How ATSSS and Trusted Wi-Fi Access Will Enable the Converged Mobile User Experience

A Technical Paper prepared for SCTE by

Christopher Burke
Principal Engineer III
Charter Communications
6360 S Fiddler's Green Circle, Greenwood Village, CO
720-699-6430
christopher.burke@charter.com

Table of Contents

List of Figures

1. Introduction

Mobile devices today can connect to services over cellular and Wi-Fi networks; two completely different technologies with their own designs and sets of standards. Additionally, mobile services are often combined with other services, such as video or internet, and charged to the customer on a single bill. Does this provide a converged user experience? Not really.

While bundling of services is convenient to the customer, it doesn't really converge the delivery of these services. And a device that can connect to multiple networks is great, but if the networks are completely separate, with different authentication methods, policy enforcement, charging rates, and data paths to services, then these networks merely coexist and are not converged.

The convergence vision is to deliver ubiquitous connectivity to customers anywhere and on any device, delivered on high capacity and low latency networks. This means that customers would carry their applications, services, policies, and identity with them wherever they go – inside or outside of home, on a fixed or mobile device.

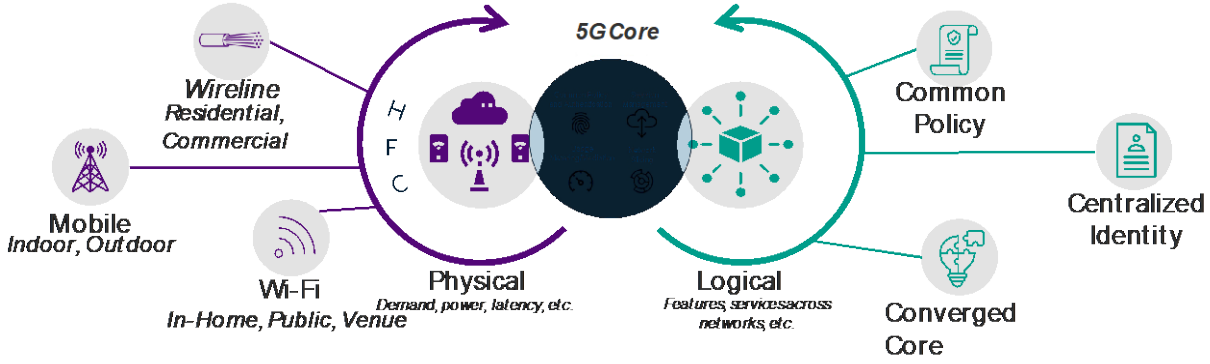

Figure 1 - Convergence Concept

The emergence of 5G networks provides the ability to deliver on this experience, with standards detailing the early beginnings of the convergence vision. While 5G convergence looks at several different convergence opportunities, one of the first areas to explore is mobile 5G/Wi-Fi convergence because it can offer significant benefits such as:

- Mobility: The ability to seamlessly combine Wi-Fi with cellular connectivity is extremely valuable, especially for use cases like moving through indoor/outdoor campuses.
- Resiliency: Combining 5G and Wi-Fi to provide better coverage in any space and making use of both simultaneously.
- Security: Benefits from the ability to authenticate all devices via 5G cores, even as some operate over non-cellular networks.
- Differentiation: Many cable operators with extensive Wi-Fi deployments now act as mobile virtual network operators (MVNOs). New public/private solutions that tightly integrate 5G with Wi-Fi could open compelling new business.

A converged mobile experience is about having a singular experience that follows you wherever and however you connect, utilizing the same authentication credentials, subscriber policies, charging rules, and gateways. This paper explores how two 5G mobile technologies, access traffic steering, switching,

and splitting (ATSSS) and trusted Wi-Fi access, can work together to provide the first converged mobile user experience.

2. Access Traffic Steering, Switching, and Splitting

Beginning with 3GPP Release 16, 5G introduces the access traffic steering, switching, and splitting (ATSSS) feature, which allows the service provider to steer, switch, and split traffic across 3GPP (5G cellular) and non-3GPP (Wi-Fi) access networks.

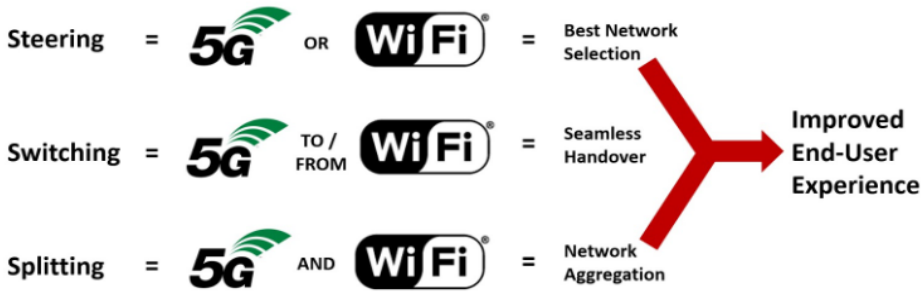

Figure 2 - ATSSS Concept

As a key technology in 5G/Wi-Fi convergence, the implementation of ATSSS by service providers can improve the overall quality of experience (QoE) through:

- Use of standards-based common authentication and policy control to select the best available access network.
- The ability to facilitate seamless transition between cellular and Wi-Fi networks.
  - Customers don't need to disable Wi-Fi due to dead zones.
  - Improved performance for sensitive applications (gaming, banking, OTT voice).
- 5G cellular and Wi-Fi data aggregation, which will deliver speeds that combine the channels from both access networks to be used simultaneously.

ATSSS provides simultaneous connectivity across 3GPP networks and non-3GPP networks to a common user plane function (UPF) within the 5G core, allowing for common authentication and policy control and the smoothing of transitions between access types.

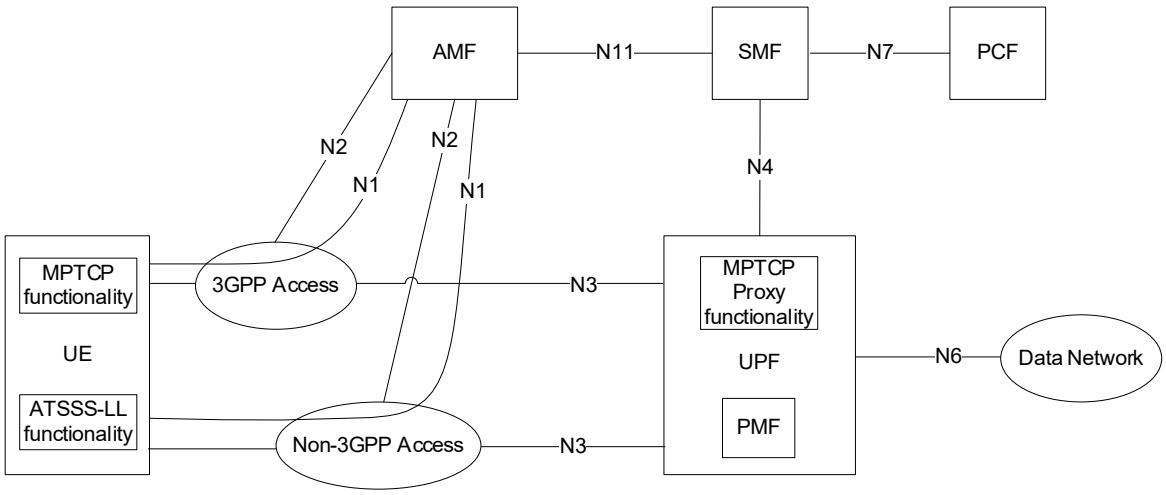

Figure 3 - ATSSS architecture as described in 3GPP TS 23.501

To enable ATSSS, the user equipment (UE) requests a multi-access packet data unit (MA-PDU) session, which may have user plane resources on two access networks: one 3GPP access network and one non-3GPP access network, with independent N3 tunnels between each access network and a single UPF in the 5G core.

An ATSSS capable UE specifies support for one or more steering functionalities:

- High Layer Steering: Steering functionality that operates above the IP layer.
  - The initial support for high layer steering is multi-path TCP (MPTCP), which can be applied to steer, switch, and split TCP traffic. The MPTCP functionality in the UE communicates with an associated MPTCP proxy functionality in the UPF, using MPTCP protocol over the 3GPP and/or the non-3GPP user plane.
  - In 3GPP Release 18, high layer steering will include multi-path QUIC (MPQUIC), which can be applied to steer, switch, and split UDP traffic. This is not covered in this paper but operates functionally the same as MPTCP.
- Low Layer Steering: Steering functionality that operates below the IP layer.
  - ATSSS-LL steering functionality can be applied to steer, switch and split all types of traffic, including TCP traffic, UDP traffic, Ethernet traffic, etc.

The UE may indicate support for ATSSS-LL only, or support for both ATSSS-LL and MPTCP. If using MPTCP, the UE must be assigned three IP addresses; a MA-PDU session IP address and two link-specific multipath IP addresses.

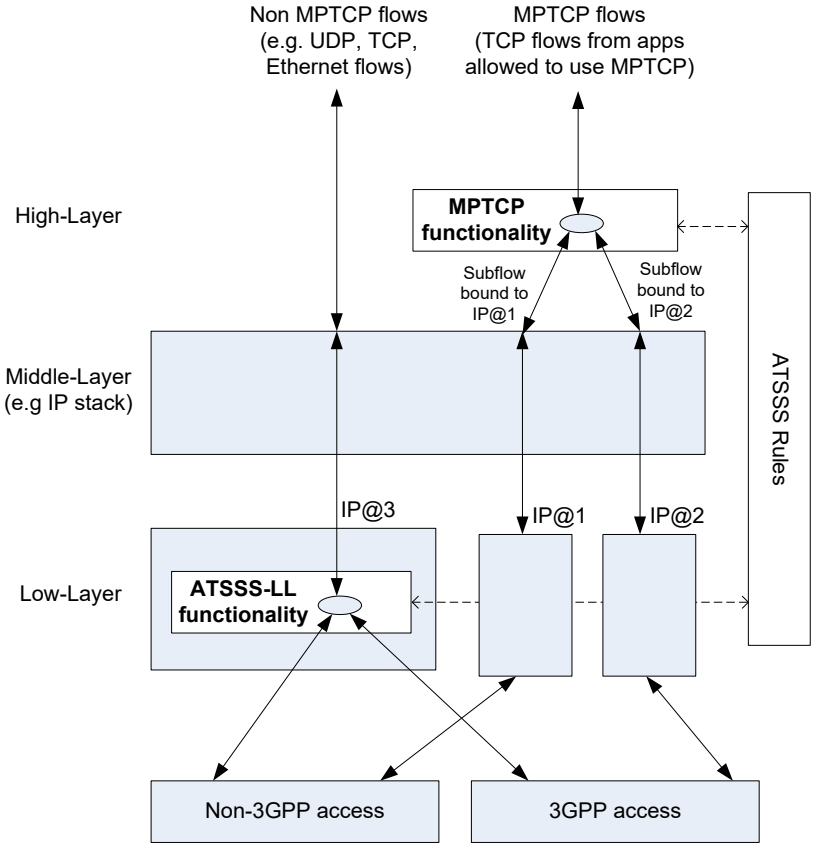

Figure 4 - UE ATSSS Steering Functionalities as described in 3GPP TS 23.501

Once the MA-PDU session is established, the UE uses network provided policy rules (ATSSS rules) and network measurements to decide how to distribute the uplink traffic across the two access networks. Likewise, the UPF uses network provided policy rules (MAR) and network measurements to decide how to distribute the downlink traffic across the two access networks. Network performance measurements are exchanged between UE and UPF performance measurement functions (PMF) using the PMF protocol (PMFP) to assist with determining the latency, packet loss, and access network availability. Traffic is routed in any combination of active/standby, smallest delay, load balancing, or priority, based as determined by policy and network conditions. The UE and UPF may make uplink and downlink routing decisions, respectively, independent of each other.

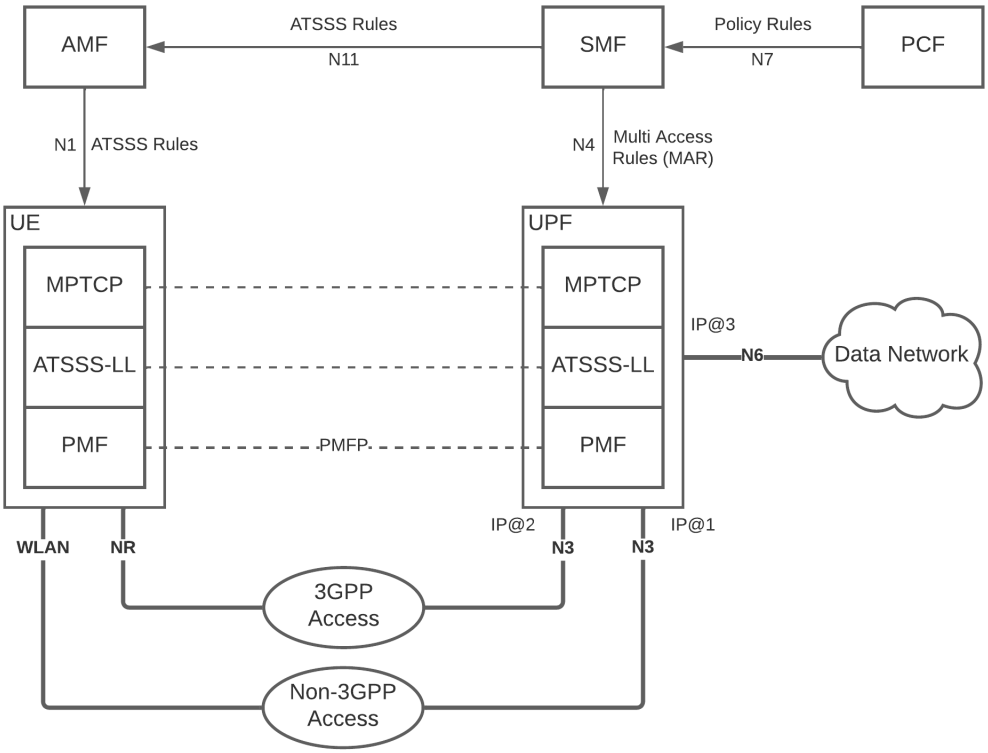

Figure 5 - ATSSS Architecture w/ Steering, Policy, and Performance Details

2.1. Wi-Fi Connectivity

3GPP access is the 5G radio access network (RAN), which connects natively to the 5G core and is well defined in 3GPP standards, making non-3GPP access the key component of ATSSS. ATSSS can technically work with any non-3GPP access (WLAN, wired, etc.), but for mobile device 5G/Wi-Fi convergence, we will focus on Wi-Fi connectivity specifically.

3. Trusted Wi-Fi Access

Beginning with 3GPP Release 16, 5G introduces the trusted non-3GPP access feature, which allows Wi-Fi access for mobile devices to behave similarly to the 5G RAN regarding network discoverability, authentication, registration, and PDU session establishment.

Trusted non-3GPP access used for mobile device Wi-Fi access is a key component in 5G/Wi-Fi convergence because it enables the mobile device to:

- Select the Wi-Fi access based on PLMN ID.
- Gain authenticated access to the Wi-Fi network using the device's SIM credentials.
- Register with the 5G core.
- Retain mobile data policies and services while connected to Wi-Fi.

Trusted non-3GPP access introduces the concept of a trusted network access network (TNAN), which consists of the trusted non-3GPP gateway function (TNGF) and the trusted non-3GPP access point.

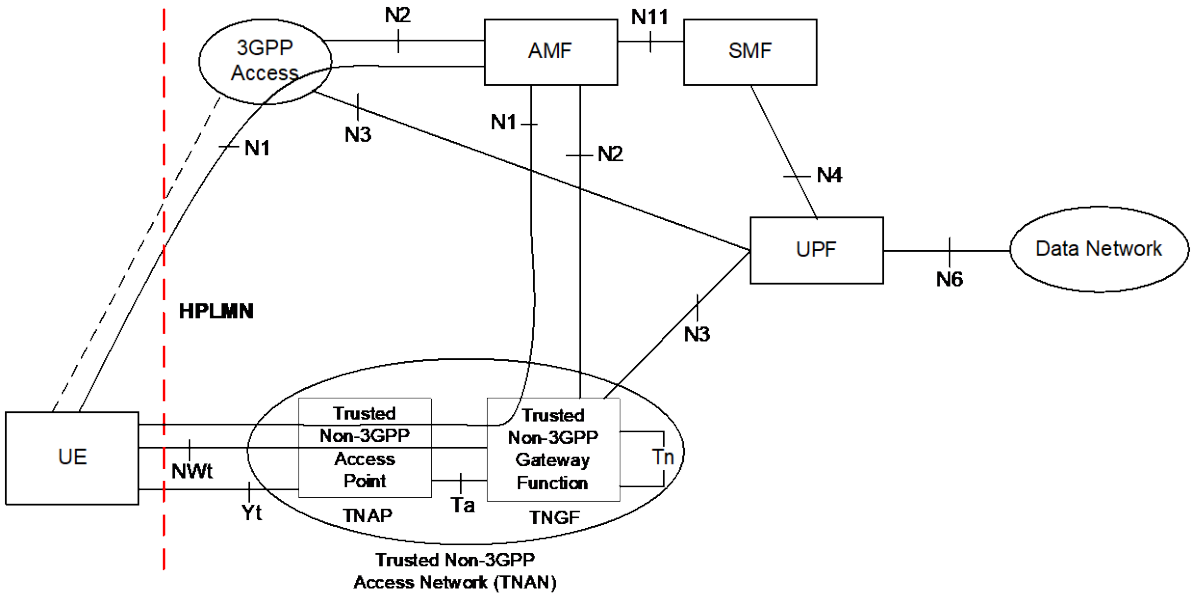

Figure 6 - Trusted Non-3GPP Access as described in 3GPP TS 23.501

The TNGF provides interworking for the UE to connect with and interface with the 5G core for 5G authentication and registration over a standard N2 interface to the AMF. The 5G user plane is handled over a standard N3 interface to a UPF.

With trusted Wi-Fi access, the TNAP is a Hotspot 2.0 compliant Wi-Fi system. The Ta interface between the TNAP and the TNGF is a AAA interface that facilitates authentication procedures between the Wi-Fi system and the 5G core using either RADIUS or diameter messaging. Any existing Wi-Fi system that supports the Hotspot 2.0 standard already supports AAA authentication; therefore, the entire Wi-Fi system effectively becomes the TNAP.

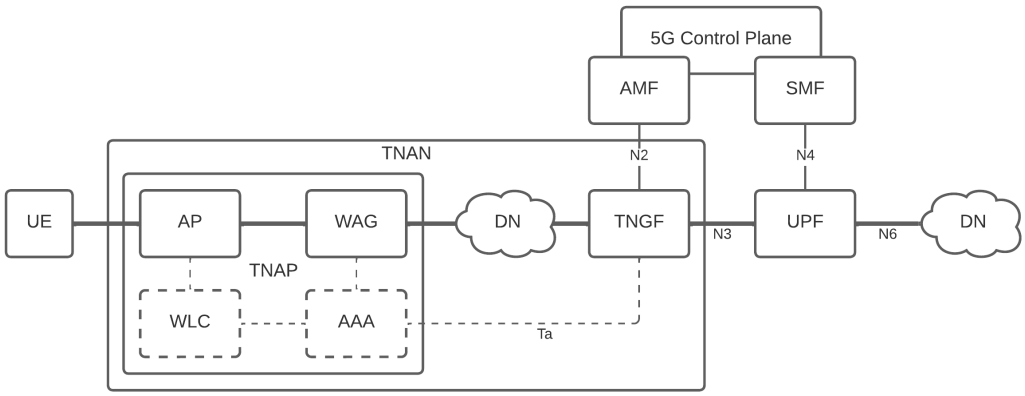

Figure 7 - Example Trusted Wi-Fi Access Architecture Using Existing Wi-Fi System

In the trusted Wi-Fi access system, the Wi-Fi Hotspot 2.0 access point (AP), using the access network query protocol (ANQP), advertises the public land mobile network identifier (PLMN ID) and an indicator that it supports 5G connectivity. The mobile device requests the "3GPP cellular network" information

over ANQP and selects the highest priority service set identifier (SSID) of a WLAN that contains a suitable PLMN ID with 5G connectivity.

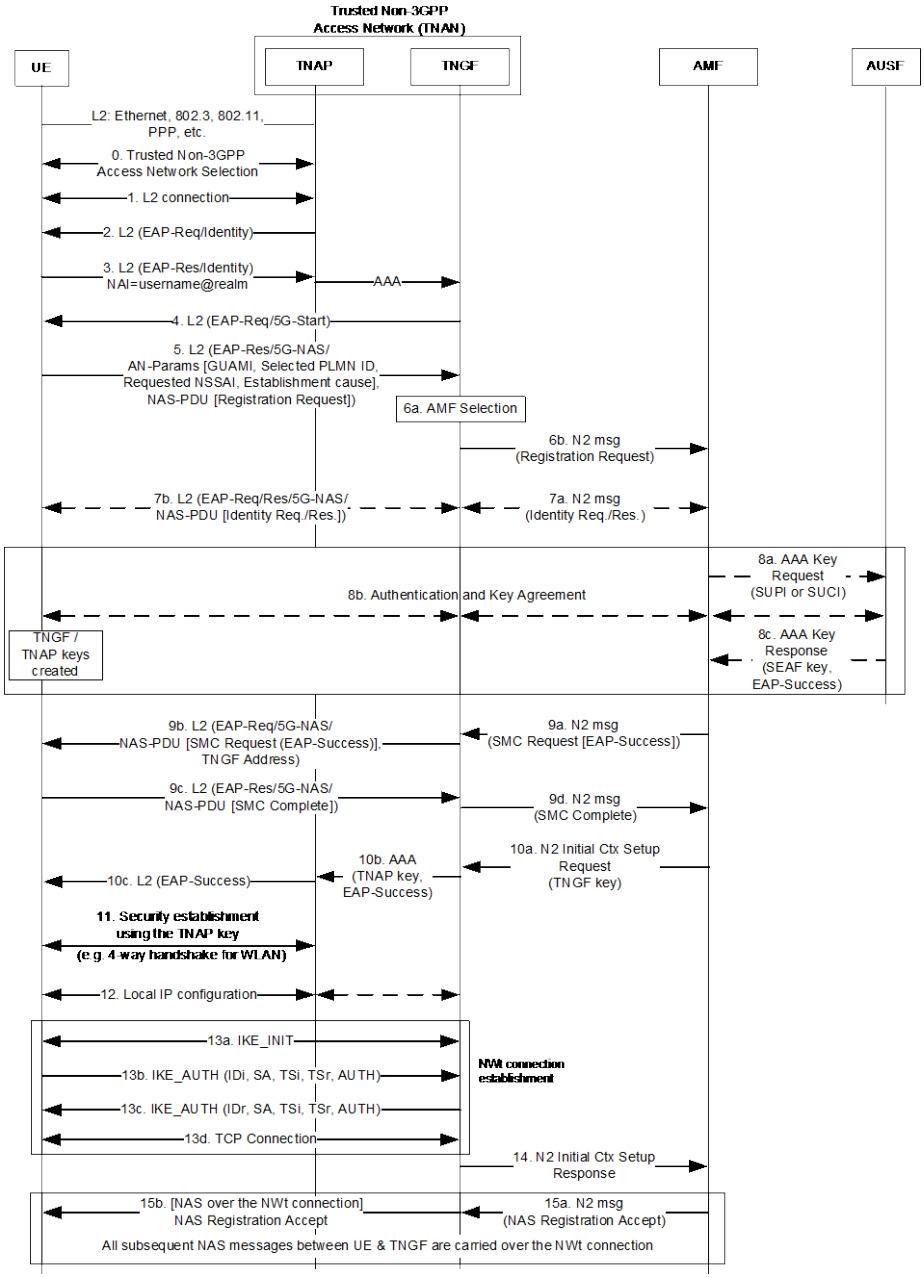

Figure 8 - Trusted non-3GPP Access Authentication and Registration as described in 3GPP TS 23.502

The UE then uses standard EAP authentication procedures to authenticate with the 5G core through the trusted network gateway function (TNGF). The TNGF has an AAA interface (Ta) that supports the exchanging of EAP messages with the Wi-Fi authentication systems using either RADIUS or diameter messaging. The EAP payload is set to “EAP-5G” which is an extended EAP type method that allows for the full exchange of 5G NAS messages between the UE and the 5G core.

Once authenticated, the mobile device is granted access to the WLAN and receives an IP address. The UE then establishes an IPSec tunnel directly to the TNGF (NWt) to complete 5G registration and establish PDU sessions using 5G NAS. The TNGF creates IPSec child security associations to the UE for each PDU session.

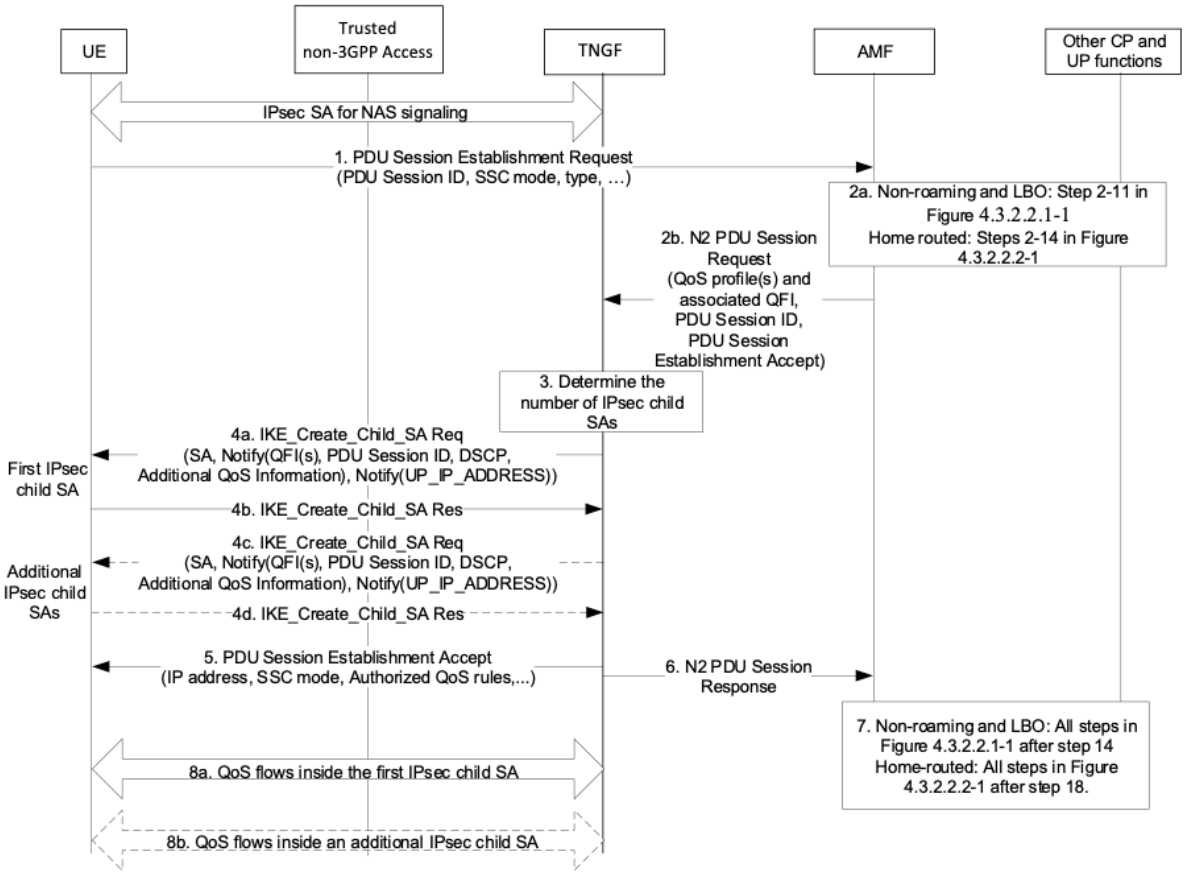

Figure 9 - Trusted non-3GPP Access PDU Session Establishment as described by 3GPP TS 23.502

The complete trusted Wi-Fi access flow enables the mobile device to authenticate, register, and establish data sessions to the 5G core over Wi-Fi access as if it were connecting over cellular, using the exact same credentials, 5G NAS control plane, and 5G user plane.

4. What About Untrusted Wi-Fi Access?

The goal of convergence is to bring together disparate networks and services to provide a new user experience. Part of the requirements of convergence is the seamless nature of the converged experience. 5G untrusted non-3GPP access does not define how the user connects to a Wi-Fi network and does not define a method or architecture to support authentication with the 5G core. This is different from 4G.

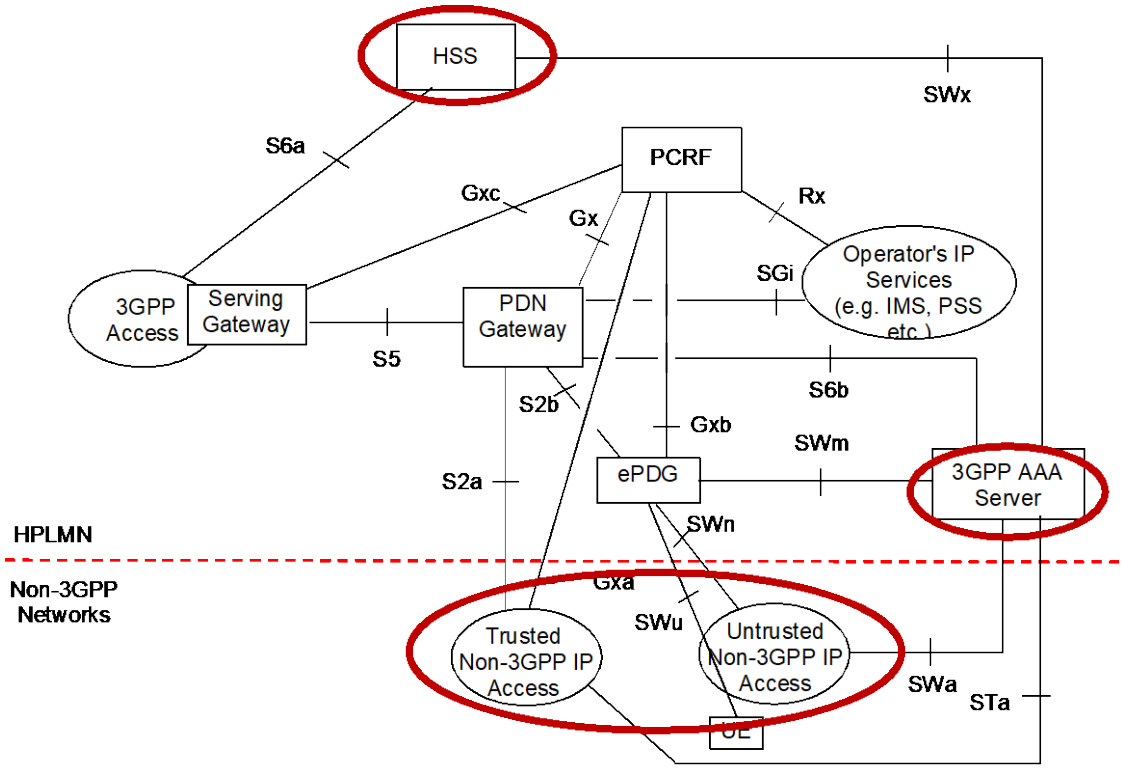

Figure 10 - 4G non-3GPP Architecture as described by 3GPP TS 23.402

If we look at 4G architectures, both trusted and untrusted non-3GPP access have interfaces to a 3GPP AAA server (STa and SWa, respectively) to facilitate authentication to the HSS. However, in 5G, the untrusted non-3GPP access contains no such interface. Only trusted non-3GPP access provides an authentication interface (Ta) between the Wi-Fi network and the 5G core.

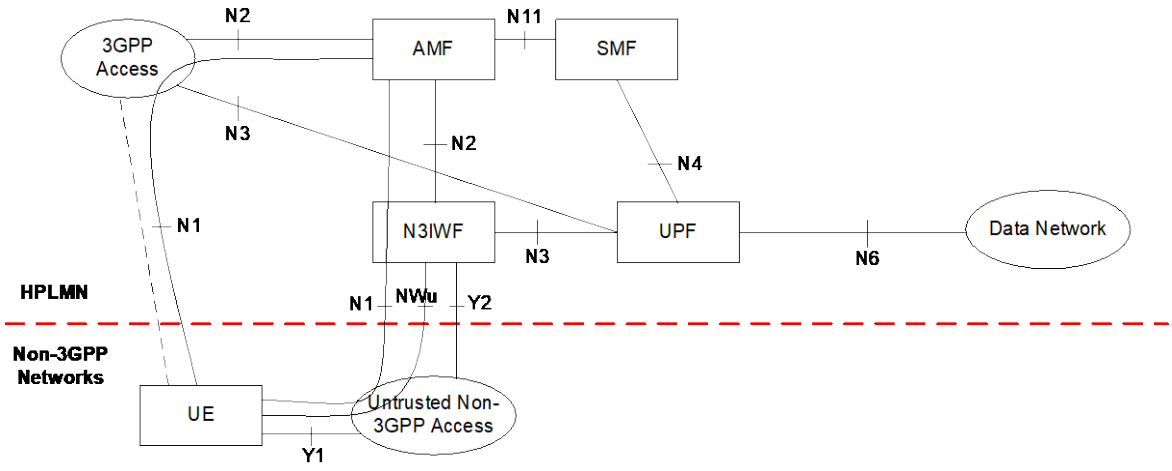

Figure 11 - Untrusted non-3GPP Access as described in 3GPP TS 23.501

In release 17, 3GPP defined non-seamless WLAN offload (NSWO), which allows for authentication to the 5G core without automatically registering or establishing PDU sessions with the 5G core, very much like a 3GPP AAA did in 4G.

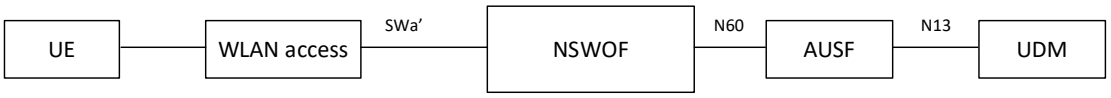

Figure 12 - NSWO as described in 3GPP TS 23.501

Theoretically, NSWO could be combined with untrusted non-3GPP access to have a behavior more closely related to the 4G experience. However, NSWO with untrusted Wi-Fi access has several drawbacks.

1. NSWO and untrusted non-3GPP access each require an authentication. This means there are two authentications: one to gain access to the Wi-Fi network and a second to allow for untrusted access. This is like the current 4G experience.
2. NSWO requires EAP-AKA' to be used for authentication. Most 5G networks are using 5G-AKA as the primary authentication method. This means the authentication method for the NSWO is potentially different from the authentication method for the untrusted access. Additionally, the authentication method is specified in the subscriber record in the UDR as an either/or selection. It is unclear currently how to configure the subscriber to authenticate using one method for NSWO and another method for cellular and untrusted access.
3. The requirements for NSWO to work over Wi-Fi are identical to the requirements for trusted Wi-Fi access. NSWO requires PLMN lists, and their ability to support NSWO must be specified as an option in the ANQP by the Wi-Fi AP, just like trusted Wi-Fi. The UE must be able to have logic to select the correct PLMN and construct a NSWO specific NAI for authentication, just like trusted Wi-Fi. The actual authentication exchange is EAP between the NSWO server and the UE, just as it is between the TNGF and the UE.
4. NSWO with untrusted access requires two new platforms to be deployed (NSWOF and N3IWF) to perform the same functionality of the TNGF.
5. NSWO is designed for legacy Wi-Fi offload behavior only. However, trusted Wi-Fi access can also be used for offload as policy rules, such as UE route selection policy (URSP), can be configured to route traffic locally instead of through a PDU session back to the 5G core.

Essentially, using NSWO and untrusted Wi-Fi access is more complicated, less efficient, and requires the same amount of effort to implement without providing any additional benefit when compared to trusted Wi-Fi access.

Untrusted access still has a place for connecting when the WLAN does not support Hotspot 2.0, or the trusted WLAN cannot be used in the user's current location. 3GPP standards for trusted access have untrusted access as the fallback option when trusted networks are not available. In these cases, untrusted networks may be used, requiring manual Wi-Fi selection and authentication, to connect back to the 5G core to leverage the ATSSS technology.

5. Putting 5G/Wi-Fi Convergence to Use

Trusted Wi-Fi access provides seamless authentication and connectivity of a mobile device to the 5G core over a compatible Hotspot 2.0 Wi-Fi system. ATSSS provides the ability to steer, switch, and split 5G

user traffic between the UE and 5G core over both NR and Wi-Fi in real time. When these two technologies are combined, the first stages of the converged experience may be realized.

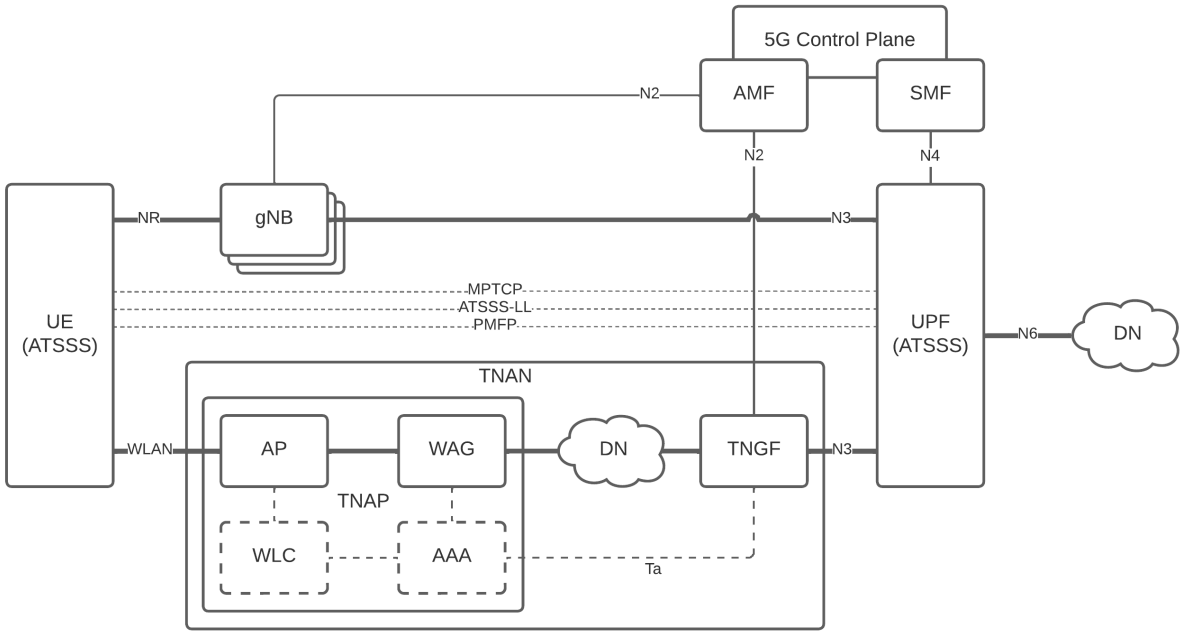

Figure 13 - ATSSS and Trusted Wi-Fi Combined Architecture

5.1. Converged Experience #1: Mobility Coverage and Network Resiliency

Since trusted Wi-Fi access treats access to Wi-Fi networks like a cellular RAN, a mobile operator who provides both 5G NR and Wi-Fi access can take advantage of the seamless authentication, registration, and PDU session establishment of trusted Wi-Fi access and the traffic switching capabilities of ATSSS to extend coverage to indoor areas or other obscure areas where cellular coverage doesn't reach. This creates a seamless experience where the user experiences no interruptions to services and maintains a consistent user policy across the two accesses, which is important when considering parental control policies.

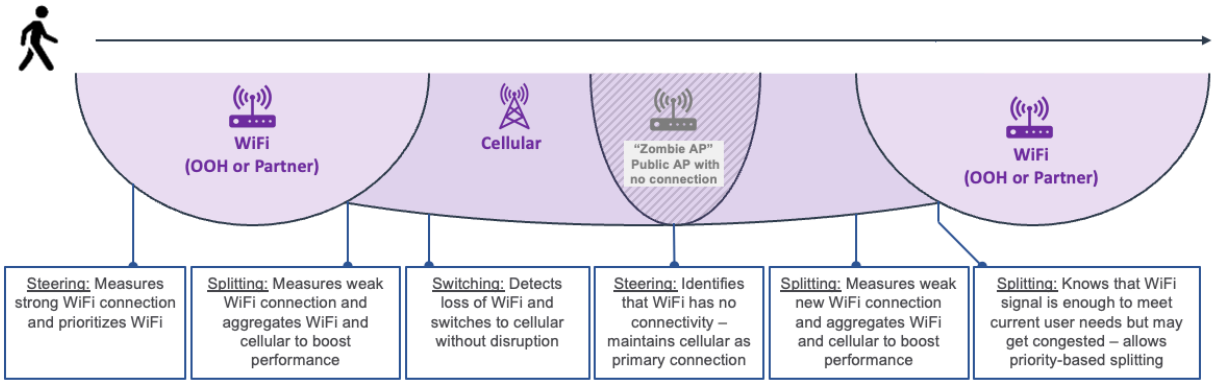

Figure 14 - 5G/Wi-Fi Convergence User Transitions

Additionally, in areas where both cellular and Wi-Fi are available, the splitting capabilities of ATSSS can dynamically route traffic over the best possible access network. ATSSS features can improve the switching experience as the user transitions between access networks, and the steering functionality of ATSSS ensures users never suffer from a "zombie" Wi-Fi AP.

5.2. Converged Experience #2: Mixed Private Wireless

In private wireless, a mixed CBRS and Wi-Fi deployment on a university, hospital, or factory campus can be leveraged to serve a multitude of deployment specific use cases. For many of the same reasons a mobile operator would deploy 5G/Wi-Fi convergence, private wireless deployments would benefit greatly from such a converged architecture and are more likely to have much more overlap of unlicensed access networks. This can be especially powerful for users who use a dual-SIM, dual-standby (DSDS) device to access the private network. If the private wireless network is hosted or managed by a MNO, the MNO may design a deal with the private network, allowing MNO customers to connect over the private network assets and back to the MNO core.

5.3. Converged Experience #3: Improved Full MVNO Offload

Mobile virtual network operators (MVNOs) who provide large out of home Wi-Fi systems, such as a major cable operator, may be able to take advantage of 5G/Wi-Fi convergence to improve their service offering. This would require the MVNO to operate a full MVNO model where the cellular RAN is provided by the MNO partner, and the 5G core and all end services are provided by the MVNO.

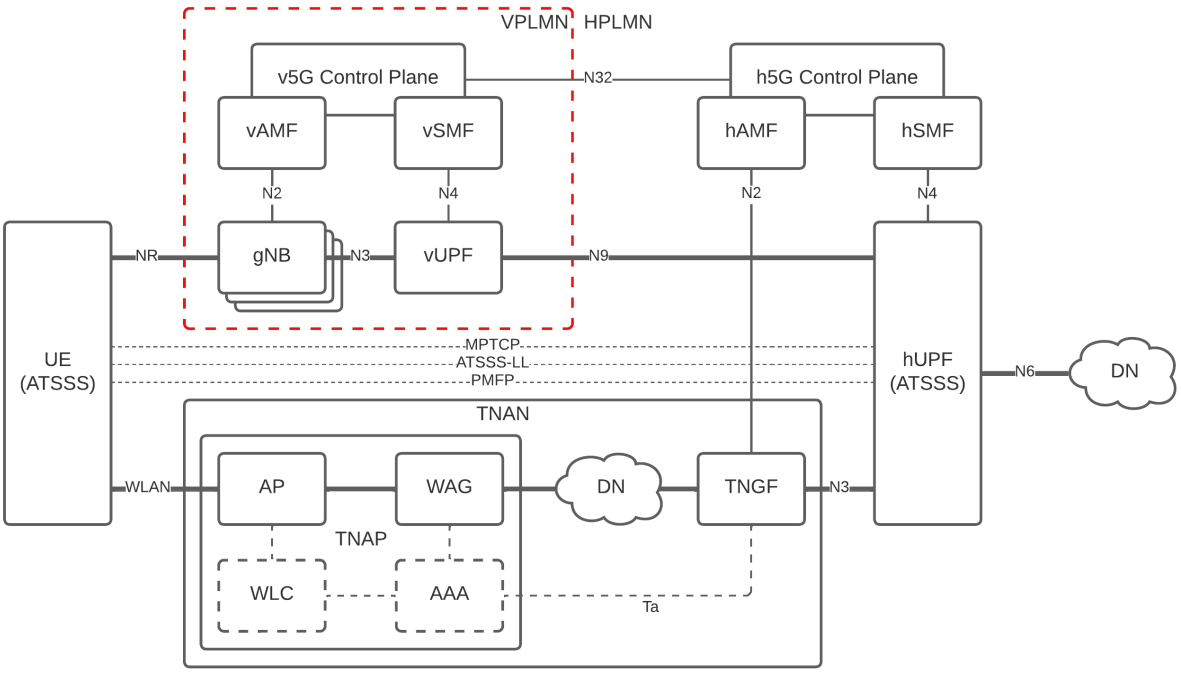

Figure 15 - Full MVNO ATSSS Architecture

Because the cellular traffic is routed to the MVNO's 5G core, the implementation of trusted Wi-Fi access connecting back to the common 5G core enables a seamless offload experience for the users. ATSSS features can improve the switching experience as the user transitions between networks, and the steering

functionality of ATSSS ensures users never suffer from a "zombie" Wi-Fi AP. Users are less likely to turn off Wi-Fi because they will never detect a bad connection, which will improve offload metrics as they pass into working Wi-Fi APs.

5.4. Converged Experience #4: Wi-Fi Mobile Operators

Because trusted Wi-Fi access treats the Wi-Fi network as a RAN to the 5G core, it is now possible to configure a fully secure mobile service that works over Wi-Fi. This can create new entrants to mobile network operators, especially if paired with CBRS. Not only could Wi-Fi only, or Wi-Fi preferred, MNOs begin to offer service directly, but their networks can be easily monetized to support new roaming relationships between traditional operators and these new Wi-Fi preferred operators.

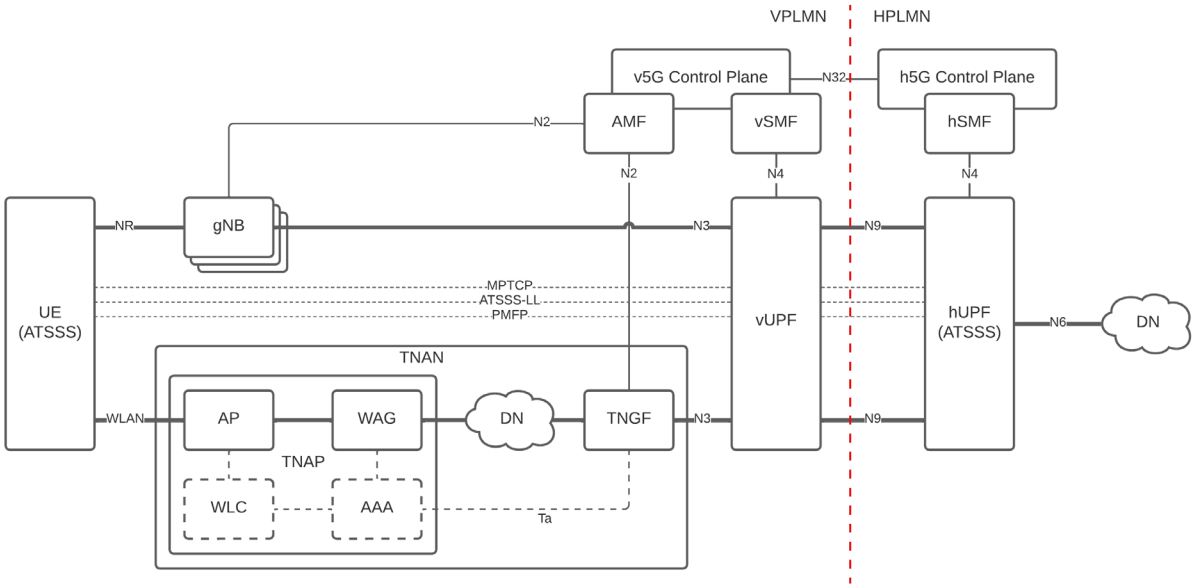

Figure 16 - Example Home Routed Roaming Architecture with Trusted Wi-Fi Access

6. Conclusion

5G networks provide a lot of opportunity for convergence, bringing together networks and services to enhance the user experience. The first opportunity to demonstrate the converged user experience in 5G is to combine cellular and Wi-Fi access networks to provide seamless, integrated connectivity of a mobile device to a common 5G core. 5G trusted Wi-Fi access connectivity provides seamless authentication, registration, and PDU session establishment, similar to cellular access, allowing the use of Wi-Fi networks as another RAN for the 5G core. When combined with ATSSS, a user's device can seamlessly move between the two access networks, load-share traffic, and avoid service disruptions. This converged network also opens new opportunities for private networks, MVNOs, and Wi-Fi network providers, changing the landscape of mobile network deployment options.

Abbreviations

3GPP	3rd Generation Partnership Project
4G	4th generation
5G	5th generation
5G-AKA	5G authentication and key agreement
AAA	authentication, authorization, accounting
AMF	access mobility management function
ANQP	access network query protocol
AP	access point
ATSSS	access traffic steering switching splitting
ATSSS-LL	ATSSS lower layer
AUSF	authentication server function
EAP	extensible authentication protocol
EAP-AKA’	extensible authentication protocol for authentication and key agreement prime
MA-PDU	multi-access packet data unit
MAR	multi-access rules
MNO	mobile network operator
MPQUIC	multi-path QUIC
MPTCP	multi-path TCP
MVNO	mobile virtual network operator
N3IWF	non-3GPP interworking function
NAS	non-access stratum
NSWO	non-seamless WLAN offload
NSWOF	non-seamless WLAN offload function
PCF	policy control function
PDU	packet data unit
PLMN ID	public land mobile network identifier
PMF	performance measurement function
PMFP	performance measurement function protocol
QoE	quality of experience
QUIC	quick UDP internet connections
RAN	radio access network
SCTE	Society of Cable Telecommunications Engineers
SMF	session management function
SSID	service set identifier
TCP	transmission control protocol
TNAN	trusted non-3GPP access network
TNAP	trusted non-3GPP access point
TNGF	trusted non-3GPP gateway function
UDP	user datagram protocol
UE	user equipment
UPF	user plane function
URSP	UE route selection policy
WAG	wireless access gateway
WLAN	wireless local area network
WLC	wireless LAN controller

Bibliography & References

3GPP TS 23.402: *Architecture enhancements for non-3GPP accesses*; 3rd Generation Partnership Project

3GPP TS 23.501: *System architecture for the 5G System (5GS)*; 3rd Generation Partnership Project

3GPP TS 23.502: *Procedures for the 5G System (5GS)*; 3rd Generation Partnership Project

3GPP TS 23.503: *Policy and charging control framework for the 5G System (5GS)*; 3rd Generation Partnership Project

3GPP TS 24.193: *Access Traffic Steering, Switching and Splitting (ATSSS)*, 3rd Generation Partnership Project

3GPP TS 24.502: *Access to the 3GPP 5G Core Network (5GCN) via Non-3GPP Access Networks (N3AN)*; 3rd Generation Partnership Project

3GPP TS 24.526: *User Equipment (UE) policies for 5G System (5GS)*; 3rd Generation Partnership Project

