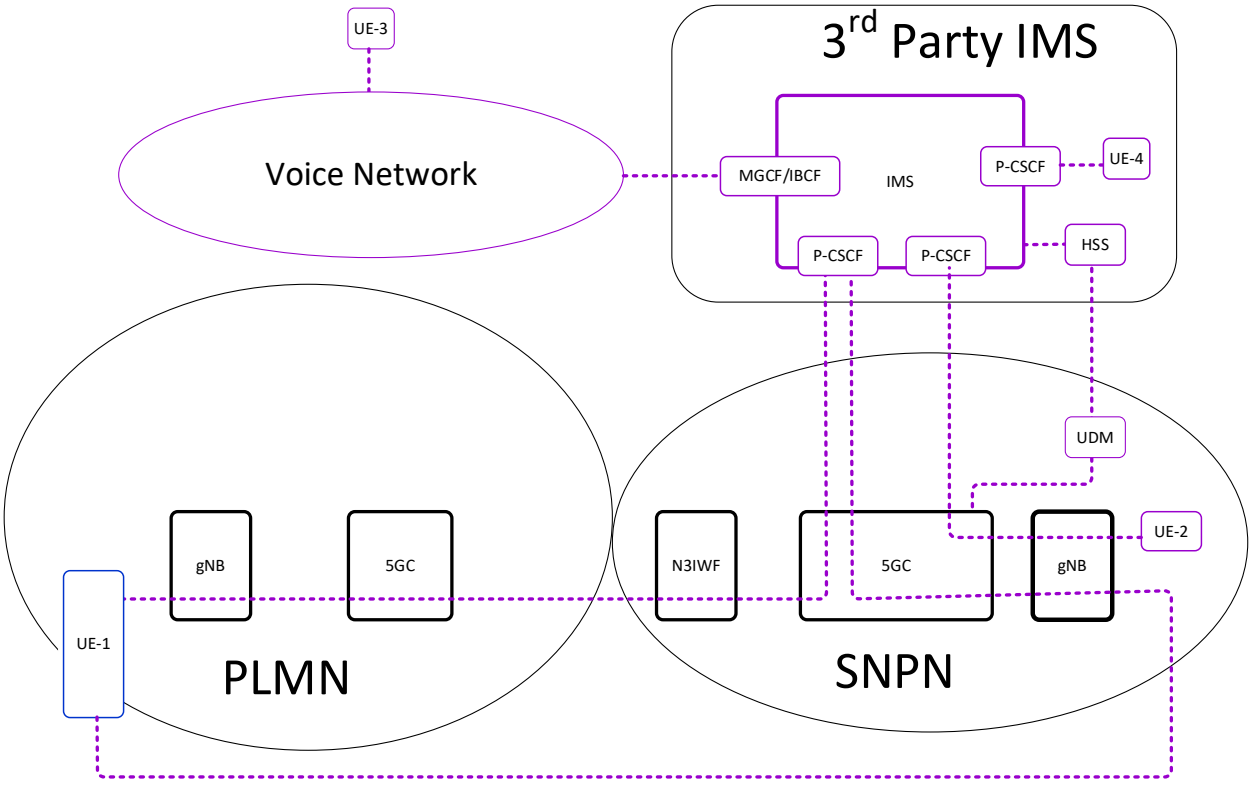

Figure A.5-1: Third-party-based IMS

Figure A.5-1 shows a third-party IMS that is used to provide the voice services for SNPN users. The third-party IMS can be configured to allow the SNPN users (UE-1, UE-2) to use abbreviated dialling plans for intra-SNPN calls. An SNPN user (UE-1) camping on a PLMN can be connected to the SNPN via non-3GPP access (from SNPN perspective) to get the same voice services provided by the third-party IMS. Note that the two methods shown in Figure A.2-1 are also possible but not relevant to this illustration.

If the SNPN user is allowed to use a PLMN-based voice service as shown in Figure A.2-1, then that SNPN user will be assigned two separate telephone numbers.

A.6 PLMN-Based IMS as Third-Party IMS

With this option, an SNPN user while connected to access the SNPN services will be allowed to engage in voice services with another SNPN user within the same SNPN or with another user outside the SNPN. The difference between this option and the option shown in clause A.5 is that here the IMS is provided by the PLMN, which is viewed as a third party from the SNPN's perspective. This option is illustrated below:

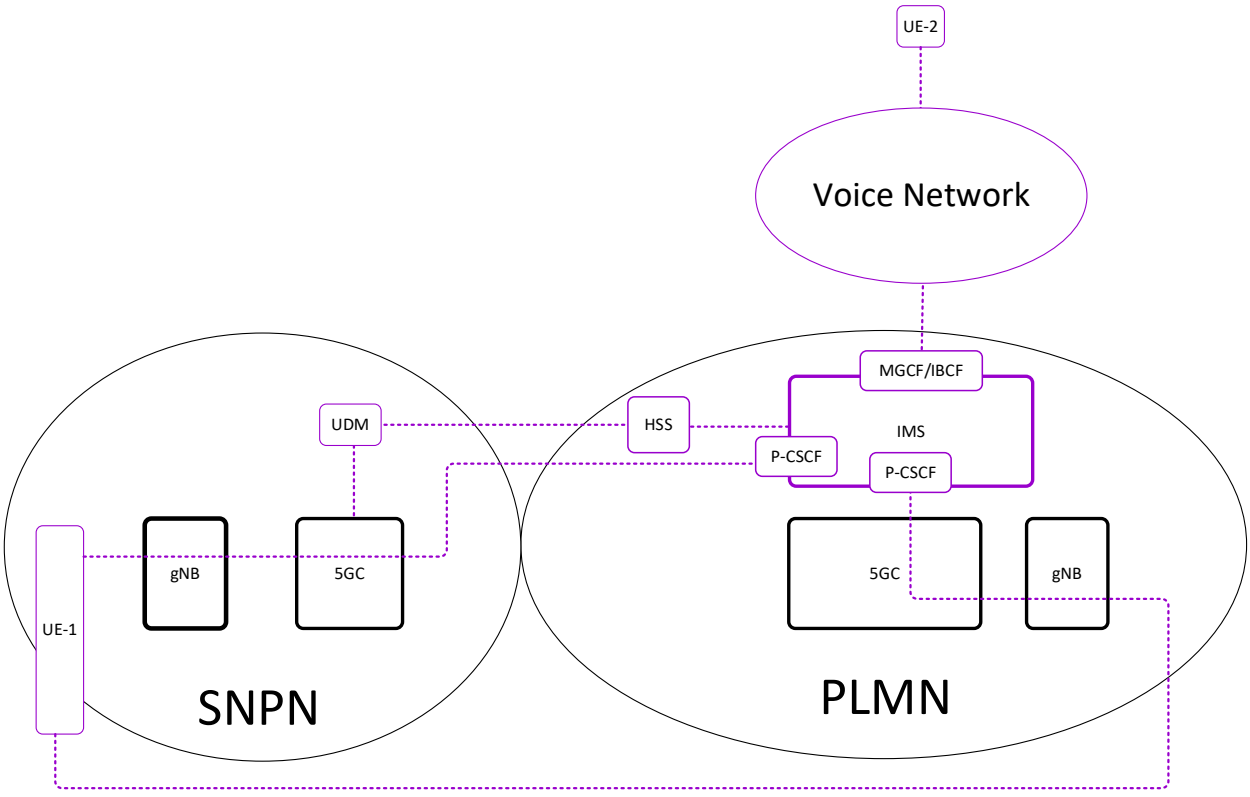

Figure A.6-1: PLMN-based IMS as third-party IMS

Figure A.6-1 shows that the PLMN IMS happens to be the third-party IMS that is used to provide the voice services for SNPN users. While serving the SNPN users as a third-party IMS, the PLMN IMS can be configured to allow the SNPN users (UE-1) to use abbreviated dialling plans for intra-SNPN sessions.

An SNPN user (UE-1) camping on a PLMN can be connected to the SNPN (not shown in Figure A.6-1 but shown in Figure A.5-1) via non-3GPP access (from the SNPN perspective) to get the same voice services provided by the PLMN IMS as a third-party IMS. Also, the SNPN user camping on the PLMN can be connected to the PLMN IMS (scenario of clause A.2 but shown in Figure A.6-1).

A.7 Conclusion

Method	SNPN Perspective	PLMN Perspective	UE Perspective
Option 1 (PLMN-based voice service)	• No voice service in SNPN. • For UEs camped onto SNPN, SNPN-to-PLMN connectivity is via NWu.	• PLMN-based voice services. • For UEs camped onto SNPN accessing the PLMN IMS, the ingress point is the N3IWF Gateway. • UE may also be camped onto the PLMN.	• SNPN UEs need PLMN subscription for voice services. • SNPN users may not be able to make use of abbreviated dialling plan for intra-SNPN sessions.
Option 2 (SNPN IMS with limited capability)	• SNPN has IMS with no connectivity to the external voice network. • Abbreviated dialling plan for intra-SNPN sessions are handled by the SNPN IMS TAS. • Only intra-SNPN sessions.	• Same as option 1.	• SNPN UEs need PLMN subscription for inter-SNPN sessions. • SNPN users can have abbreviated dialling plan.
Option 3 (SNPN IMA with full capability)	• SNPN has IMS with connectivity to the external voice network. • Abbreviated dialling plan for intra-SNPN sessions are handled by the SNPN IMS TAS.	• Not relevant, except that the SNPN users can still make use of the PLMN-based voice services as in the case option 1.	• SNPN users can have short-digit dial plan for intra-SNPN sessions. • If SNPN users also use PLMN-based voice services via a PLMN subscription, the users will have two distinct telephone numbers.
Option 4 (Third-party IMS)	• N6 reference point from SNPN 5GC to third-party IMS. • SNPN itself does not have the IMS.	• Not relevant, except that the SNPN users can still make use of the PLMN-based voice services as in option 1.	• SNPN users can have abbreviated dialling plan for intra-SNPN sessions.

			• If SNPN users also use PLMN-based voice services via a PLMN subscription, the users will have two distinct telephone numbers.
Option 5 (PLMN IMS as third-party IMS)	• N6 reference point from SNPN 5GC to PLMN IMS. • SNPN itself does not have the IMS.	• The SNPN users with a PLMN subscription for voice services can make voice calls while camped onto the PLMN or when connected to the PLMN services as in option 1.	• SNPN users can have abbreviated dialling plan for intra-SNPN sessions. • If SNPN users also use PLMN-based voice services via a PLMN subscription, the users may live with just one telephone number.

Table A.7-1: Summarizes the various cases illustrated in the previous clauses.

Annex B: SMS for SNPN

B.1 Background

SMS allows a mobile user to engage in a message communication with other users. This clause provides some background on SMS routing because it plays an important role in evaluating the available options for providing SMS to SNPN users.

The routing possibilities showing SMS over IP and SMS over NAS (5GC) are illustrated below:

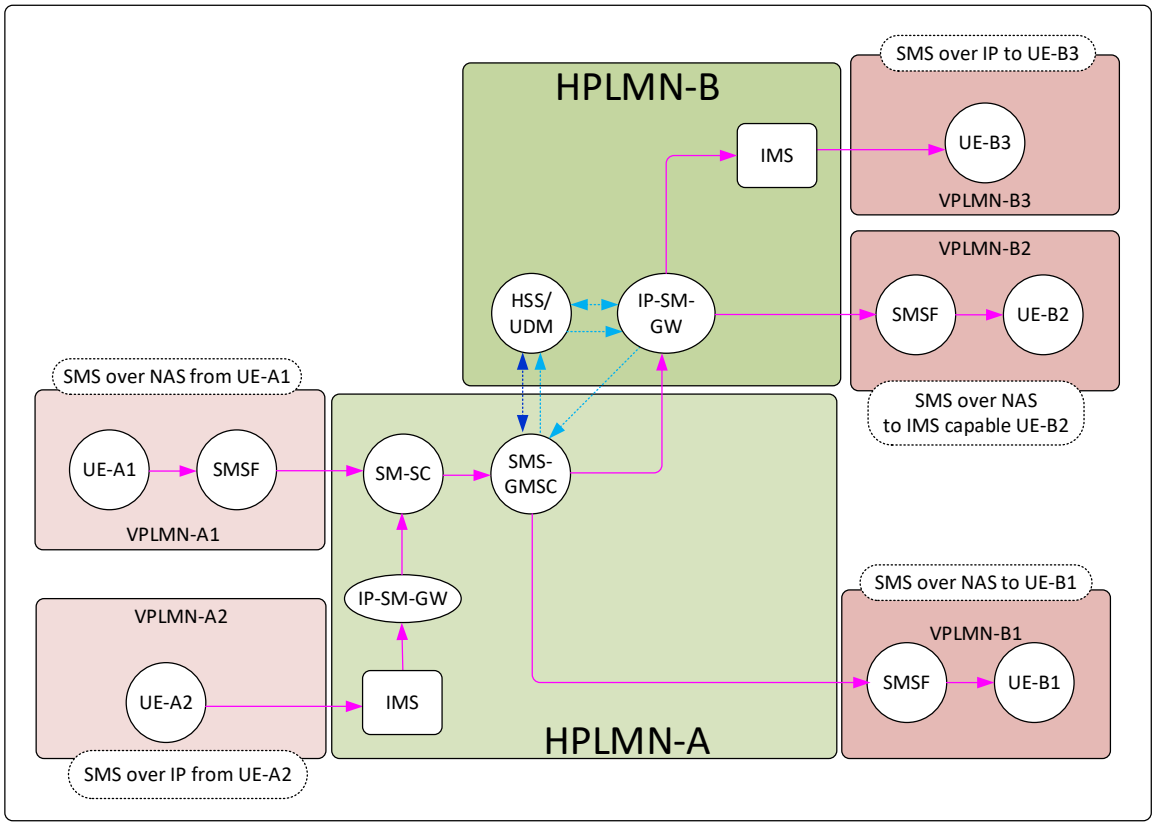

Figure B.1-1: Routing scenarios of SMS message

NOTE: The outbound roaming UEs shown in Figure B.1-1 are inside the HPLMN when not roaming.

Figure B.1-1 shows two cases of SMS originations (also referred to as Mobile-Originating (MO) SMS):

1) UE-A1 uses SMS over NAS.

2) UE-A2 uses SMS over IP.

HPLMN-A is the HPLMN of both UE-A1 (roaming in VPLMN-A1) and UE-A2 (roaming in VPLMN-A2).

Figure B.1-1 also shows three cases of SMS terminations (also referred to as Mobile-Terminating (MT) SMS):

1) SMS over NAS to UE-B1.
2) SMS over NAS to IMS-capable UE-B2 (provisioned to try SMS over NAS).
3) SMS over IP to UE-B3.

HPLMN-B is the HPLMN of UE-B1 (roaming in visited PLMN (VPLMN)-B1) and UE-B2 (roaming in VPLMN-B2) and UE-B3 (roaming in VPLNN-B3).

The SMS messages that originate from a UE are always sent to the SM-SC present in that UE's HPLMN. In other words, for an outbound roaming UE, the SMS messages that originate from the VPLMN always are routed to the SM-SC present in the HPLMN of that MO SMS UE. The SM-SC then forwards the SMS message to the SMS-GMSC present in the HPLMN of that MO SMS UE, which would interact with the HSS/UDM before routing the SMS message to the terminating UE (MT SMS UE).

The SMS over NAS is routed via the SMSF, whereas the SMS over IP is routed over IP-SM-GW of IMS. The MT SMS to IMS-enabled UE is routed through the IP-SM-GW either over SMSF or over IMS.

B.2 SMS and SNPN – Architectural Considerations

As described in clause B.1, the MO SMS are always routed to the SM-SC present in the HPLMN. To support this routing, every mobile UE must have a pre-configured SM-SC address. Operational aspect of SMS services available to SNPN users may depend on the location of the SM-SC, the address of which is pre-configured in the SNPN UEs. Furthermore, as Figure B.1-1 illustrates, for IMS-enabled UEs to support SMS over IP, the SM-SC will have to be present in the same network that provides the IMS functions.

SNPN UEs that are not IMS-enabled:

For non-IMS-capable SNPN UEs, the following three options can be possible:

- SM-SC in the SNPN only.
- SM-SC in the partnering PLMN only.
- SM-SC in the SNPN and in partnering PLMN.

In the last option, the SNPN UEs must have two pre-configured SM-SC addresses. In this case, the MO SMS would be routed to the appropriate SM-SC, depending on which network the SNPN UE is connected to. The SNPN UEs will must have two telephone numbers if the SM-SC present in the SNPN has external connectivity. When the SM-SC present in the SNPN does not have external connectivity, the SNPN users can exchange SMS with the external users only when connected to the partnering PLMN.

When the SM-SC is in the partnering PLMN only, the SNPN may or may not have the SMSF. When the SNPN has an SMSF, the HSS in the partnering PLMN has to interact with the UDM present in the SNPN to determine the SMSF that serves the SNPN UE. When the SNPN does not have the SMSF, the SNPN users may use the SMS services only when connected to the PLMN.

Similar considerations apply when the SM-SC is in the SNPN only.

SNPN UEs that are IMS-enabled:

For SMS over IP, the SM-SC should be present in the same network that has the IMS. As illustrated in Annex A, the following possibilities have to be considered:

- SNPN does not have an IMS, so PLMN IMS is used.
- SNPN does not have an IMS, so third-party IMS is used.
- SNPN has an IMS with no external connectivity.
- SNPN has an IMS with external connectivity.

The above options lead to SM-SC being present in the PLMN, or in the third-party network, or in the SNPN. When IMS is present in the SNPN or in the third-party IMS, the IMS-enabled SNPN UEs will have to have two pre-configured SM-SC addresses, along with two telephone numbers to access SMS services while connected to the PLMN.

When SMS over NAS is used for IMS-enabled SNPN UEs, the SM-SC address pre-configured in the SNPN UEs can be in the PLMN, SNPN, or third-party IMS network domain, depending on which of the above listed IMS options is used for SNPN. When PLMN IMS is used, SMSF may or not be present in the SNPN. When the third-party IMS is used or SNPN IMS is used, the SNPN should always have the SMSF.

B.3 Topology Views for SMS over NAS

B.3.1 PLMN-Based SMS

In this option, the SM-SC — the address of which is pre-configured in the SNPN UEs — is in the partnering PLMN.

Scenario 1: SNPN does not have an SMSF deployed.

From a PLMN's perspective, the user's device is either camping on the PLMN or, if camping on the SNPN, then connected to the PLMN via non-3GPP access.

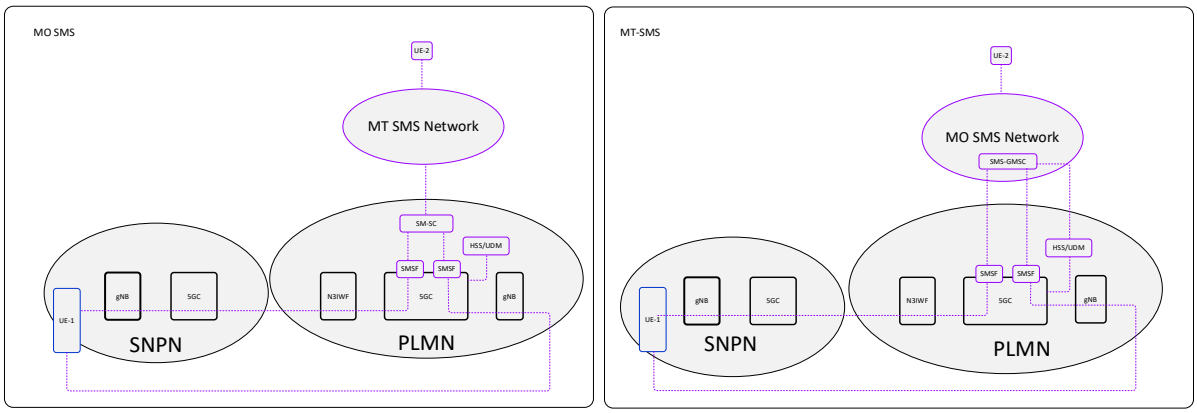

Figure B.3.1-1: PLMN-based SMS services; SNPN has no SMSF

Figure B.3.1-1 shows two ways the UE-1 can use PLMN-based SMS:

1) Camping on the SNPN but connected to PLMN via the N3IWF Gateway located in the PLMN (which is called non-3GPP access from a PLMN perspective).
2) Camping directly on the PLMN network.

To allow for such a scenario, the SNPN user needs a PLMN subscription.

Scenario 2: SNPN has an SMSF deployed.

From a PLMN's perspective, the SNPN user's device is either camping on the PLMN or, if camping on the SNPN, then the SNPN SMSF address is determinable through HSS-UDM interaction.

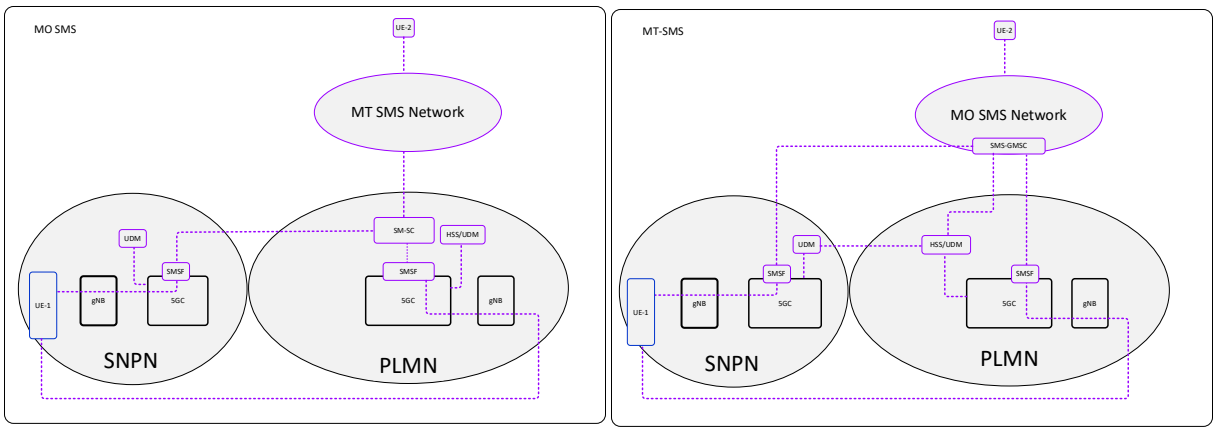

Figure B.3.1-2: PLMN-based SMS services; SNPN has an SMSF

Figure B.3.1-2 shows two ways the UE-1 can use PLMN-based SMS without connecting to the PLMN via non-3GPP access (e.g., N3IWF).

In routing the MT SMS, the HSS in the PLMN will have to interact with the UDM to determine the SMSF address.

B.3.2 SNPN has SM-SC without External Connectivity

With this option, an SNPN user connected to access SNPN services will be allowed to engage in SMS-based message communications only within the SNPN. For SMS involving users outside the SNPN, the SNPN user will have to be connected to the PLMN to use SMS, as shown in Figure B.3.2-1.

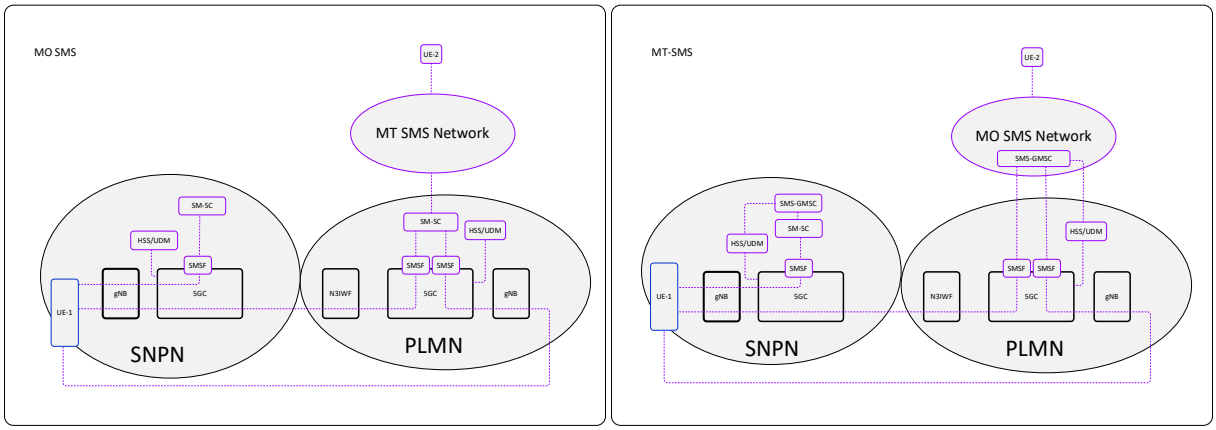

Figure B.3.2-1: SNPN has SM-SC with no external connectivity

Figure B.3.2-1 shows two ways the UE-1 can use SMS:

1) While camping on the SNPN send/receive SMS to other users within the SNPN
2) While connected to PLMN (there are two ways as shown in Figure B.3.2-1).

In this option, the SNPN UE shall have two preconfigured SM-SC addresses.

B.3.3 SNPN has SM-SC with External Connectivity

With this option, an SNPN user connected to access SNPN services will be allowed to engage in SMS-based communications within the SNPN or outside the SNPN.

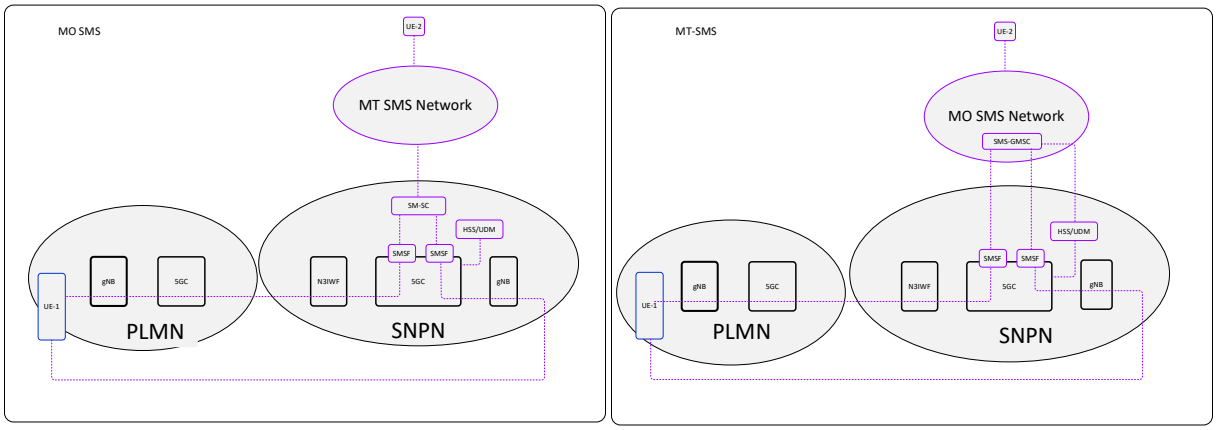

Figure B.3.3-1: SNPN has SM-SC with external connectivity

Figure B.3.3-1 is similar to the case shown in Figure B.3.1-1, with SNPN and PLMN roles reversed.

1) Camping on the PLMN but connected to SNPN via N3IWF Gateway located in the SNPN (which is called non-3GPP access from a SNPN perspective).
2) Camping directly on the SNPN network.

For the SNPN user to use PLMN-provided SMS, a separate telephone number will be needed, with the UE pre-configured with two SM-SC addresses (see clause B.3.4).

B.3.4 Two SM-SC Addresses and Two Telephone Numbers to SNPN UEs

With this option, an SNPN user while connected to access SNPN services will be allowed to engage in SMS-based message communications within the SNPN or outside the

SNPN via SNPN SM-SC, and while connected to access PLMN services will be allowed to engage in SMS-based message communications via PLMN SM-SC.

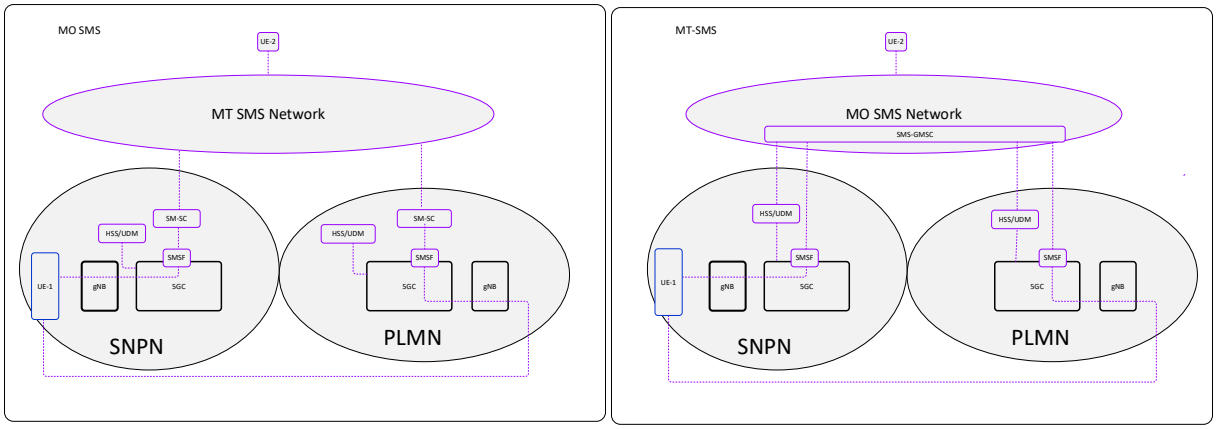

Figure B.3.4-1: SNPN has SM-SC with external connectivity

Figure B.3.4-1 shows that handling of SMS for an SNPN UE depends on which network the UE is connected to.

The SNPN UEs shall have two telephone numbers and shall be pre-configured with two SM-SC addresses.

B.4 Topology Views for SMS over IP

B.4.1 Overview

The following sub-clauses show the routing of SMS for IMS-enabled SNPN UEs with SMS over IP as the preferred option.

B.4.2 PLMN-based IMS

In this option, from a PLMN's perspective, the user's device is either camping on the PLMN or, if camping on the SNPN, then connected to the PLMN via non-3GPP access.

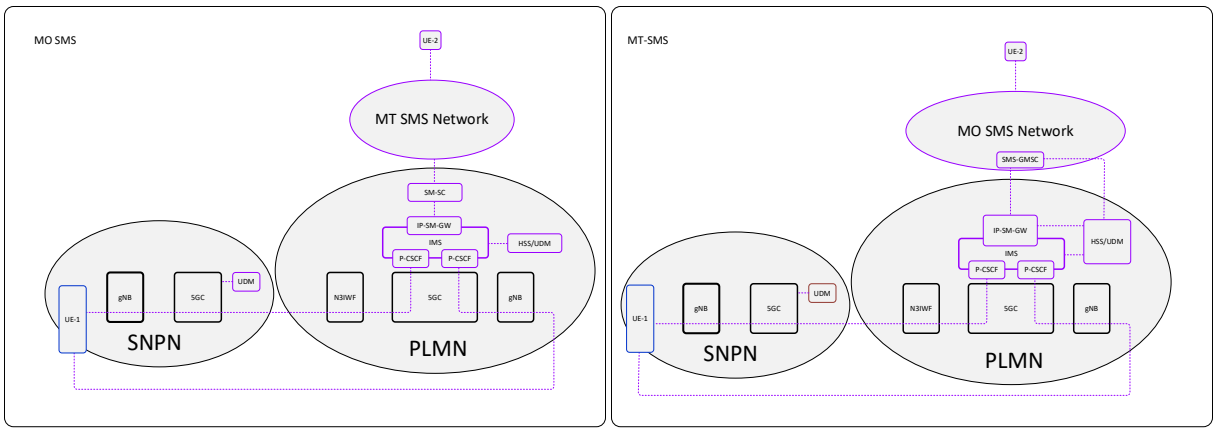

Figure B.4.2-1: PLMN-based IMS

Figure B.4.2-1 shows two ways the UE-1 can be connected to PLMN-based IMS:

1) Camping on the SNPN but connected to PLMN via the N3IWF Gateway located in the PLMN (which is called non-3GPP access from a PLMN perspective)
2) Camping directly on the PLMN network.

To allow for such a scenario, the SNPN user needs a PLMN subscription. The SNPN UEs will have the pre-configured address of SM-SC located in the PLMN.

B.4.3 SNPN-based IMS with limited capabilities

With this option, an SNPN user while connected to access SNPN services will be allowed to engage in SMS-based message communications only within the SNPN. For SMS involving the users outside the SNPN, the SNPN user will have to be connected to the PLMN to use SMS, as shown in Figure B.4.3-1.

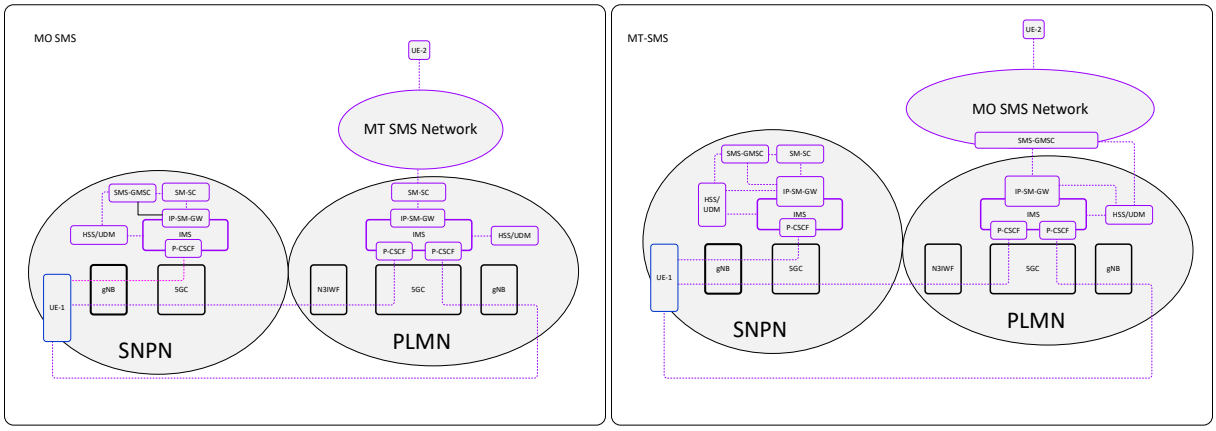

Figure B.4.3-1: SNPN-based voice services with limited capabilities

In this option, the SNPN UE shall have two pre-configured SM-SC addresses.

B.4.4 SNPN-based IMS with full capabilities

With this option, an SNPN user while connected to access SNPN services will be allowed to be engaged in SMS-based message communications within the SNPN or outside the SNPN.

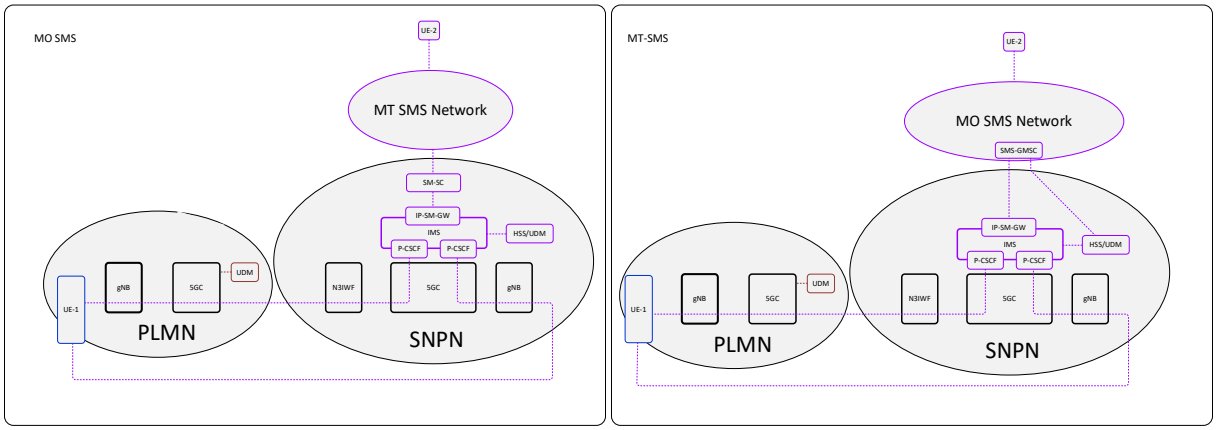

Figure B.4.4-1: SNPN-based IMS with full capabilities

The option is similar to the case shown in Figure B.4.2-1, with SNPN and PLMN roles reversed. For the SNPN user to use PLMN-provided SMS, a separate telephone number will be needed, with the UE pre-configured with two SM-SC addresses.

B.4.5 Third-Party-Based IMS

With this option, an SNPN user while connected to access SNPN services will be allowed to engage in SMS-based message communications with another SNPN user within the same SNPN or another user outside the SNPN. The difference between this option and the option shown in Figure B.4.4-1 is that here the IMS is provided by a third party.

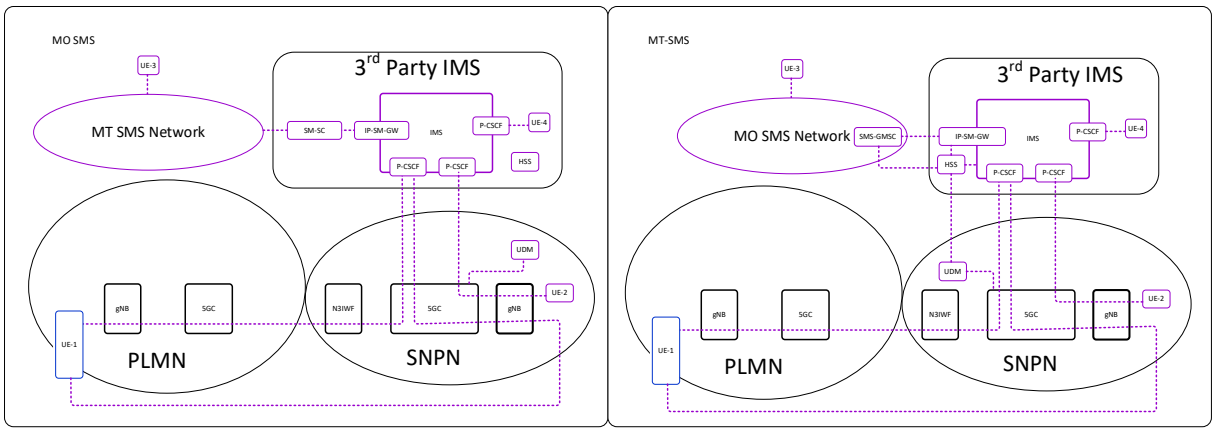

Figure B.4.5-1: Third-party-based IMS

For the SNPN user to use PLMN-provided SMS, a separate telephone number will be needed, with the UE pre-configured with two SM-SC addresses.

B.4.6 PLMN-Based IMS as Third-Party IMS

With this option, an SNPN user while connected to access the SNPN services will be allowed to engage in SMS-based message communications with another SNPN user within the same SNPN or another user outside the SNPN. The difference between this option and the option shown in Figure B.4.5-1 is that here the IMS is provided by the PLMN, which the SNPN views as a third party.

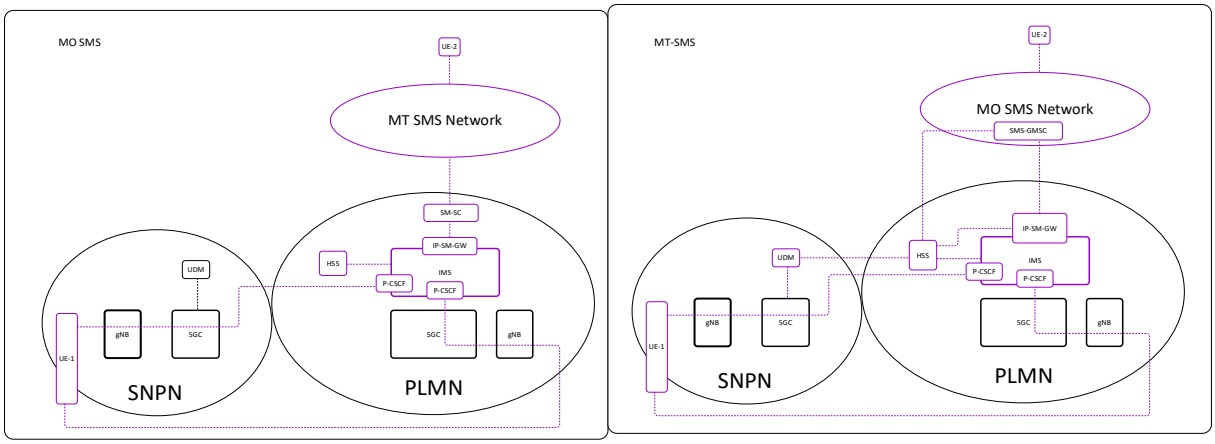

Figure B.4.6-1: PLMN-based IMS as third-party IMS

An SNPN user camping on the PLMN can be connected to the PLMN IMS. In this option, the SNPN UE is pre-configured with one SM-SC address, and SNPN users will have one telephone number.

B.5 SMS over NAS for IMS-Enabled UEs

The MO SMS from SNPN UEs are routed from the SMSF to the SM-SC, as illustrated in the topology views of clause B.3.

The MT SMS will be routed from the SMS-GMSC present in the originating network through the IP-SM-GW present in the IMS network over SMSF to the SNPN UE.

SM-SC is located in the IMS network domain.

Figure B.5-1 shows one topology view when third-party IMS is used.

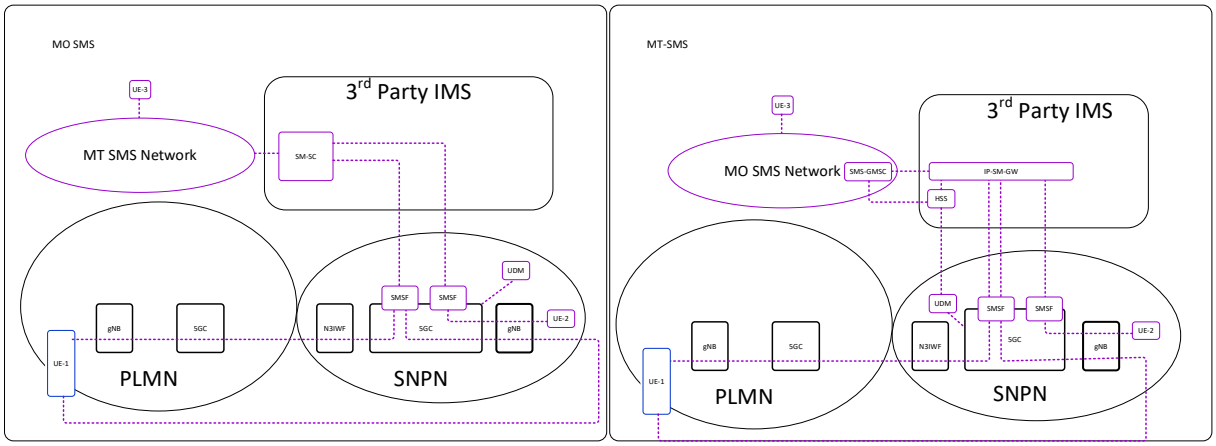

Figure B.5-1: Third-party-based IMS; SMS over NAS for IMS-enabled SMS UE

In Figure B.5-1, the SM-SC is in the third-party IMS network domain. The MO SMS is routed from the SMSF present in the SNPN to the SM-SC.

The MT-SMS is routed from the SMS-GMSC through the IP-SM-GW over SMSF present in the SNPN. The HSS present in the third-party IMS shall interact with the UDM present in the SNPN to determine the SMSF address for MT SMS.

B.6 Conclusion

Method	SNPN Perspective	PLMN Perspective	UE Perspective
Option 1 (PLMN-based SMS over IP)	• No SMS over IP support in SNPN. • For UEs camped onto SNPN, SNPN-to-PLMN connectivity is via NWu.	• PLMN provides the SMS services to SNPN UEs. • For UEs camped onto SNPN accessing the PLMN IMS, the ingress point is the N3IWF Gateway. • UE may also be camped onto the PLMN.	• SNPN users need PLMN subscription to use SMS. • SNPN UEs are pre-configured with PLMN SM-SC address. • SNPN UEs have to register with the PLMN IMS to use SMS.
Option 2 (SNPN IMS with limited capability)	• SNPN has IMS with no connectivity to the external network. • Intra-SNPN SMS messages are handled in the SNPN.	• Same as option 1 for SNPN UEs registered to the PLMN IMS.	• SNPN users need PLMN subscription for SMS outside the SNPN domain. • SNPN UEs need to be pre-configured with two SM-SC addresses (PLMN SM-SC and SNPN SM-SC). • SNPN UEs have to be registered to the PLMN IMS to use SMS outside the SNPN domain.
Option 3 (SNPN IMS with full capability)	• SNPN has IMS with connectivity to the external voice network. • SMS over IP can be provided by the SNPN.	• Not relevant, except that the SNPN users can still make use of the PLMN-based SMS as in the case option 1.	• If PLMN-provided SMS is to be used (via PLMN subscription), then SNPN UEs have to be pre-configured with two SM-SC addresses (PLMN SM-SC and SNPN SM-SC) and such SNPN UEs need to have two telephone numbers.
Option 4 (Third-party IMS)	• N6 reference point from SNPN 5GC to third-party IMS. • SNPN itself does not have the provide the SMS over IP.	• Not relevant, except that the SNPN users can still make use of the PLMN-based SMS services, as in the case option 1.	• SNPN UEs are pre-configured with third-party IMS domain SM-SC address. • If PLMN provided SMS is to be used (via PLMN subscription), then SNPN UEs have to be pre-configured also with the PLMN SM-SC address and such SNPN UEs need to have two telephone numbers.

Option 5 (PLMN IMS as third-party IMS)	• N6 reference point from SNPN 5GC to PLMN IMS. • SNPN itself does not provide the SMS over IP.	• PLMN provides the SMS services to the SNPN UEs.	• SNPN users have one pre-configured SM-SC address and one telephone number even if PLMN-based SMS services are used via PLMN subscription.

Table B.6-1: Summarizes the SMS over NAS cases.

Method	Network Configuration	IMS Capable UE	Non-IMS-Capable IE
Option 1	• SNPN has no SM-SC. • SNPN has no IMS. • SNPN has no SMSF. • PLMN IMS is used. • PLMN SM-SC is used.	• SNPN users need PLMN subscription to use SMS. • SNPN UEs are pre-configured with PLMN SM-SC address. • SNPN UEs have to be registered to the PLMN IMS to use SMS over IP. • SNPN UEs have to connected to PLMN to use SMS over NAS.	• SNPN users need PLMN subscription to use SMS. • SNPN UEs are pre-configured with PLMN SM-SC address. • SNPN UEs have to connected to PLMN to use SMS.
Option 2	• SNPN has no SM-SC. • SNPN has SMSF. • SNPN has no IMS. • PLMN IMS is used. • PLMN SM-SC is used. • SNPN UDM and PLMN HSS has connectivity.	• SNPN users need PLMN subscription to use SMS. • SNPN UEs are pre-configured with PLMN SM-SC address. • SNPN UEs have to be registered to the PLMN IMS to use SMS over IP. • SNPN UEs can have SMS over NAS without connecting to the PLMN.	• SNPN users also need PLMN subscription to use SMS. However, SNPN UEs can have SMS services without connecting to the PLMN. • SNPN UEs are pre-configured with PLMN SM-SC address.
Option 3	• SNPN has SM-SC with no external connectivity • SNPN has IMS with no external connectivity. • SNPN has SMSF. • SNPN UDM and PLMN HSS has connectivity.	• SNPN users need PLMN subscription for SMS outside the SNPN domain. • SNPN UEs need to be pre-configured with two SM-SC addresses (PLMN SM-SC and SNPN SM-SC). • SNPN UEs have to be registered to the PLMN IMS to use SMS	• SNPN users need PLMN subscription for SMS outside the SNPN domain. However, SNPN UEs can have SMS outside the SNPN domain without connecting to the PLMN. • SNPN UEs are pre-configured with two SM-SC addresses

		over IP outside the SNPN domain. • SNPN UEs can have SMS over NAS outside the SNPN domain without connecting to the PLMN.	(PLMN SM-SC and SNPN SM-SC).
Option 4	• SNPN has SM-SC with external connectivity • SNPN has IMS with external connectivity. • SNPN has SMSF.	• If PLMN-provided SMS is to be used (via PLMN subscription), then SNPN UEs have to be pre-configured with two SM-SC addresses (PLMN SM-SC and SNPN SM-SC), and such SNPN UEs need to have two telephone numbers.	• If PLMN-provided SMS is to be used (via PLMN subscription), then SNPN UEs have to be pre-configured with two SM-SC addresses (PLMN SM-SC and SNPN SM-SC), and such SNPN UEs need to have two telephone numbers.
Option 5	• SNPN has no SM-SC. • SNPN has SMSF. • Third-party IMS is used. • SNPN UDM and HSS in third-party IMS domain has connectivity.	• SNPN UEs are pre-configured with third-party IMS domain SM-SC address. • If PLMN-provided SMS over IP is to be used (via PLMN subscription), then SNPN UEs have to be pre-configured also with the PLMN SM-SC address, and such SNPN UEs need to have two telephone numbers.	• SNPN users also need PLMN subscription to use SMS. However, SNPN UEs can have SMS services without connecting to the PLMN. • SNPN UEs are pre-configured with PLMN SM-SC address.

Table B.6-2: Summarizes the SMS over IP cases