VIRTUAL EXPERIENCE
OCTOBER 11-14

2021 Fall Technical Forum
SCTE • NCTA • CABLELABS

New Service Paradigm With 5G Private Network

A Technical Paper prepared for SCTE by

Curt Wong
Sr. Dir – Wireless Standards, R&D
Charter Communications, Inc
6360 S Fiddlers Green, Greenwood Village, CO 80111
425-395-4379
Curt.Wong@Charter.com

Yildirim Sahin
Director – Wireless Standards, R&D
Charter Communications, Inc
6360 S Fiddlers Green, Greenwood Village, CO 80111
720-536-9394
yildirim.sahin@charter.com

Deh-Min Richard Wu
Director – Wireless Standards, R&D
Charter Communications, Inc
6360 S Fiddlers Green, Greenwood Village, CO 80111
256-763-1202
deh-minrichard.wu@charter.com

Umamaheswar Achari Kakinada
Director – Wireless Standards, R&D
Charter Communications, Inc
6360 S Fiddlers Green, Greenwood Village, CO 80111
847-544-6560
Achari.Kakinada@charter.com

Table of Contents

Title **Page Number**

List of Figures

Title **Page Number**

1. Introduction

Traditionally, a universal subscriber identity module (USIM) and roaming agreement between the serving network (visited public land mobile network (PLMN)) and home network (home PLMN) is needed in order for the user equipment (UE) to gain access to normal services (i.e., data/voice) when roaming. This type of "control" has been a long tradition used within the mobile network operators (MNO) to control which roaming network that their subscribers are authorized to gain services using 3GPP radio access technologies (RAT). With the ongoing development of 5G private network in the 3GPP ecosystem, a new service paradigm with 5G standalone architecture (5G SA) and 3GPP RAT is being created. USIM (or eSIM) are no longer the only storage mechanism for credentials when using 3GPP RAT. Onboarding can be performed locally for non-initialized UE to access the network. UE credential storage at the network side can be separated from the network that is providing the access to the users. And overall, the 5G private network can take advantage of the native support for edge computing to allow service hosting environment to be locally deployed for services with ultra-low latency and better quality of experience (QoE).

This paper first describes in a high level on how a UE obtains services with the current 4G cellular networks to contrast with the new capabilities offered with 5G private networks (also known as Stand-alone non-public network (SNPN)[1] [2]). These new capabilities defined by 3GPP 5G system architecture standards for SNPN set a course for a new service paradigm possibility for 5G private networks.

2. Services Provided By The Current Cellular Networks

Nowadays, a typical service provided by the cellular networks is mainly a best effort bit pipe connecting the UE to the external data networks (i.e., the Internet). When the bit pipe is characterized as best effort or non-guaranteed bit rate, it means that everyone shares the available bandwidth within the network and in some cases the user may exhibit congestion where the QoE became unsatisfactory.

Some services like real-time voice or public safety related services can be tailored by the network by setting the quality of service (QoS) parameters for that the bit pipe. This requires the network to be aware of at least two properties: 1) who is using the network, and 2) the type of QoS for which the user is eligible.

[1] SNPN is defined by 3GPP. Another type of 5G private network called public network integrated non-public network which is not described in this paper.

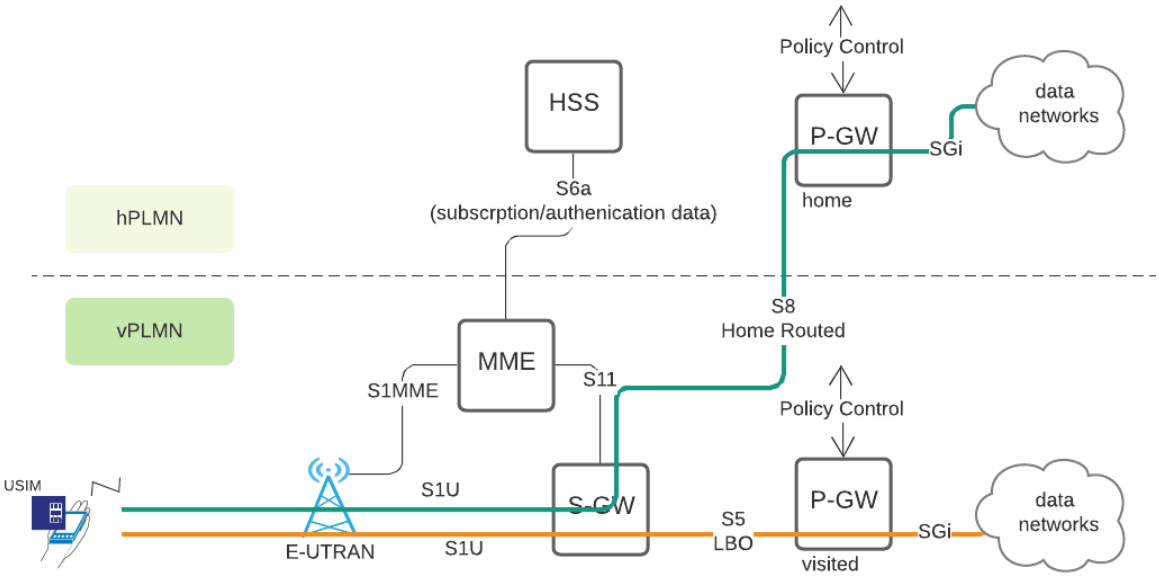

Figure 1 – Simplied EPS Architecture With Roaming Interfaces Illustrated

To determine who is using the network, a USIM with mutual authentications is used between the UE and the vPLMN. This requires the vPLMN to obtain the authentication vectors from the user's home (i.e., hPLMN) in order to perform mutual authentications with the USIM. With this requirement, a user must somehow obtain a USIM from a hPLMN before a cellular service can be rendered. In addition, a business relation (i.e., roaming relation) between vPLMN and hPLMN is needed in order to fetch the authentication vectors from hPLMN.

In the roaming example shown in figure 1, the UE has two protocol data network (PDN) connectivity services established from the vPLMN. The user's subscription in the home subscriber server (HSS) indicates that S8 home routed for internet traffic is used and local breakout (LBO) is used for e.g., voice media with IP-multimedia subsystem (IMS). Effectively, this means one user plane tunnel is breaking out locally at the vPLMN while the other is routed back to hPLMN.

The type of PDN connectivity service allowed (and their associated QoS profile) is based on user subscription data from hPLMN (but can be modified by the vPLMN if dynamic policy control is used).

The following list shows the QoS parameters related to each PDN connection:

- QoS class identifier (QCI) – a scalar that points to a set bearer level packet forwarding treatment (delay budget, packet loss, scheduling priority, etc.).
- Allocation and retention priority (ARP) – for admission related criteria during congestion with priority level (scalar), the pre-emption capability (flag) and the pre-emption vulnerability (flag).
- Guaranteed bit rate (GBR) (as oppose to the best effort).
- Maximum bit rate (MBR) – the upper limit of the bit rate that is expected to be provided by a bearer.
- Access Point Name Aggregate Maximum Bit Rate (APN-AMBR) – to limit the aggregate bit rate that can be expected to be provided across all non-GBR bearers and across all PDN connections of the APN.

- UE Aggregate Maximum Bit Rate (UE-AMBR) – to limit the aggregate bit rate that can be expected to be provided across all non-GBR bearers of a UE.

3. Why 5G Private Network Is Different?

As described in the previous section, a user who is able to obtain connectivity service in a vPLMN must first have a prior relationship with a hPLMN and that both vPLMN and hPLMN must have roaming relationship with each other in order to allow the vPLMN to authenticate the user and to obtain the subscription information for QoS settings and for user plane routing between the UE and the networks.

For 5G private networks – namely SNPN, it is neither necessary to use USIM to gain access to local access network using 3GPP RAT nor that a roaming interface is required from the SNPN in order to reach hPLMN.

3GPP SNPN [2] offers the following new capabilities which are different from technologies used for prior cellular services described in the early section.

- Subscriber identifier (SUPI) is no longer restricted to IMSI. Network access identifier (NAI) using the NAI RFC 7542 based user identification (e.g., lux_luther@phantom.zone) can be defined and used.
- Mutual authentication is no longer restricted with the shared secret stored in the USIM. Extensible authentication protocol (EAP) with TLS/TTLS can be used (e.g., certificate, username/password) as well. The credentials can be stored in the device itself as well.
- SNPN is identified with the addition of NID (Network identifier) – i.e., PLMN ID + NID. PLMN ID is not required to be unique. It the traditional cellular network, PLMN ID (i.e., MCC and MNC pair) is assigned by either ITU or regional organization like ATIS IOC (IMSI Oversight Council) and is globally unique. For SNPN using MCC with 999 [1] any MNC and also any NID can be used. Operator can also choose to use its own dedicated PLMN ID plus any self-managed NID value as deployment choice. In addition, 3GPP allows the option of using a globally unique NID value independent of the PLMN ID.
- NG-RAN may also broadcast a human-readable network name to ease the user to select SNPN. This is mainly used for manual selection based on network name awareness of the user.
- Onboarding service allows a UE without any prior relationship (i.e., no credential to access the network) to obtain the necessary authorization and credentials on demand from a local SNPN.
- Authentication vectors can be stored externally from SNPN (e.g., in an external AAA server, other UDM from 3rd party) to allow neutral hosts type of deployment.
- Accessing to hPLMN service via SNPN is also possible with untrusted access procedure over 3GPP RAT.

Please note that real time voice communication and emergency session can also be supported with SNPN toward the local PSTN.

The following figure illustrates an example of a simplified SNPN architecture.

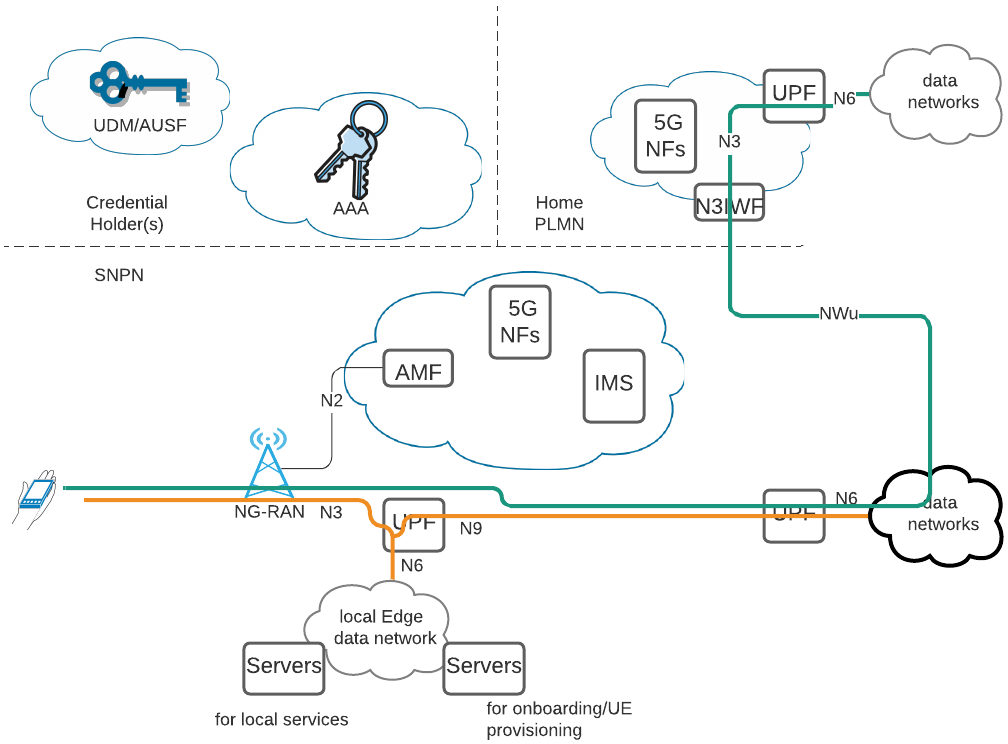

Figure 2 – Simplied SNPN Architecture With User Plane Routing For Different Services

The following section describes some of the key capabilities [2] [3] with more details using SNPN that is differed from PLMN.

3.1. UE Onboarding

Onboarding is the service to allow a non-provisioned UE to obtain SNPN credentials in order to get connectivity service from the SNPN.

The following figure shows a simplified view on how a non-initialized UE is provisioned with SNPN credentials.

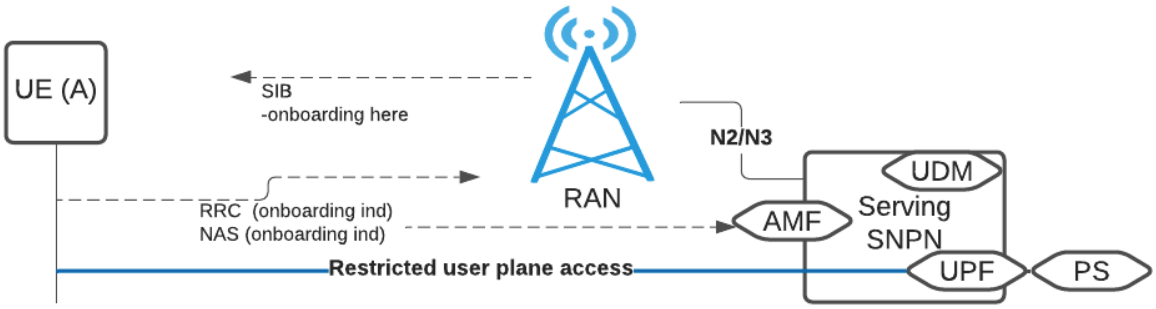

Figure 3 – Onboarding Process For A Non-initialized UE.

The SNPN which allows onboarding process will broadcast an indication at the cell level that onboarding is supported. UE, which wants to be provisioned with SNPN credentials for connectivity service from the SNPN, will signal to the network with onboarding indication in both radio resource control signaling (RRC) and non-access stratum signaling (NAS). This allows the RAN to forward this request from the UE to a dedicated onboarding access and mobility management function (AMF). AMF uses the NAS level indication to select a session management function (SMF) used for remote provisioning and to setup a restricted user data plane between the UE and the provisioning server (PS). The SMF may send the PS fully qualified domain name (FQDN) to the UE as part of protocol configuration options (PCO) in the PDU session establishment response. After PDU session is set up, the application in the UE is then interacting with the PS to obtain the SNPN credentials. The PS may request certain information from the UE/user (e.g., name, type of connectivity services requested, credit card, etc.) prior to sending the SNPN credentials to the UE. The PS may also provision the UDM with corresponding SNPN subscription data if it has not been prefilled already. The applications in the UE for handling provisioning task is out of scope of 3GPP standards and is left for OEM implementation.

Once the UE has received the SNPN credentials from the PS, it will restart and use the downloaded SNPN credential to access the network.

3.2. Access to SNPN With Credentials Owned By An Entity Separate From The SNPN

Credentials holder is defined in 3GPP [2] as an entity which authenticates and authorizes access to an SNPN separate from the credentials holder. It means that the serving SNPN does not store the credentials that can be used to authenticate/authorize the UE. This is also commonly known as neutral host offering as it allows the SNPN to provide connectivity service to the users using credentials from 3rd party.

The following simplified figure shows how a serving SNPN interacts with credential holders.

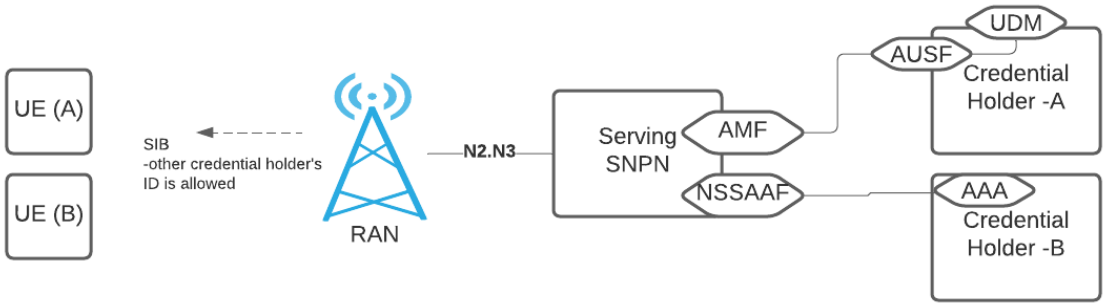

Figure 4 – SNPN Interacting With Credential Holders

The following figure shows two 5G architecture views from 3GPP TS 23.501 [2] with credentials holder and SNPN.

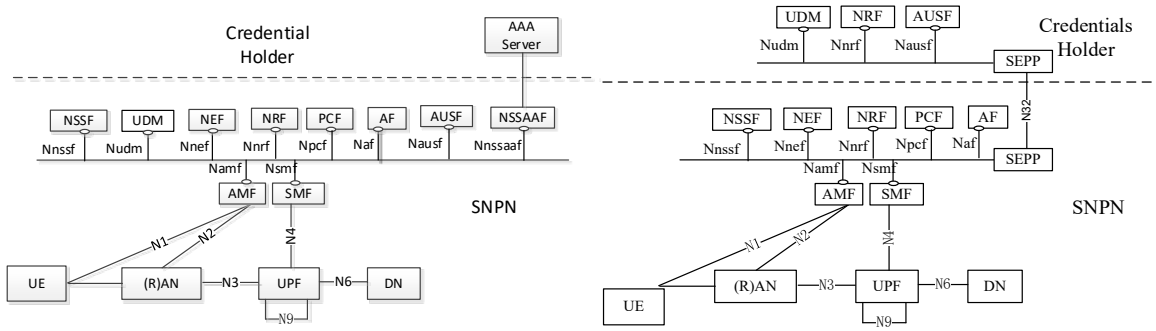

Figure 5 – SNPN and Credential Holder From 3GPP TS 23.501

Please note that from 3GPP's point of view, the architecture for SNPN and credentials holder is always depicted as a non-roaming reference architecture even though a roaming reference point (i.e., N32) is used. In this sense, the 3GPP does not support roaming for UE between SNPN and MNO.

When accessing a SNPN with credentials from 3rd party (credential holder), the UE must first check the system information block (SIB) broadcast message from the RAN to determine which 3rd party (credential holder) is supported by this SNPN. This could be in the form of a list of PLMN ID + NID or group ID (GIN) for network selection. GIN represents a group of 3rd parties using a common Network ID to minimize the broadcast list in the SIB. If the UE has been configured with a credential from one of those 3rd parties that is shown in the SIB then the UE may proceed to register to the SNPN using the 3rd party credential.

RAN may also broadcast an additional indication in the SIB to indicate that UE with any 3rd party (credential holder) information can try to access this SNPN. This type of uncontrolled access may be useful for general public usage (e.g., public access at the park, public library, etc.).

Credential holder can be from another SNPN or PLMN or from enterprise domain in the case of AAA.

If the credential information is stored in 3rd party UDM, AMF in SNPN forwards the EAP message to the AUSF of the 3rd party based on PLMN ID + NID received from the UE.

If the credential information is stored in an AAA Server in the credential holder, the authentication function (AUSF) in SNPN selects a network slice-specific and SNPN authentication and authorization function (NSSAAF) to handle the related EAP messages from the UE. The NSSAAF selects AAA server based on the domain name to the realm part of the SUPI, relays EAP messages between AUSF and AAA server (or AAA proxy) and performs related protocol conversion. The AAA server acts as the EAP server for the purpose of primary authentication. UDM is still used for storing subscription information and to decide that the primary authentication is performed by AAA or AUSF.

3.3. Accessing PLMN Services From SNPN

Interesting enough that even when 3GPP does not support roaming between SNPN and PLMN, the specification does allow a UE with dual credentials (e.g., similar to dual SIM dual standby (DSDS) or dual SIM dual active (DSDA)) to access both SNPN and PLMN services at the same time. This is particularly useful when a user wants to separate their usage between enterprise and personal domains or when the user is in a remote SNPN environments like caves or shielded factory where PLMN coverage is not available or accessible.

3GPP defines the following terms to cover this usage:

- Overlay network: When UE is accessing SNPN service via NWu using user plane established in PLMN, SNPN is the overlay network. When UE is accessing PLMN services via NWu using user plane established in SNPN, PLMN is the overlay network.
- Underlay network: When UE is accessing SNPN service via NWu using user plane established in PLMN, PLMN is the underlay network. When UE is accessing PLMN services via NWu using user plane established in SNPN, SNPN is the underlay network.

The following figure illustrate this architecture setup using hPLMN as overlay as an example. Please note that the other direction is also valid (i.e., accessing SNPN via PLMN's 3GPP RAT) but is not used here for illustration.

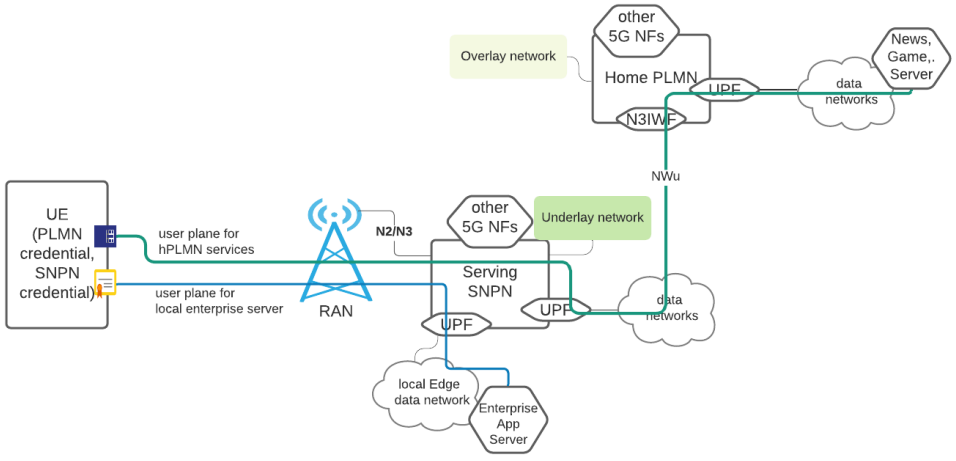

Figure 6 – Accessing HPLMN Services Via SNPN

The UE has both the SNPN credential and the PLMN credential. The enabler here is that the UE is able to use the untrusted non-3GPP access procedure over the 3GPP RAT of the SNPN in order to create a NWu

tunnel toward the hPLMN. The SNPN credential is needed in order to get access to the data network via SNPN. The PLMN credential is needed in order to access the hPLMN via the NWu tunnel.

On the SNPN side, UE maintains at least one PDU session in the network that can reach the N3IWF of the hPLMN, and UE keeps its state in CM-CONNECTED state as if the UE is using WiFi access.

From hPLMN's perspective, UE is accessing the hPLMN as if the UE is using any WiFi access even though the UE is actually using 3GPP RAT from SNPN.

When UE is moving out of the SNPN coverage and into the 3GPP radio coverage of the hPLMN, the user data session can also be transferred from SNPN to hPLMN using non-3GPP to 3GPP handover procedures as described in 3GPP specifications. In other words, when UE has detected that the radio coverage of the PLMN is sufficient, it can initiate a registration procedure to the hPLMN with an indication that an existing user plane session from NWu needs to be moved over to this 3GPP radio interface. In the figure below, the data carried via green path will be moved to blue path after this handover procedure is completed.

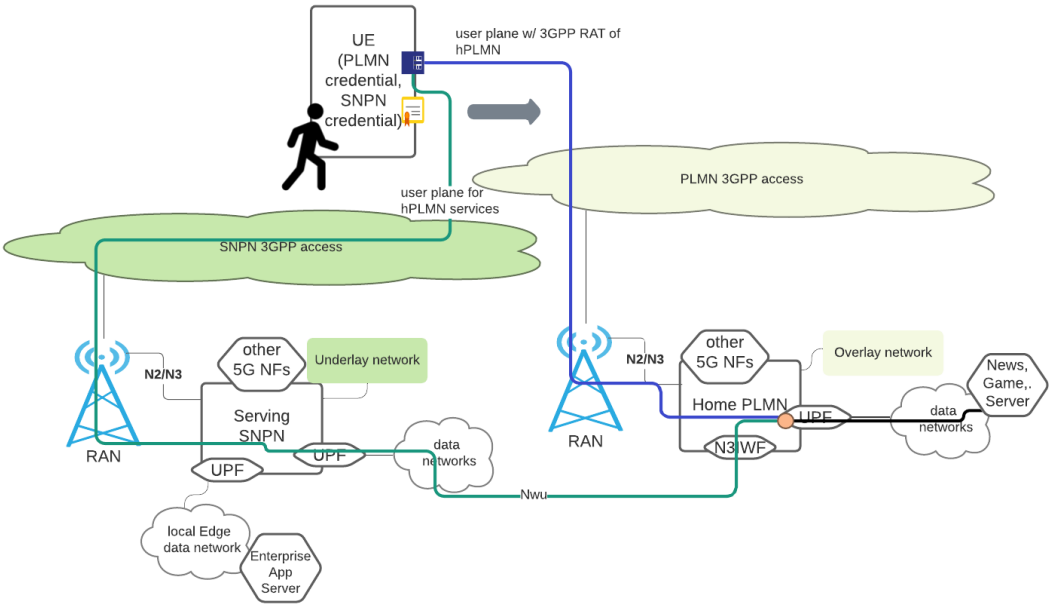

Figure 7 – Mobility Into PLMN's 3GPP RAT Coverage From SNPN

With the network based non-3GPP to 3GPP handover procedure, the data path is switched from one tunnel to another (i.e., from blue to green in the above figure). This means that even if the UE is able to maintain Rx/Tx connections to both 3GPP RATs at the same time, the UE must decide which tunnel is used for data transfer.

If the UE is bouncing between both networks then the tunnel switching will also happen each time the UE is switching between the networks. This may induce excessive network signaling procedure with the hPLMN. To minimize the signaling induced by tunnel switching with HPLMN, and to allow mobility procedure between SNPN and PLMN, a 3GPP feature called access traffic steering, switching, splitting (ATSSS) can be used. ATSSS allows the UE and the network to transfer user plane data via one or more data paths using MPTCP and/or ATSSS low-layer (ATSSS-LL). MPTCP is a protocol defined by IETF

and has been widely used in the industry already for reliable delivery via different data paths for TCP traffic. For UDP, 3GPP develops its own ATSSS-LL as IETF MP-QUIC is not yet finalized. Overall, ATSSS defines the following different steering modes to steer the traffics between two paths:

- Active-standby: One path is denoted as primary access and is always used even when the other path is available.
- Smallest delay: The path with the smallest round-trip time (RTT) is used.
- Load-balancing: Traffic is split across different paths.
- Priority-based: The primary path is used until it reaches certain congestion level in which case the other path is used.

4. Services That Can Be Offered With 5G Private Networks

3GPP in Release 18 has been studying new use cases for 5G networks providing access to localized services and identifying relevant requirements. The study takes a number of relevant aspects into consideration as depicted in a business model in Figure 8 [5]:

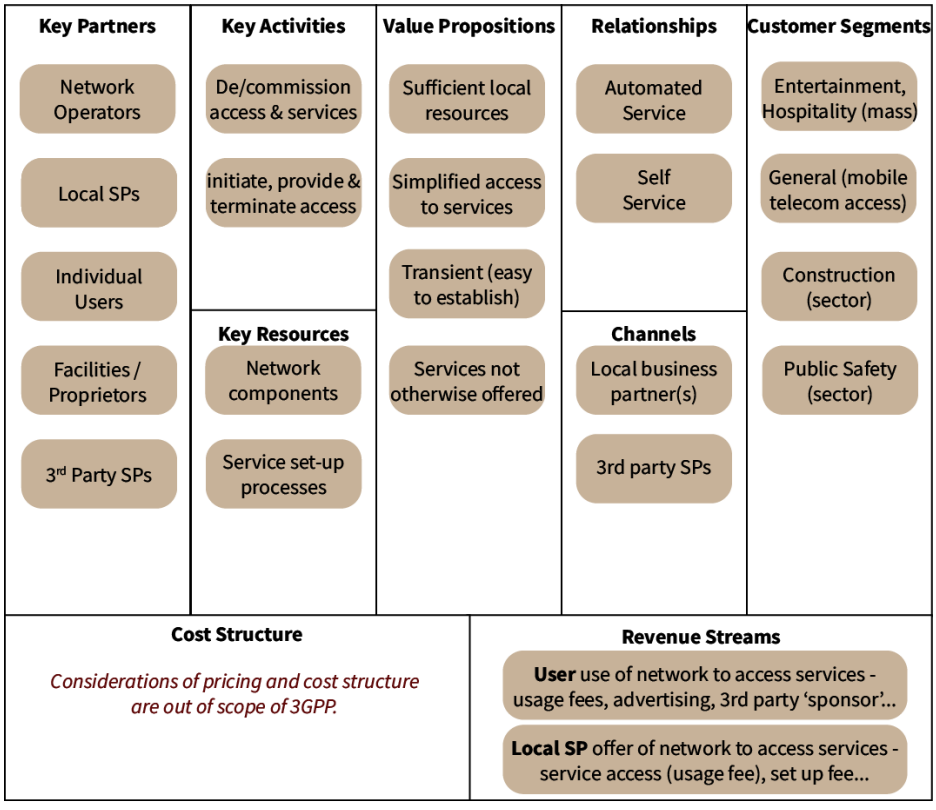

Figure 8 – Business Model For Providing Access To Localized Services

- *Key partners* may include network operators (MNOs, private network operators, MSOs, etc.), local service providers, individuals (users), owners of facilities or proprietors of businesses in which the local access network will be available, and 3rd party service providers. These stakeholders need to work together to provide local access to services.
- *Key activities* may involve how to commission/decommission access to local network and a localized services offered by any of the key partners using the local network. Since the access is local and may

be bounded in time and space, the effort to commission/decommission accesses and services needs to be aimed to be requiring short lead-time and low complexity, etc. From a user perspective, the user needs to become aware of access and local services to choose and access them. The process for the user and his/her equipment to gain access to the network, to use and terminate access and services needs to be efficient, simple and convenient. The offered resources and services cannot be accessed by any other way.

- *Value proposition* perspective providing access to local services can result in some distinct opportunities for users and service providers.
    - The access can be provided that is sufficient in areas that otherwise would lack them, for example, on a fairground established far from other infrastructure.
    - The access to local services can be simpler than access would be without this service. For example, obtaining network access may result in associated local service configuration and effortless presentation to the user.
    - The access and local services operation can be established as needed, without the need for long term business relationships such as facilities, permanently installed equipment, etc.
- In order to establish the set of business *relationships* and arrangements from the perspective of all involved key partners that could be very complex, business processes need to be automated, or at the very least available for self-service.
- *Customer segments* for localized services can be broad. The ones listed in the figure are just some sample ones.
- Two kinds of key *resources* are needed to provide access to local services:
    - Network components: The network operator needs to have or be able to make use of other operators' network infrastructure, both for mobile access and for configuration of services, authorization and other aspects.
    - Service set-up processes: A set of service set-up processes need to be in place such that the service providers (local service providers, 3rd party service providers and the network operator provided services) are able to arrange for their services to be offered via the local access.
- These local service access can be promoted and arranged through different *channels*. Principally the local service operators, such as an entertainment venue, can provide and promote information to potential users so that they can seek to access the local services. Third party service provider, such as a sports club, can also inform, motivate and prepare their users to expect local access to services in a particular place and at a particular time.
- *Cost* and *revenue* due to offering and usage of localized services can vary such that the key partners need to make necessary business agreements to get their proper share. The cost of using some localized services to users may be free-of-charge or usage-based. Some offered localized services may be sponsored, for example, by any of the key partners, advertisers, or 3rd party sponsors.

In the light of the aspects listed above, as an example for providing access to localized services, an SNPN deployed at a sporting venue may offer various services to their customers visiting the venue for a game: The offered services may be like the Internet access, real-time video or AR/3D services from various camera angles of the field (e.g., the perspective of the referee or a favorite player) that are only available to visitors at the venue. Any services in the venue may be offered by one or more key partners such as the sporting venue owner, infrastructure network provider, broadcasting agency like a TV station, 3rd party sponsor or one of the athletic clubs, etc. The visitors can be made aware of the offered services and how to get onboarded to the local access network and the localized services before or when they come the venue by one or more of the key partners. The offered services can be broadcasted by the local access network and compatible UEs can show the available services to the users; and guide the interested users for easy onboarding and then start using the services. When new services or an update to the previously

offered services become available, the visitors can be made aware via various means such as updating service broadcast at access network or via a venue application, etc. While some or all services offered might be free-of-charge or usage-based to the users. The service provider may generate advertising revenue by offering advertising services to 3rd party companies while users rendering localized services.

5. Standards Development For 5G Private Networks

Standardization work for 5G private networks (i.e., SNPN) was started from 3GPP Rel 16 using 5G standalone architecture as the baseline. The development has continued in Rel 17 [3] with more capabilities and features. Currently, the industries are discussing further possible enhancements in Rel 18 [4] [5] [6].

Rel 16 was frozen at June 2020. Rel 17 is currently under development and is scheduled to be frozen by March 2022. R18 has already been started with new requirements gathering by 3GPP SA1 since the end of 2020 and most likely that the freeze date for Rel 18 will be by the end of 2023 or early 2024.

The following figure shows some of the key features related to 5G private networks per 3GPP release cycle under the umbrella of the system architecture group (3GPP SA). Rel 18 content is only at the initial phase of the development; hence, it is a best guess from the authors of this paper.

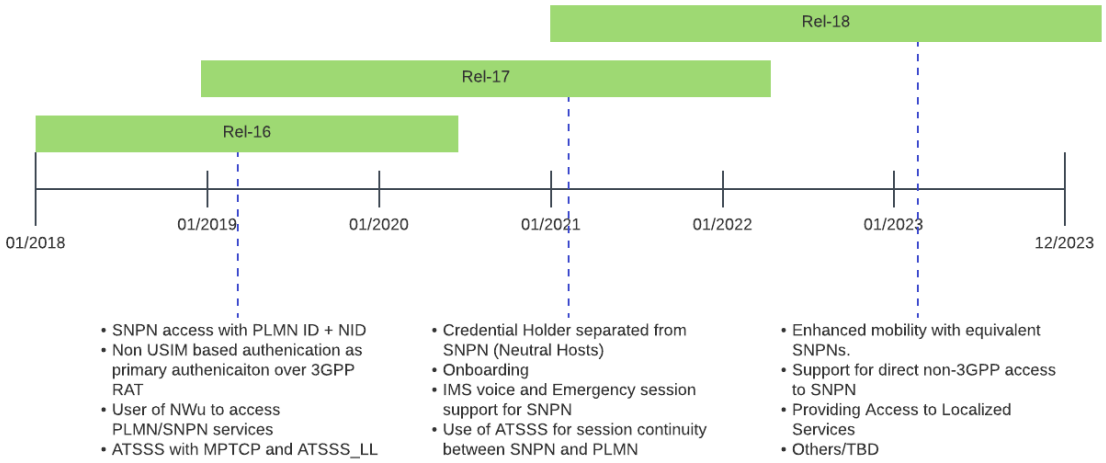

Figure 9 – SNPN Related Feature Per 3GPP Release

In 3GPP Release 18, in addition to providing access to localized services studied in [5], other potential Rel 18 features are aiming for better mobility experience. Enhanced mobility with equivalent SNPNs, allows a UE with subscription for one of the SNPNs has access to its all equivalent SNPN(s), similar to how equivalent (h)PLMNs work today. 5G system architecture can already support non 3GPP access like Wi-Fi or fixed broadband access. The SNPN feature has so far been focusing on using 3GPP RAT due to time pressure, however documenting the support for SNPN for non-3GPP access will make the standards specifications to be more holistic.

6. Conclusion

The new capabilities available for 5G private networks (i.e., SNPN) open a new realm of service possibilities that was previously not available with 4G systems based on evolved packet core (EPC). The on-demand credential provisioning with onboarding feature, the adoption of using network access identifier (NAI) for user identity and EAP with TLS/TTLS, flexible network ID assignment (PLMN ID + NID), and neutral host offering are some of the features that make 5G private network unique from any of the previous 3GPP systems, and this allows much wider applicability of using 3GPP eco-system with 3GPP RAT and non-3GPP RATs (WiFi, fixed-broadband access) for new service creation.

Abbreviations

3GPP	3rd Generation Partnership Project
AAA	authentication, authorization, accounting
AMF	access and mobility management function
ATIS	Alliance for Telecommunication Industry Solutions
ATSSS	access traffic steering, switching and splitting
ATSSS-LL	ATSSS low-layer
AUSF	authentication server function
CH	credentials holder
DSDA	dual SIM dual active
DSDS	dual SIM dual standby
EAP	extensible authentication protocol
eSIM	embedded SIM
EPC	evolved packet core
FQDN	fully qualified domain name
GIN	group ID for network selection
hPLMN	home PLMN
HSS	home subscriber server
IETF	Internet Engineering Task Force
IMS	IP-multimedia subsystem
LBO	local breakout
MCC+MNC	mobile country code + mobile network code
MNO	mobile network operator
MSO	multi system operator
MP-QUIC	multi-path quick UDP internet connections
MPTCP	multi-path transport control protocol
N3IWF	non-3GPP interworking function
NAI	network access identifier
NAS	non-access stratum
NF	network function
NG-RAN	next generation radio access network
NID	network identifier
NSSAAF	network slice-specific and SNPN authentication and authorization function
NWu	reference point for untrusted non-3GPP access network to 5GC
PCO	protocol configuration options
PDN	packet data network
PDU	protocol data unit
PLMN	public land mobile network
PS	provisioning server
QoE	quality of experience
QoS	quality of service
RAN	radio access network
RAT	radio access technology
RRC	radio resource control

RTT	round trip time
SA	Stand Alone
SIB	system information block
SMF	session management function
SNPN	stand-alone non-public network
TCP	transport control protocol
TLS	transport layer security
TTLS	tunneled transport layer security
UDM	unified data management
UDP	user datagram protocol
UE	user equipment
UPF	user plane function
USIM	universal subscriber identity module
vPLMN	visited PLMN
GBR	Guaranteed bit rate
MBR	Maximum bit rate
ARP	Allocation and retention priority
APN-AMBR	Access Point Name Aggregate Maximum Bit Rate
QCI	QoS class identifier
UE-AMBR	UE Aggregate Maximum Bit Rate
SUPI	Subscriber identifier
ITU	International Telecommunication Union
OEM	Original Equipment Manufacturer (to describe smartphone vendor)
TX	Transmit
RX	Receive

Bibliography & References

[1] International Telecommunication Union (ITU), Standardization Bureau (TSB): Operational Bulletin No. 1156; http://handle.itu.int/11.1002/pub/810cad63-en (retrieved October 5, 2018)

[2] 3GPP TS 23.501 V16.8 and V17.1, System Architecture for the 5G System (5GS); Stage 2

[3] 3GPP TR 23.700-07 V17.0, Study on Enhanced Support of Non-Public Networks (NPN)

[4] 3GPP Study Item proposal for Rel-18, Study on Enhanced Support of Non-Public Networks; Phase 2 (S2-2104337)

[5] 3GPP TR 22.844 V18.0, Study on 5G Networks Providing Access to Localized Services; Stage 1

[6] 3GPP Work Item proposal for Rel-18, 5G Networks Providing Access to Localized Services (SP-210588)

