वर्गीय आवश्यकताओं के लिए मानक

टी.ई.सी XXXX:२०२५

STANDARD FOR GENERIC REQUIREMENTS

TEC XXXX:2025

WLAN Interworking Gateways/Network Functions in 4G/ 5G Systems

4जी और 5जी सिस्टम में डब्ल्यूएलएएन इंटरवर्किंग गेटवे/नेटवर्क फ़ंक्शन

ISO 9001:2015

दूरसंचार अभियांत्रिकी केंद्र
खुर्शीदलाल भवन, जनपथ, नई दिल्ली–110001, भारत
TELECOMMUNICATION ENGINEERING CENTRE
KHURSHIDLAL BHAWAN, JANPATH, NEW DELHI–110001, INDIA
www.tec.gov.in

Release: XXXX, 2025

FOREWORD

Telecommunication Engineering Centre (TEC) functions under Department of Telecommunications (DOT), Government of India. Its activities include:

- Issue of Standards for Generic Requirements (GR), Interface Requirements (IR) and Service Requirements (SR) as well as Test guides for Telecom Products and Services;
- Issue of Technical regulations in the form of essential Requirements (ER);
- Field evaluation of products and Systems;
- National Fundamental Plans;
- Support to DOT on technology issues;
- Testing & Certification of Telecom products; and
- Designation of Conformance Assessment Bodies (CABs) for testing.

For the purpose of testing, four Regional Telecom Engineering Centers (RTECs) have been established which are located at New Delhi, Bangalore, Mumbai, and Kolkata.

ABSTRACT

This document specifies the Generic Requirements (GR) for WLAN Interworking Gateways/Network Functions in 4G/5G Systems within the Indian telecommunication networks. It outlines the architecture, functional requirements, interoperability requirements and other relevant technical requirements for the Gateways (GWs)/Network Functions (NFs) that enable interworking between WLAN access networks (a type of non-3GPP access network) and 3GPP core networks, namely the Evolved Packet Core (EPC) and the 5G Core (5GC).

HISTORY SHEET

Sl. No.	Standard/Document No.	Title	Remarks
1.	TEC XXXX:2025	WLAN Interworking Gateways/Network Functions in 4G/5G Systems	New Release

CONTENTS

REFERENCES

S.No.	*Document No.*	*Title/Document Name*
1)	3GPP TS 24.301	Non-Access-Stratum (NAS) protocol for Evolved Packet System (EPS)
2)	3GPP TS 23.402	Architecture enhancements for non-3GPP accesses
3)	3GPP TS 23.501	System Architecture for the 5G System; Stage 2
4)	3GPP TS 23.502	5G; Procedures for the 5G System (5GS)
5)	3GPP TS 24.501	Non-Access-Stratum (NAS) protocol for 5G System (5GS); Stage 3
6)	3GPP TS 24.502	Access to the 3GPP 5G Core Network (5GCN) via Non-3GPP Access Networks (N3AN); Stage 3
7)	3GPP TS 24.302	Access to the 3GPP Evolved Packet Core (EPC) via non-3GPP access networks; Stage 3
8)	3GPP TS 29.273	3GPP EPS AAA interfaces
9)	3GPP TS 29.274	Evolved General Packet Radio Service (GPRS) Tunnelling Protocol for Control plane (GTPv2-C); Stage 3
10)	3GPP TS 29.275	Proxy Mobile IPv6 (PMIPv6) based Mobility and Tunnelling protocols; Stage 3
11)	3GPP TS 29.303	Technical Specification Group Core Network and Terminals; Domain Name System Procedures; Stage 3
12)		
13)	3GPP TS 33.402	3GPP System Architecture Evolution (SAE); Security aspects of non-3GPP accesses
14)	3GPP TS 33.501	Security Architecture and Procedures for 5G System
15)	3GPP TS 38.413	NG-RAN; NG Application Protocol (NGAP)
16)	RFC 5996	Internet Key Exchange Protocol Version 2 (IKEv2)

17)	RFC 4739	Multiple Authentication Exchanges in the Internet Key Exchange (IKEv2) Protocol
18)	RFC 3948	UDP Encapsulation of IPsec ESP Packets
19)	RFC 3715	IPsec-Network Address Translation (NAT) Compatibility Requirements
20)	RFC 3588	Diameter Base Protocol
21)	ITU-T 2255	Voice and video call continuity over LTE, Wi-Fi and 2G/3G

CHAPTER 1

1. Introduction

1.1. Scope

This document specifies the Generic Requirements (GR) for WLAN Interworking Gateways/Network Functions in 4G/5G Systems within the Indian telecommunication networks. It outlines the architecture, functional requirements, interoperability requirements and other relevant technical requirements for the Gateways (GWs)/Network Functions (NFs) that enable interworking between WLAN access networks (a type of non-3GPP access network) and 3GPP core networks, namely the Evolved Packet Core (EPC) and the 5G Core (5GC).

This GR covers the following GWs/NFs for interworking between WLAN and EPC/5GC[1]:

S. No.	Gateway	Access Type	Core Network
1.	Trusted WLAN Access Gateway (TWAG)	Trusted	EPC
2.	Evolved Packet Data Gateway (ePDG)	Untrusted	EPC
3.	Trusted Non-3GPP Gateway Function (TNGF)	Trusted	5GC
4.	Non-3GPP InterWorking Function (N3IWF)	Untrusted	5GC
5.	Trusted WLAN Interworking Function (TWIF)	Trusted	5GC
6.	Non-Seamless WLAN Offload Function (NSWOF)	Both Trusted and Untrusted	5GC

These GWs/NFs enable interworking between WLAN and 3GPP core networks by

[1] *Note: ePDG and N3IWF provide interworking capability between the 3GPP core network and multiple types of non-3GPP IP access networks, however, the scope of this GR is restricted to interworking between WLAN access networks and the 3GPP core network only.*

supporting authentication, tunnelling, mobility management, and policy enforcement for both trusted and untrusted access scenarios.

The GWs/NFs may be deployed as hardware-based or software-based solutions, depending on the design and vendor implementation. The technical requirements specified in the subsequent chapters shall apply to these GWs/NFs based on their respective architectural role and deployment model

1.2. Description

The EPC and 5GC support interworking with Non-3GPP IP access network such as WLAN through two approaches: Trusted Access and Untrusted Access, as specified in 3GPP TS 23.402 and TS 23.501.

A WLAN may advertise the PLMNs for which it supports trusted connectivity, including the applicable trusted access capabilities. Based on this information, UEs can discover such networks that provide trusted connectivity for one or more PLMNs.

In a non-roaming scenario, the determination is made by the HPLMN operator. If one or more security feature sets provided by the WLAN are considered insufficient by that operator, the network is treated as Untrusted WLAN.

In a roaming scenario, the UDM in the HPLMN makes the final determination based on the access network and visited network identities. The UDM may consider VPLMN policy, capabilities received from the AMF, and roaming agreements before classifying the access as Trusted or Untrusted.

This trusted and untrusted access to the WLAN network determines the type of GWs/NFs to be used, resulting in differences in authentication mechanisms, security controls, and interworking architecture.

The following sections describe the GWs/NFs involved in the interworking of the WLAN access networks and 3GPP core networks for 4G/5G systems.

1.2.1. TWAG

The TWAG is a gateway function within the Trusted WLAN Access Network (TWAN), which is functionally divided into three parts: the Trusted WLAN AAA Proxy (TWAP), the Trusted WLAN Access Gateway (TWAG) and WLAN Access Point (WLAN AP) representing one or more WLAN access points that provide radio connectivity to user equipment (UE). Figure 1 provides the key network elements and interfaces involved in the interworking of EPC and TWAN:

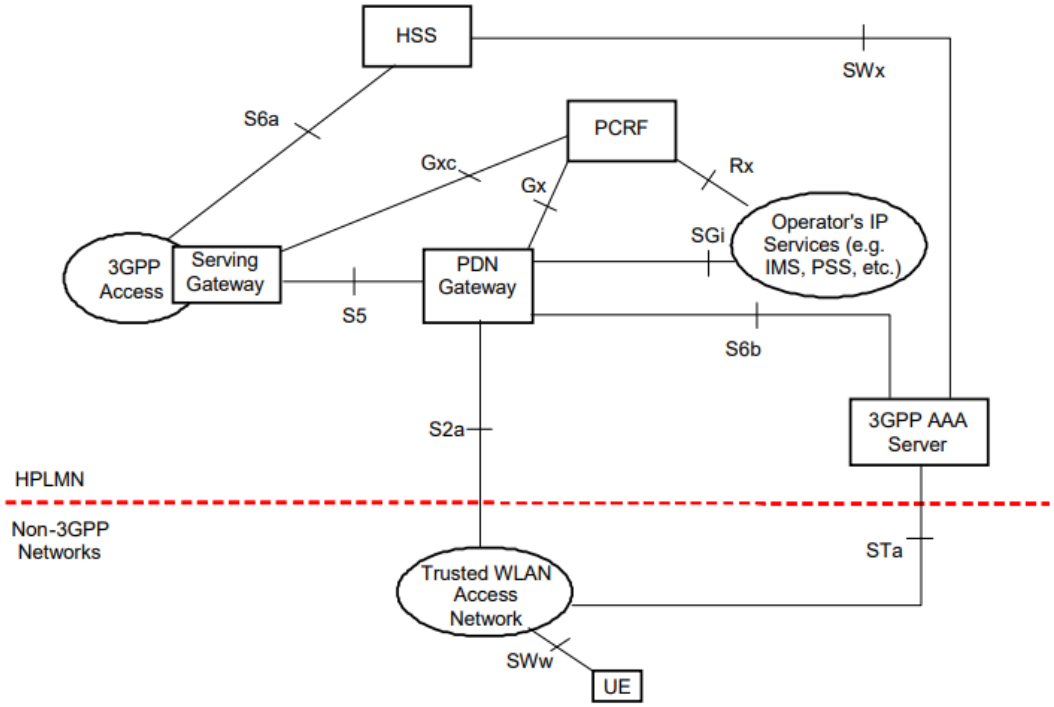

Figure 1: Functional Architecture for Trusted WLAN Access to EPC[2]

The key network elements involved in the interworking between EPC and TWAN are as follows:

a) **TWAG:** TWAG enables UEs to connect to the P-GW (Packet Data Network Gateway) through a TWAN, securely and efficiently offloading data traffic from WLAN to the cellular network. It serves as the gateway between the trusted WLAN and the EPC via the S2a interface, leveraging IEEE 802.11-2012 security features (802.11i/AES) over the SWw interface between the UE and WLAN Access Network, eliminating the need for an IPsec tunnel.

b) **TWAP**: It relays AAA information between the WLAN Access Network and the 3GPP AAA server. It also establishes a binding between the UE's

[2] *3GPP TS 23.402: Universal Mobile Telecommunications System (UMTS); LTE; Architecture enhancements for non-3GPP accesses*

subscription data (including IMSI) and its MAC address within the WLAN Access Network, and provides the TWAG with the UE's subscription data during the initial attach or when the subscription data is updated.

c) **3GPP AAA Server**: The 3GPP AAA (Authentication, Authorization, and Accounting) server provides authentication and authorization to UEs accessing EPC through the trusted WLAN using EAP-based procedures.
d) **HSS:** The HSS (Home Subscriber Server), is the master user database that supports the IMS network entities and provides information about the subscriber's location and IP information.
e) **PGW:** The PGW provide PDN connectivity to the UEs over TWAN. It enforces policy and charging, performs packet filtering.
f) **PCRF:** The PCRF (Policy and Charging Rules Function) determines policy rules in the IMS network for the connected UE.

The TWAN supports the following reference points, as defined in 3GPP TS 23.402, to enable interworking with the EPC:

a) **S2a:** Between TWAG and P-GW for authentication, authorization, and mobility management.
b) **SWw:** Between WLAN UE and WLAN AN handles authentication, IP address allocation, and security (such as encryption and integrity protection).
c) **STa:** Between the TWAG and the 3GPP AAA server to support non-roaming EAP-based authentication and authorization over trusted WLAN access.

1.2.2. ePDG

The ePDG is a key component in the EPC which acts as a security gateway, ensuring secure interworking between the EPC and untrusted WLAN access network by establishing an IPSec tunnel between the UE and the ePDG. Figure 2 provides the key network elements and interfaces involved in the interworking of EPC and untrusted WLAN via ePDG:

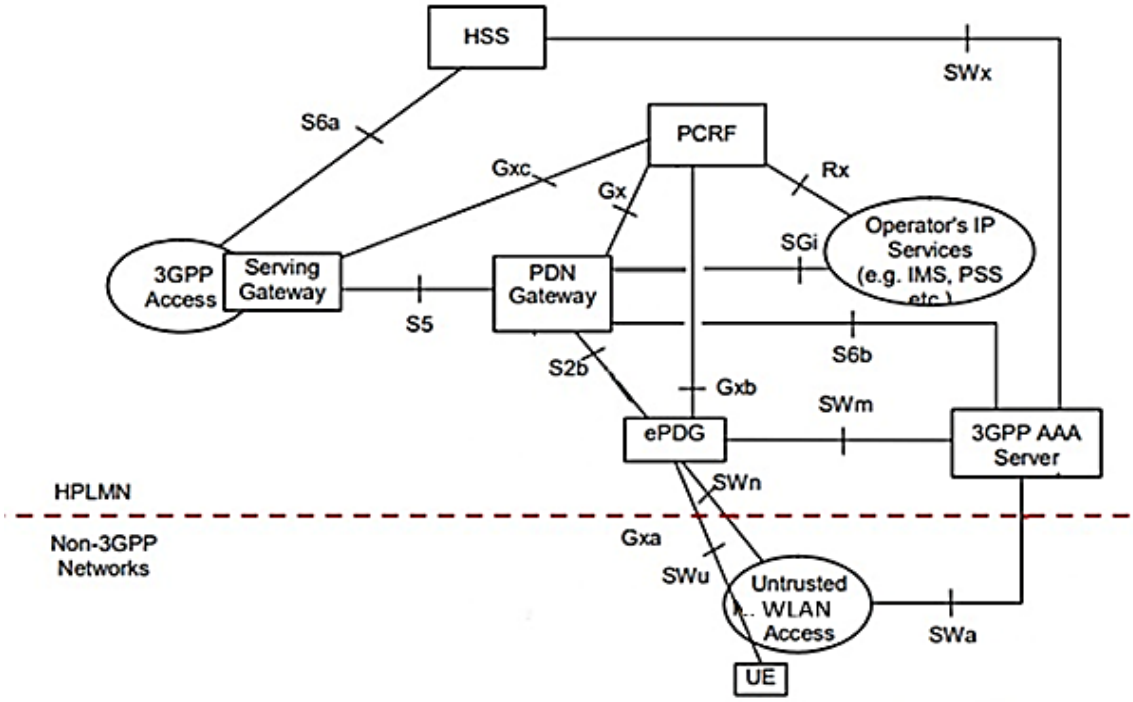

Figure 2: Functional Architecture for Untrusted WLAN Access to EPC[3]

The network elements involved in the interworking between EPC and untrusted WLAN access are as follows:

a) **ePDG:** It enables interworking between the EPC and untrusted WLAN access network through the establishment of an IPsec tunnel between the UE and the ePDG.

b) **P-GW:** The P-GW allocates an IP address to the subscribers and provides connectivity to external PDNs. The P-GW acts as mobility anchor for both trusted and untrusted WLAN access networks.

c) **3GPP AAA Server:** The 3GPP AAA server provides UE authentication via the EAP-AKA (Extensible Authentication Protocol - Authentication and Key Agreement) authentication method.

d) **HSS:** The HSS, is the master user database that supports the IMS network entities and provides information about the subscriber's location and IP information.

e) **PCRF:** The PCRF determines policy rules in the IMS network for the connected UE.

[3] *3GPP TS 23.402: Universal Mobile Telecommunications System (UMTS); LTE; Architecture enhancements for non-3GPP accesses*

The ePDG supports the following reference points, as defined in 3GPP TS 23.402, to enable interworking between EPC and untrusted WLAN access network:

a) **S2b:** Between ePDG and P-GW. It supports both the user plane and the associated control functions, and facilitates mobility management between the ePDG and the P-GW.

b) **SWu**: Between UE and ePDG. It supports the establishment, maintenance, and termination of IPsec tunnels for secure communication over the untrusted WLAN.

c) **SWm**: Interface between 3GPP AAA Server and ePDG supports AAA signaling for user authentication and authorization using EAP-based procedures.

1.2.3. N3IWF

The N3IWF in a 5G network facilitates interworking between an untrusted WLAN and the 5G core network. When a UE requires access to 5GC services over an untrusted WLAN, it establishes an IPsec tunnel with the N3IWF following the WLAN connection setup. The N3IWF provides IPsec-based secure connectivity towards the UE, while simultaneously supporting both N2 (control plane) and N3 (user plane) interfaces towards the 5GC. Figure 4 illustrates the network elements and interfaces involved in the interworking between 5GC and untrusted WLAN.

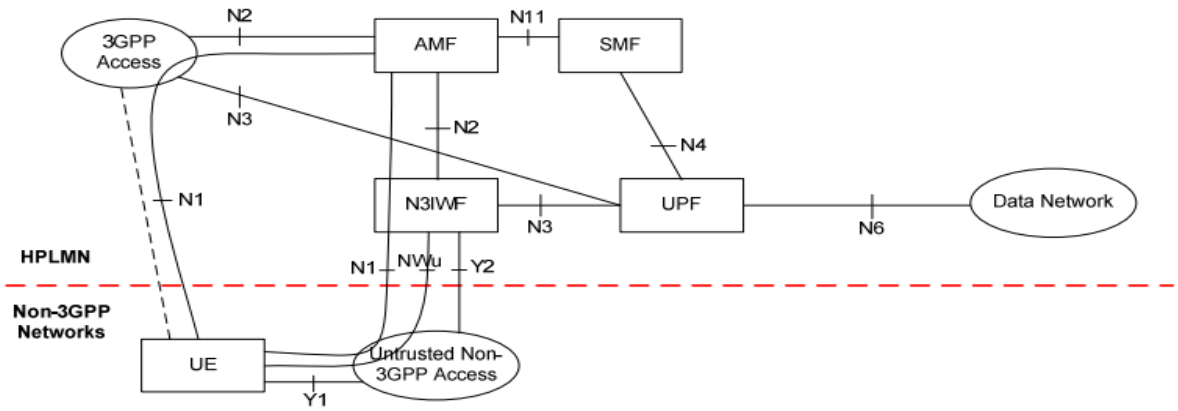

Figure 3: Functional architecture of 5G core network interworking with untrusted Non-3GPP Access[4]

[4] *3GPP TS 23.501: 5G; System architecture for the 5G System (5GS)*

The network elements involved in the interworking between 5GC and untrusted WLAN access are as follows:

a) **N3IWF:** The N3IWF terminates the IKEv2/IPsec protocols with the UE over NWu and relays over N2 the information needed to authenticate the UE and authorize its access to the 5G Core Network.
b) **AMF:** The AMF (Access and Mobility Function) manages UE registration, authentication, and mobility procedures. It interfaces with the N3IWF over N2 to handle signaling and control-plane function.
c) **SMF:** The SMF (Session Management Function) is responsible for managing PDU sessions, including session establishment, modification, and release. It handles N2 signaling related to PDU sessions and QoS, which is relayed to the N3IWF via the AMF.
d) **UPF:** The UPF (User Plane Function) handles user-plane traffic forwarding between the N3IWF and external Data Networks. It enforces QoS and traffic policies and connects to the N3IWF over N3 and to Data Networks over N6.

The N3IWF supports the following reference points, as defined in 3GPP TS 23.501, to enable interworking between 5GC and untrusted WLAN access network:

a) **NWu:** Between the UE and N3IWF for establishing secure tunnel(s) between the UE and N3IWF so that control-plane and user-plane exchanged between the UE and the 5G Core Network is transferred securely over untrusted WLAN.
b) **Y1:** Between the UE and the untrusted WLAN.
c) **Y2:** Between the WLAN and the N3IWF for the transport of NWu traffic.
d) **N1:** Between the UE and the AMF used NAS signaling over the secure tunnel established via the N3IWF.
e) **N2:** Between the N3IWF and the AMF for the control-plane signaling to support registration, connection management, and mobility procedures.
f) **N3:** Between the N3IWF and the UPF for user-plane data transfer between the UE and the 5GC.

1.2.4. TNGF

The TNGF is a network function within a Trusted Non-3GPP Access Network (TNAN), which also includes the Trusted Non-3GPP Access Point (TNAP). The TNAP provides access connectivity between the UE and the TNGF, while the TNGF

provides interworking between the TNAN and the 5G Core (5GC). TNGF enables UEs connected via TNAN to access the 5G Core, enabling them to access services such as mobility, session continuity, and policy enforcement.

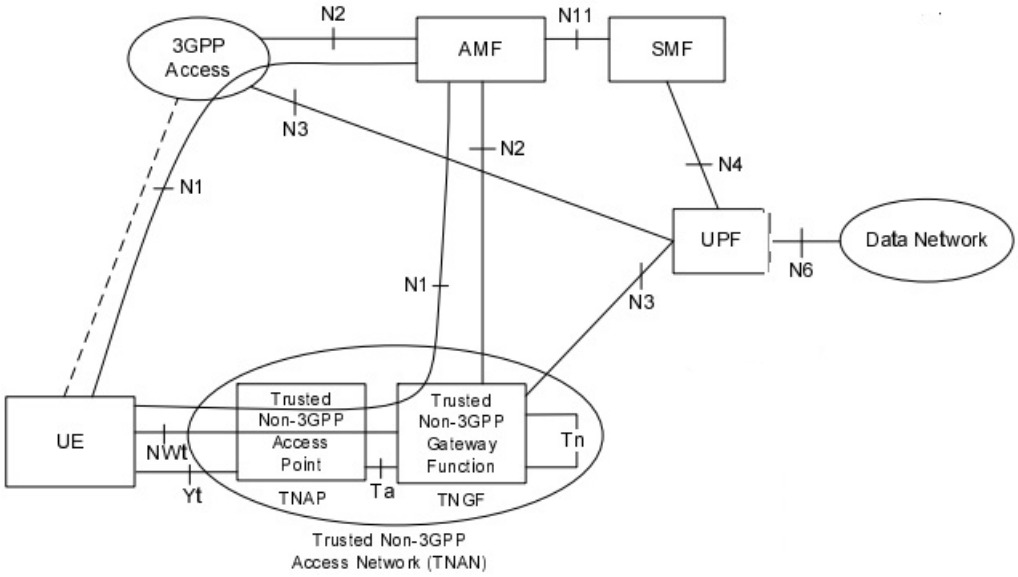

Figure 4: Functional architecture of 5G core network interworking with untrusted Non-3GPP Access[5]

The key network elements involved in interworking between the TNAN and the 5GC through the TNGF are as follows:

a) **TNGF:** The TNGF provides interworking between the TNAN and the 5G Core Network. It connects with the Access and Mobility Management Function (AMF) over the N2 interface for control-plane signaling, and with the User Plane Function (UPF) over the N3 interface for user-plane data transfer.
b) **AMF:** The AMF handles UE registration, mobility management, and authentication procedures. It interfaces with the TNGF via N2 and with the Session Management Function (SMF) via N11.
c) **SMF:** The SMF manages PDU sessions, including IP address allocation, policy control, and session lifecycle management. It interacts with the AMF over N11 and the UPF over N4.
d) **UPF:** The UPF handles user-plane packet forwarding between the TNGF and the Data Network (DN). It enforces QoS and policy rules, and connects via N3 (to the TNGF) and N6 (to the DN).
e) **TNAP:** It represents a trusted WLAN or fixed access network connecting the

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

UE to the TNGF. It interfaces with the UE via the Yt interface, and connects to the TNGF via Ta for transport and control signaling.

The TNGF supports the following reference points, as defined in 3GPP TS 23.501, to enable interworking between 5GC and TNAN:

a) **N1**: Between the UE and AMF. It carries Non-Access Stratum (NAS) signaling for registration, authentication, and mobility management.
b) **N2**: Between the TNGF and AMF. This interface handles control-plane signaling, including session management and mobility procedures.
c) **N3**: Between the TNGF and UPF. It is responsible for user-plane data transfer between the UE and external data networks.
d) **Ta:** Between the TNGF and TNAP. It supports access authentication and mobility management functions.
e) **NWt**: Between the UE and the TNGF. A secure NWt connection is established over this reference point and NAS messages between the UE and the AMF are transferred via this NWt connection.
f) **Yt**: Between the UE and TNAP for radio link connection over TNAN. It facilitates the radio link and initial access procedures.

1.2.5. TWIF

A TWIF is a network function with which act as a gateway between a Trusted WLAN Access Network (TWAN) and the 5GC for Non-5G capable over WLAN (N5CW) devices. The TWIF enables N5CW connected through the TWAN to access the 5GC, enabling them to access services such as mobility, session continuity, and policy enforcement just like on 3GPP access. The TWIF operates within the TWAN, alongside the Trusted WLAN Access Point (TWAP), which provides radio connectivity to the UEs.

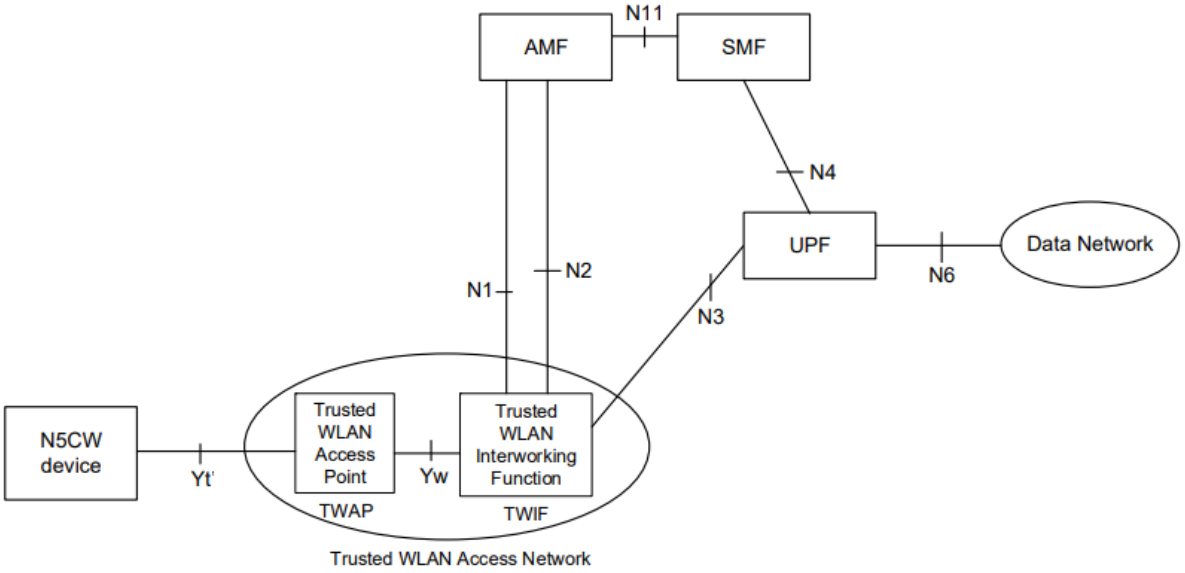

Figure 5: Functional architecture of 5GC interworking with TWAN for N5CW devices[6]

The key network elements involved in interworking between the TWAN and the 5GC through the TWIF are as follows:

a) **TWIF:** The TWIF provides interworking between trusted WLAN and the 5G Core for N5CW devices. It connects with the Access and Mobility Management Function (AMF) over the N2 interface for control-plane signaling and with the User Plane Function (UPF) over the N3 interface for user-plane data transfer.

b) **AMF:** The AMF handles UE registration, mobility management, and authentication procedures. It interfaces with the TWIF via N2 and with the SMF via N11.

c) **SMF:** The SMF manages PDU session establishment, IP address allocation, and policy control. It interacts with the AMF over N11 and the UPF over N4.

d) **UPF:** The UPF handles user-plane packet forwarding between the TWIF and the Data Network (DN). It enforces Quality of Service (QoS) and policy rules, connecting via N3 (to the TWIF) and N6 (to the DN)

e) **DN:** Represents external networks such as the Internet, IMS, or enterprise networks, which provide services to the UE through the UPF.

f) **TWAP (Trusted WLAN Access Point):** Represents the trusted WLAN access providing radio connectivity to the UE via the Yt′ interface, and connects to the TWIF via the Yw interface for control and user-plane data transport.

[6] *3GPP TS 23.501: 5G; System architecture for the 5G System (5GS)*

The TWIF supports the following reference points, as defined in 3GPP TS 23.501, to enable interworking between 5GC and TWAN:

a) **N1:** Between the TWIF and AMF for UE NAS signaling on behalf of N5CW UE.
b) **N2:** Between the TWIF and AMF for control-plane signaling.
c) **N3:** Between the TWIF and UPF for user-plane data transfer.
d) **Yw:** Between the TWIF and TWAP supports the following functions:
    - Transport of authentication messages between the TWAP and the TWIF to enable authentication of an N5CW device.
    - Allowing the N5CW device to request and receive IP configuration parameters from the TWIF, including the allocation of an IP address (e.g., via DHCP).
    - Transport of user-plane traffic between the N5CW device and the TWIF.

1.2.6. NSWOF

NSWOF is a network function in 5GS, which supports authentication for Non-seamless WLAN offload (NSWO). NSWO is an optional capability of a UE supporting WLAN radio access. A UE supporting non-seamless WLAN offload may, while connected to WLAN access, route specific IP flows directly via the WLAN access without traversing the 3GPP core network, while other IP flows continue to be served via the 3GPP data path. NSWOF enables the UE to connect to a WLAN access network using 5GS credentials without registration in 5GS.

Figure 6 (a). Reference architecture to support authentication for Non-seamless WLAN offload in 5GS[7]

[7] *3GPP TS 33.501: 5G; Security architecture and procedures for 5G System*

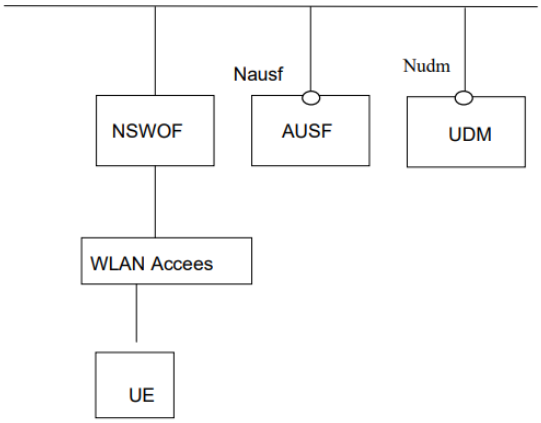

Figure 6 (b). Service based reference architecture to support authentication for NSWO in 5GS[8]

The key network elements involved in NSWO between the WLAN access network and the 5GS are as follows:

a) **NSWOF:** It enables a UE to connect to a WLAN access network using its 5GS credentials without registration to 5GS.
b) **AUSF:** The Authentication server function (AUSF) handles authentication requests for WLAN Access from UE. It informs the UDM that a successful or unsuccessful authentication of a subscriber has occurred.
c) **UDM:** The Unified Data Management (UDM) holds subscriber data relevant to authentication and policy and connects to AUSF via N13

The NSWOF architecture supports the following reference points, as defined in 3GPP TS 23.501, to enable interworking between 5GC and WLAN access network:

a) **SWa:** It connects the WLAN access network with the NSWOF and transports access authentication, authorization and charging-related information.
b) **N60:** Reference point between AUSF and NSWOF.
c) **N13:** Reference point between the UDM and Authentication Server function the AUSF
d) **Nausf:** NSWOF interfaces the AUSF using the Nausf SBI performing protocol translation and AUSF discovery

[8] *3GPP TS 33.501: 5G; Security architecture and procedures for 5G System*

CHAPTER 2

2. Functional Requirements

2.1. ePDG Functional requirements

2.1.1. The SWu interface shall carry IPSec tunnels.

2.1.2. The UE and the ePDG shall use IKEv2 signaling in order to establish IPSec security associations. ePDG shall also support the negotiation of configuration attributes such as IP address, DNS, and P-CSCF in the CP (Configuration Parameters) payload of IKE_AUTH Request and Response messages.

2.1.3. ePDG shall also support:

a. DNSSEC validation when querying PGW DNS records to prevent spoofing.

b. IKEv2 rekeying procedure for long-lived tunnels.

c. IKEv2 fragmentation (RFC 7383) for large messages over SWu.

2.1.4. The interface to the P-GW, the S2b interface shall run GTPv2 protocol to establish WLAN UE sessions with the P-GW.

2.1.5. The SWm interface is the reference point between the ePDG and the 3GPP AAA server. It shall authenticate and authorize the Wireless Local Area Networks (WLAN) User Equipment (UE) access.

2.1.6. ePDG shall support the Diameter (may optionally support Radius) client function to connect with the AAA server. The node shall adopt the Extensible Authentication Protocol-Authentication and the Key Agreement (EAP-AKA) authentication method to authenticate the User Equipment (UE). In the authentication model, the ePDG acts as the authenticator, and the UE is the EAP peer and the AAA server is the EAP authentication server.

2.1.7. ePDG shall support mapping of SWm to SWu error codes so that device can identify whether its temporary failure or permanent and can accordingly try connecting to the ePDG.

2.1.8. ePDG may include protocol configuration information, such as IPv4 and/or IPv6 DNS requests, when sending mobility management signaling messages (e.g., Proxy Binding Update) towards the P-GW, to allow the UE to obtain necessary IP configuration parameters

2.1.9. ePDG shall support emergency APN session to enable emergency voice calls over WLAN access (VoWiFi).

2.1.10. ePDG shall support collection and display of bearer-level duration information for each active bearer established during a PDN session. The information shall be available at the QCI level, and include at minimum: Bearer identifier (default/dedicated), QCI value), start and stop time of the bearer, total bearer duration.

2.1.11. The operator providing the untrusted WLAN access solution through ePDG may enable fast-reauthentication in AAA-server and UE in order to perform faster authentication and reduce the load in HSS. (Optional)

2.1.12. ePDG shall support offline charging for WLAN 3GPP IP Access, involving the following functions:

a. Charging Trigger Function
b. Charging Data Function
c. Ga Reference Point

2.1.13. ePDG shall support CDRs to bill the UEs for network resource usage as defined in 3GPP specification TS32.298.

2.1.14. ePDG Offline Charging feature shall populate the following additional fields:

a. IKEv2 tunnel endpoint IP address (UE Side tunnel endpoint address)
b. Source Port number used in IKEv2 tunnel
c. ePDG SWu interface IP address (ePDG side tunnel endpoint address)
d. Destination Port number used in IKEv2 tunnel
e. AP-MAC address used by UE to connect in WLAN network

2.1.15. The ePDG shall select P-GW node based one of the logic:

a. DNS
b. DNS over TCP
c. P-GW re-selection on session timeout
d. PGW re-selection on call attempt failure due to PGW reject

2.1.16. ePDG may support extended DNS client to handle DNS response larger than 512 bytes.

2.1.17. ePDG shall support dynamic P-GW node selection by attempting to set up the PDN connection with the next P-GW entry from the P-GW candidate list returned during the S-NAPTR procedure, if the initially selected P-GW is unreachable.

2.1.18. ePDG shall attempt to select an alternate PGW when the initial PGW

rejects the call with specific error causes (e.g., cause code 64 or 73). The ePDG shall continue PGW selection attempts sequentially from the configured PGW list until a successful connection is established or until the PGW list is exhausted.

2.1.19. VoLTE Support

a. ePDG shall support VoLTE call marking when the dedicated bearer corresponding to the QCI configured as VoLTE is created

b. ePDG shall allow the data for non-VoLTE calls during Inter Chassis Session Recovery (ICSR) switchover to reduce the data-outage for non-VoLTE calls and is configuration controlled to either allow data traffic for both VoLTE and non-VoLTE calls or only VoLTE calls.

2.1.20. ePDG shall support IKEv2 (Internet Key Exchange version 2) and IPSec (IP Security) ESP (Encapsulating Security Payload) encryption as per RFCs 4303 and 5996.

2.1.21. ePDG shall support DPD (Dead Peer Detection) protocol messages originating from the ePDG and the WLAN UEs.

2.1.22. ePDG shall be capable of authenticating itself to the UE using certificates and does so in the response to the first IKE_AUTH Request message from the UE.

2.1.23. ePDG shall support hash and URL based encoding of certificate payloads in IKE exchanges.

2.1.24. ePDG shall support inter-access handovers between two different interfaces, such as a handover between a 3GPP network and an untrusted WLAN access network, or between two untrusted WLAN access networks.

2.1.25. ePDG shall propagate the MAC (Media Access Control) address of each WLAN access point to the P-GW.

2.1.26. ePDG shall support ICSR with fault detection and automatic switch over. The subscriber session details for all ePDG interfaces are replicated in stand by, in case of a switchover, the new chassis processes all subsequent control and data traffic for the subscriber session.

2.1.27. The ePDG shall support IKEv2 Cookie challenge payload, this feature helps protect against opening too many half-opened IPSec sessions.

2.1.28. The ePDG shall support following IPv6 capabilities:

a. Support for any combination of IPv4, IPv6, or dual stack IPv4/v6 address

assignment from address pools on the P-GW

b. Support for native IPv6 transport and service addresses on the GTPv2 S2b interface with the P-GW

2.1.29. The ePDG shall support incoming IKEv2 requests from UE over an IPv6 transport as well

2.1.30. ePDG shall support Lawful Interception (LI).

2.1.31. If no appropriate PGWs can be selected from the DNS server after the DNS query, or if the DNS server is undeployed, ePDG shall perform the PGW selection from the local PGW list configured for each APN. The local APN configuration table shall contain one or multiple configurable local PGW addresses. The selection preference of the local PGW addresses shall be configured in the local APN configuration table based on the priority and weight attributes configured for each particular local PGW.

2.1.32. The ePDG service shall be configured indicating preferred method of PGW selection, whether local configuration or DNS/AAA server based PGW selection. Local Configuration based PGW selection as fallback mechanism shall be default configuration behavior.

2.1.33. ePDG shall support connectivity of non-UICC devices to EPC via ePDG using certificate-based UE authentication subsequent to authorization by the AAA server.

2.1.34. ePDG shall support the X.509 certificate-based authentication and also communicates with OCSP (Online Certificate Status Protocol) server for completing the authentication for non-UICC devices.

2.1.35. ePDG shall support both UICC and non-UICC devices simultaneously for same ePDG service.

2.1.36. ePDG shall receive the IMEI information from the UE over SWu interface and communicate the same to AAA server over the SWm interface.

2.1.37. ePDG shall support PDN connection, session establishment and release, along with support for dedicated bearer creation, deletion and modification that is initiated by the P-GW

2.1.38. ePDG shall send a "delete session request" message to P-GW, and shall handle the corresponding "delete session response" message from the P-GW during the following scenarios:

a. UE/ePDG initiated detach with GTP on S2b

b. UE requested PDN disconnection with GTP on S2b
c. AAA initiated detach with GTP on S2b

2.1.39. ePDG shall handles the received "create bearer request" message and shall send a "create bearer response" message for the dedicated bearer creation triggered from the P-GW.

2.1.40. ePDG also stores mapping information between the uplink packet filters received from the P-GW (For example; in the Create Bearer Request message), and the corresponding S2b bearer.

2.1.41. ePDG receives the "delete bearer request" message and sends a "delete bearer response" message for the dedicated bearer deletion triggered by the P-GW.

2.1.42. ePDG shall support path failure detection for control plane by using Echo Request and Echo Response messages. A peer's IP address-specific counter shall be reset every time an Echo Response message is received from the peer's IP address.

2.1.43. ePDG shall support session recovery for IPv4, IPv6, and IPv4/v6 sessions and ensure that data and control planes are re-established as they were before the recovery procedure.

2.1.44. ePDG shall support the static UE IP address communicated by AAA to ePDG over SWm interface (as Served-Party-IP-Address AVP in DEA). ePDG shall also communicate the same to PGW over S2b interface (as PAA IE of create session request GTP message).

2.1.45. ePDG shall support both single-connection mode and multi-connection mode for PDN connectivity

a. To support IPv4 connectivity, the P-GW shall allocate the IPv4 address during PDN connection establishment. The ePDG shall relay the assigned IPv4 address and associated configuration parameters to the UE via the IKEv2/IPSec tunnel using Protocol Configuration Options (PCO).

b. To support IPv6 connectivity, the P-GW shall handle Router Solicitation (RS) and Router Advertisement (RA) messages within the tunnel, enabling Stateless Address Auto Configuration (SLAAC) on the UE. For IPv6 parameter configuration (e.g., DNS servers), the UE may use stateless DHCPv6, with the P-GW acting as the DHCPv6

server. The ePDG shall support relaying such IPv6 configuration messages transparently between the UE and the P-GW.

2.2. TWAG Functional Requirements

2.2.1. TWAG shall act as DHCPv4/v6 server for the UE and shall handle the Router Solicitation and Router Advertisement (RS/RA) signaling for Stateless Address Auto Configuration.

2.2.2. TWAG shall support the following in both single-connection mode and multi-connection mode:

a. To support IPv4 connectivity, the IPv4 address shall be allocated and sent to the UE during PDN connection establishment.

b. To support IPv6 connectivity, the PGW shall handle the RS/RA messages and to support IPv6 parameter configuration the UE may use stateless DHCPv6. The PGW shall acts as DHCPv6 server.

2.2.3. The PDN connectivity service shall be provided by the point-to-point connectivity between the UE and the TWAG concatenated with S2a bearer(s) between the TWAG and the P-GW.

2.2.4. The TWAG shall handle the uplink packets based on the uplink packet filters in the Traffic Flow Templates (TFTs) received from the PDN GW for the S2a bearers of the PDN connection in the same way as an ePDG does for GTP based S2b interface.

2.2.5. The trusted access may be used in the following modes:

a. **Single-connection mode:** Support of a single connection at a time (non-seamless or with a single PDN connectivity). The use of the Single Connection mode and the associated parameters of the connection can be negotiated during authentication over TWAN. Seamless mobility between accesses in this mode is possible.

b. **Multi-connection mode:** This mode support multiple connections simultaneously. One connection may be used for Non-Seamless offload and one or more simultaneous connections may be used for PDN connectivity.

c. **Non-Seamless offload mode:** This mode does not make use of a P-GW (however EAP-AKA' supported) and the traffic is routed directly to an external data network via the TWAG. It can also be considered as a specific case of a Single connection mode.

d. **Transparent connection mode:** Single connection to P-GW using S2a but without mobility support between 3GPP and WLAN. Selective

offload (e.g. moving one PDN out of two from one access to another) is not possible. This nomadic PDN connectivity enables to have a consistent 3GPP service (re-use of PGW functionalities) while using a WLAN.

2.2.6. TWAG shall establish a dedicated point-to-point link per UE for traffic routed over the S2a interface.

2.2.7. TWAG shall transport user plane traffic for every PDN connection or S2a bearer

2.2.8. The UE's MAC address and an associated TWAG's MAC address shall be used to identify the point-to-point link between the UE and its serving TWAG that is associated to a specific PDN connection or S2a bearer

2.2.9. TWAG shall support TWAG-CP and TWAG-UP Address.

2.2.10. TWAG shall locally disconnect the PDN connection towards the UE without any WLCP signalling between the TWAG and the UE, in case when TWAG needs to stop a procedure or close a PDN connection.

2.2.11. TWAG shall abort the procedure and deactivate the PDN connection locally without any peer-to-peer WLCP signalling between the TWAG and the UE, when there is a need arises

2.2.12. The TWAG shall implement procedures to handle cases where an unknown, erroneous, or unexpected Procedure Transaction Identity (PTI) is received in a WLAN Control Plane (WLCP) message from the UE

2.2.13. TWAG shall use the standardized WLCP UDP port number as both the source UDP port and the destination UDP port when transmitting WLCP messages to and from the UE.

2.2.14. The UE shall use the IP address of the selected TWAG control-plane address as the destination IP address of WLCP messages.

2.2.15. The UE shall apply the following procedures to set the source IP address of the WLCP message:

a. If the TWAG IP address for WLCP is an IPv4 address and if the UE supports IPv4, the UE shall obtain an IPv4 address via DHCPv4 to be used as the source IP address for WLCP;

b. If the TWAG IP address for WLCP is an IPv6 link-local address and if the UE supports IPv6, the UE shall use the IPv6 link-local address configured on the WLAN interface as the source IP address for WLCP;

and

c. If the TWAG IP addresses for WLCP are an IPv4 address and an IPv6 link-local address, which IP version the UE selects depends on the implementation.

2.2.16. The TWAN shall include TWAG Control Plane IP Address Information Element (IE) if it indicates support of the Multiple Connectivity Mode (MCM) in the Supported TWAN Connection Modes IE. This IE shall contain the TWAG Control Plane IPv4 Address, or the TWAG Control Plane IPv6 link local address, or both (if the TWAG supports IPv4 and IPv6), to be used for WLCP by the UE if the MCM is used.

2.2.17. The TWAG shall use a TWAG control plane address which was included in TWAG_CP_ADDRESS item provided to the UE during EAP-AKA' authentication as described in 3GPP TS 24.302, as the source IP address for WLCP

2.2.18. The TWAG shall use the TWAG control plane address of the same IP version as the IP version received from the UE in the WLCP message

2.2.19. The TWAG shall use the source IP address received from the UE in the WLCP message as the destination IP address for further WLCP message to the UE.

2.2.20. TWAG may include a Protocol configuration options IE in PDN connectivity establishment procedure in order to exchange (protocol) data (e.g. configuration parameters, error codes or messages/events).

2.2.21. When the TWAG receives a failure indication of the EAP-AKA’ re-authentication procedure, the TWAG shall initiate TWAG-initiated PDN disconnection procedure.

2.3. N3IWF Functional Requirements

N3IWF acts as a gateway for the 5GC with support for N2 and N3 interface towards the 5GC.

2.3.1. The N3IWF shall support of IPsec tunnel establishment with the UE. The N3IWF terminates the IKEv2/IPsec protocols (with IKEv2 fragmentation support) with the UE over NWu and relays over N2 the information needed to authenticate the UE and authorize its access to the 5G Core Network.

2.3.2. The N3IWF shall support termination of N2 and N3 interfaces to 5G Core Network for control - plane and user-plane respectively.

2.3.3. The N3IWF shall provide both control plane and user plane connectivity between the UE connected via untrusted WLAN access and the 5G Core Network.

2.3.4. The N3IWF shall support initial registration for UEs accessing via untrusted WLAN networks.

2.3.5. The N3IWF shall support relaying uplink and downlink control-plane NAS (N1) signalling between the UE and AMF.

2.3.6. The N3IWF shall support handling of N2 signalling from SMF (relayed by AMF) related to PDU Sessions and QoS.

2.3.7. The N3IWF shall ensure integrity protection, confidentiality, and replay protection for all traffic exchanged over the untrusted access network.

2.3.8. The N3IWF shall support establishment of IPsec Security Association (IPsec SA) to support PDU Session traffic.

2.3.9. The N3IWF shall support relaying uplink and downlink user-plane packets between the UE and UPF. This involves:

a. De-capsulation/ encapsulation of packets for IPSec and N3 tunnelling
b. Enforcing QoS corresponding to N3 packet marking, taking into account QoS requirements associated to such marking received over N2 - N3 user-plane packet marking in the uplink.

2.3.10. The N3IWF shall support the following Control Plane functionalities:

a. Support of IPsec tunnel establishment with the UE over NWu using IKEv2/IPsec protocols.
b. Establishment of signalling IPsec Security Associations (SAs) for securing NAS messages.

c. Establishment of IPsec SAs for securing PDU session traffic.
d. Termination of the N2 interface towards the AMF using NGAP (Next-Generation Application Protocol) over SCTP Stream Control Transmission Protocol (This makes N3IWF act like a "gNB control-plane proxy" for the UE on untrusted Wi-Fi)
e. Relaying uplink and downlink NAS (N1) signalling messages between the UE and AMF.
f. Support of NAS messages for UE authentication, registration, and authorization of access to the 5GC.
g. Support of NAS messages for PDU session establishment.
h. Handling of N2 signalling from the SMF (relayed via the AMF) related to PDU sessions and QoS.
i. Support of AMF selection.
j. Support of local mobility anchor within untrusted WLAN access networks using MOBIKE (IETF RFC 4555).

2.3.11. N3IWF shall support the following user-plane functionalities:
a. Termination of the N3 interface towards the UPF using the GTP-U protocol.
b. Relaying uplink and downlink user-plane packets between the UE and UPF.
c. Decapsulation and encapsulation of packets for IPsec and GTP-U tunnelling.
d. Uplink N3 user-plane packet marking and enforcement of QoS based on QoS parameters received over N2.

2.3.12. N3IWF shall support QoS differentiation and mapping of QoS flows to WLAN access resources.

2.3.13. N3IWF shall support authentication of the UE using 5G-AKA or EAP-based authentication procedures.

2.3.14. N3IWF shall support mobility management procedures for UEs moving between 3GPP and untrusted WLAN accesses.

2.3.15. N3IWF shall support handover of PDU Sessions between untrusted WLAN access and 3GPP access without session interruption.

2.3.16. N3IWF shall support re-configuration of IPsec tunnels upon changes in UE connectivity (e.g., change of IP address).

2.3.17. The N3IWF shall support IPv4, IPv6, and dual-stack operation for IPsec tunnel establishment and transport.

2.3.18. The N3IWF shall support UE-specific access control and authorization using subscription data from the UDM via the AMF.

2.3.19. The N3IWF shall support Dead Peer Detection (DPD) to detect unresponsive UEs and tear down idle tunnels accordingly.

2.3.20. The N3IWF shall support IKEv2 redirection and multi-homing, allowing redirection of the UE to an alternate N3IWF instance if required.

2.3.21. The N3IWF shall maintain tunnel statistics including tunnel establishment time, duration, throughput, and packet counters for each active UE session.

2.3.22. The N3IWF shall support redundancy and session recovery by synchronizing IPsec and session contexts to standby nodes. In case of failover, the standby N3IWF shall resume session handling with minimal disruption.

2.3.23. The N3IWF shall support performance monitoring, including number of active IPsec tunnels, N2/N3 traffic counters, and control plane message counts, accessible through standard management interfaces.

2.3.24. The N3IWF shall support uplink and downlink packet filtering based on policies received from the SMF for each QoS flow.

2.3.25. The N3IWF shall support emergency PDU sessions over untrusted WLAN access as defined in 3GPP TS 23.167.

2.3.26. IMS Voice Support

a. N3IWF shall support IMS-based voice service (VoNR) over untrusted WLAN access by maintaining QoS flow identification for 5QI values configured for conversational voice, as specified in 3GPP TS 23.501 and TS 23.503.

b. N3IWF shall allow continuity of data traffic for IMS and non-IMS services during inter-chassis session recovery or switchover procedures, to minimize data outage. This behavior shall be configuration controlled to either allow data traffic for both IMS voice and non-voice services or restrict it to IMS voice traffic only.

2.3.27. The N3IWF shall support PDU Session establishment, modification, and release procedures over untrusted WLAN access. The N3IWF shall enable control and user plane establishment between the UE and the 5GC and

support SMF-initiated session modifications, including creation, deletion, or modification of QoS flows associated with a PDU Session.

2.3.28. The N3IWF shall support release of PDU Sessions as initiated by the UE, SMF, or network management entities. The N3IWF shall handle the corresponding session release procedures by:

a. Processing UE-initiated PDU Session release requests received over the NWu interface;
b. Handling Network initiated session release commands received over the N2 interface

2.3.29. The N3IWF shall ensure proper deletion of IPsec Child Security Associations (SAs) corresponding to the released PDU Session and notify the SMF of successful session termination.

2.3.30. N3IWF shall support dynamic discovery and selection of 5GC network functions (AMF, SMF, UPF) using DNS procedures as specified in 3GPP TS 23.501.

2.3.31. N3IWF shall support collection and reporting of PDU session–level statistics for each active session established via untrusted WLAN access. The information shall include, at minimum: PDU Session Identifier, 5QI value, session start and stop time, total session duration, and data volume counters for uplink and downlink directions.

2.3.32. The N3IWF shall support IKEv2 and IPsec ESP for establishment of secure tunnels with the UE over untrusted WLAN access, in accordance with RFCs 7296 and 4303.

2.3.33. The N3IWF shall support connectivity of non-UICC devices to the 5G Core via untrusted WLAN access using certificate-based UE authentication.

2.3.34. The N3IWF shall support connectivity for both UICC-based and non-UICC devices.

a. For UICC-based devices, the N3IWF shall support EAP-AKA′ authentication as defined in 3GPP TS 33.501
b. For non-UICC devices, where EAP-AKA′ is not applicable, the N3IWF shall support certificate-based authentication methods such as EAP-TLS in accordance with 3GPP TS 33.501 and RFC 5216.

2.3.35. The N3IWF shall be capable of authenticating itself to the UE using X.509 digital certificates during the IKEv2 authentication phase.

2.3.36. The N3IWF shall present its certificate to the UE in response to the initial IKE_AUTH Request message, as specified in RFC 7296 and 3GPP TS 33.501, to enable mutual authentication and establishment of the IPsec tunnel.

2.3.37. The N3IWF shall support hash-and-URL-based encoding of certificate payloads in IKEv2 exchanges in accordance with RFC 6920, RFC 7306, and RFC 7296, allowing efficient transmission of large certificates during IKE negotiation.

2.3.38. The N3IWF shall support inter-access mobility and handover procedures between 3GPP and untrusted WLAN access networks, and between multiple untrusted WLAN accesses The N3IWF shall ensure seamless service continuity by maintaining PDU session context and tunnel mapping during such inter-access handovers, under the control of the AMF and SMF

2.4. TNGF Functional Requirements

2.4.1. The functionality of the TNGF in the case of trusted WLAN access shall support the following:

a. Termination of the N2 and N3 interfaces.
b. Termination of EAP-5G signalling and acting as the authenticator when the UE attempts to register to the 5GC via the TNAN.
c. Implementation of the AMF selection procedure.
d. Transparent relaying of NAS messages between the UE and the AMF, via N2.
e. Handling of N2 signalling with the SMF (relayed by the AMF) for supporting PDU sessions and QoS.
f. Transparent relaying of PDU data units between the UE and UPF(s).
g. Support as a local mobility anchor within the TNAN.
h. Support for EAP Re-authentication (ER) server (as per RFC 6696) to facilitate mobility within the TNAN.

2.4.2. The TNGF shall act as the gateway between trusted WLAN access networks and the 5G Core Network, supporting the termination of the N2 interface for control plane and the N3 interface for user plane.

2.4.3. The TNGF shall support registration of the UE to 5GC via trusted WLAN access using the EAP-5G method, encapsulating NAS messages between the UE and the AMF.

2.4.4. The TNGF shall support the relaying of NAS signalling messages between the UE and the AMF over trusted WLAN access.

2.4.5. The TNGF shall support secure key establishment, where after successful authentication (EAP-5G), a TNGF key is derived and used for subsequent communication between TNGF, TNAP, and the UE, as specified in TS 33.501.

2.4.6. The TNGF shall include UE Location Information, including the TNAP ID and UE IP address, in N2 messages to the AMF.

2.4.7. The TNGF shall allocate an “inner” IP address to the UE as part of the authentication and NWt connection setup and provide the NAS_IP_ADDRESS, TCP port number, and DSCP value to the UE.

2.4.8. The TNGF shall support the establishment and maintenance of a TCP connection for the exchange of NAS messages encapsulated in TCP/IP/ESP between the UE and TNGF.

2.4.9. The TNGF shall support mobility procedures for UEs moving between TNAPs, requiring full re-authentication via the new TNAP upon movement.

2.4.10. The TNGF shall provide support for network-initiated and UE-initiated service request, context release, and selective deactivation of user-plane connections, following the mapped procedures from untrusted WLAN access with TNGF substitutions.

2.4.11. The TNGF shall support policy-controlled slice-specific trusted access selection, facilitating the use of updated UE policies and AMF/PCF interaction as specified.

2.4.12. The TNGF shall support emergency registration and PDU Session procedures as specified for trusted WLAN access.

2.5. TWIF Functional Requirement

2.5.1. The functionality of the TWIF in the case of trusted WLAN access shall support the following:

a. Terminates the N1, N2 and N3 interfaces.
b. Implements the NAS protocol stack and exchanges NAS messages with the AMF on behalf of the N5CW device.
c. Implementation of the AMF selection procedure.
d. On the user plane, it relays protocol data units (PDUs) between the Yw interface and the N3 interface.

e. May implement a local mobility anchor within the trusted WLAN access network.

2.5.2. The TWIF shall act as the gateway between Non-5G capable WLAN devices via TWAN and the 5G core network supporting the termination of the N1, N2 interfaces for control plane and the N3 interface for user plane.

2.5.3. TWIF shall perform the 5GC registration in TWAN, on behalf of the N5CW device

2.5.4. TWIF shall provide interworking functionality that enables connectivity with 5GC and implements the NAS protocol stack and exchanges NAS messages with the AMF on behalf of the N5CW device.

2.5.5. NAS security between AMF and TWIF shall be established similar to unauthenticated emergency calls, i.e. with NULL encryption and NULL integrity protection.

2.5.6. TWIF shall support EAP-AKA' authentication requests from N5CW UE in AAA messages.

2.5.7. The TWIF shall support secure key establishment, where after successful authentication (EAP-AKA'), a TWAP key is derived and used for secure WLAN air-interface communication between TWAP & UE.

2.5.8. TWIF shall support layer-2 & layer-3 connection with the Trusted WLAN Access Point for transporting all user-plane traffic of the N5CW device. The connection shall be bound to N3 connection created for the N5CW device.

2.5.9. TWIF shall support IP configuration of N5CW devices by performing PDU session establishment with the 5GC.

2.5.10. The TWIF shall include UE Location Information, including the TWAP ID and UE IP address, in N2 messages to the AMF.

2.5.11. TWIF shall support UE / 5GC Network initiated de-registration, context release, service requests procedures of the N5CW device as per 23.502.

2.6. NSWOF Functional Requirements

2.6.1. The NSWOF shall support interfacing to the WLAN access network using the SWa interface as defined in 3GPP TS 23.402

2.6.2. The NSWOF shall support interfacing with the Authentication Server Function (AUSF) using the Nausf Service-Based Interface (SBI).

2.6.3. The NSWOF shall support authentication of UEs connecting to a WLAN

using 5GS credentials without requiring 5GS registration, as specified in TS 33.501 Annex S.

2.6.4. The NSWOF shall utilize the Network Repository Function (NRF) to discover available AUSF instances unless AUSF information is available by other means (e.g., locally configured).

2.6.5. The NSWOF shall select an AUSF instance based on the list of available instances obtained from the NRF or local configuration

2.6.6. The NSWOF shall perform protocol translation between the SWa interface (RADIUS based) and the Nausf SBI (HTTP based) to enable authentication using 5GS credentials

2.6.7. During AUSF selection, the NSWOF shall consider the following parameters when available:

a. Home Network Identifier (MCC, MNC, realm) of SUCI/SUPI,
b. Routing Indicator,
c. Optionally the Home Network Public Key identifier.

2.6.8. The NSWOF shall support authentication procedures for Non-Seamless WLAN Offload in roaming scenarios, as defined in TS 23.501 Figures 4.2.15-3 and 4.2.15-4.

2.6.9. The NSOWF shall support 5G NSWO authentication procedure by the UE.

2.6.10. The NSWOF shall support applying operator-defined policies (for example from the UE or from a policy server) to determine whether a WLAN access qualifies for non-seamless offload. The NSWOF may support dynamic updates of these policies to reflect changing network conditions or operator preferences.

2.6.11. The NSWOF may support monitoring the status of the WLAN access network (e.g., availability, load, security level) in order to determine whether offload is feasible.

2.5.12. The NSWOF may support providing status feedback to upstream functions (e.g., NEF/NWDAF) for analytics or network optimization.

CHAPTER 3

3. Interoperability Requirements

The WLAN interworking GWs/NFs , namely ePDG, TWAG, N3IWF, TNGF,TWIF and NSWOFshall conform to the interoperability requirements specified below to ensure seamless integration with the 3GPP Core Network and WLAN access networks in multi-vendor environments.

3.1. The GWs/NFs shall interoperate with 3GPP Core Network functions from other vendors over the standardized interfaces as defined in relevant 3GPP TS and IETF RFCs.

3.2. The GWs/NFs shall interoperate with UE supporting trusted and untrusted WLAN access, using standard IPsec/IKEv2 and EAP-based authentication mechanisms as per 3GPP TS 33.501 and IETF RFC 4301 / RFC 5996.

3.3. The GWs/NFs shall interoperate with WLAN access networks using standard signaling and transport protocols without reliance on vendor-specific extensions.

3.4. The GWs/NFs shall not require proprietary interfaces or adaptations for interworking with other vendors' core network functions.

3.5. The GWs/NFs shall maintain interoperability across different 3GPP releases (as applicable) to ensure backward compatibility within evolving network environments.

CHAPTER 4

4. OMC/EMC Requirements

The OMC allows centralized operation of the various units in the system and functions needed to maintain the sub-systems. The OMC provides the dynamic monitoring and controlling of the network management functions.

4.1. Management Functions

The following management functions shall be carried out through the corresponding OMCs:

4.1.1 Configuration management

4.1.2 Fault report and alarm handling

4.1.3 Performance supervision/management

4.1.4 Storage of system software and data

4.1.5 Security management

4.2. OMC database

4.2.1 The OMC shall use persistent database to store and hold the necessary information for the parameters used in the OMC

4.2.2 The OMC database shall include configuration data, maintenance data, fault data and performance / QoS data

4.2.3 The OMC shall be capable of storage of the generated performance data. The methods and capacity of storage provided with the system shall be stated.

4.2.4 Provision shall be available for collection of statistical information relating to events in the network. Collection frequency should be configurable

4.2.5 The OMC database shall contain the fault history of the whole network under its command. As a minimum, it shall be possible to search and display data according to the following criteria:

a. Network elements
b. Severity class
c. Event type

4.3. OMC Generic Features

4.3.1 OMC software – UNIX/LINUX/Windows System Platform

4.3.2 It shall optionally support interface like CORBA / TCP / IP / CMIP / SNMP/ REST / HTTP etc., to enable it to work with a remote NMS.

4.3.3 Support Ethernet connectivity with remote network elements.

4.3.4 Graphical User Interface (GUI).

4.3.5 On-Line Help.

4.3.6 Consistency Checks.

4.3.7 Configuration Change/Event Log.

4.3.8 Object Alarm Status Management / Display.

4.3.9 Collection of PM counters.

4.3.10 Limited Access Restriction by User.

4.3.11 Access Restriction by Function and by Operation.

CHAPTER 5

5. General Requirements

5.1. The equipment shall be robust, reliable, and designed for continuous operation in Indian telecom network conditions without any degradation in performance

5.2. The equipment shall comply with relevant international standards and 3GPP specifications as referenced in this GR and shall support interoperability with multi-vendor 4G EPC and 5G Core network elements.

5.3. The hardware and software components shall support scalability to handle increased subscriber load, session capacity, and throughput requirements in line with operator deployments.

5.4. The equipment shall support remote configuration, operation, and management through standard management protocols (such as SNMP/NETCONF/REST APIs), and shall provide detailed alarms, logs, and performance counters.

5.5. The equipment shall provide redundancy for critical modules, interfaces, and power supplies to ensure high availability. In case of hardware or software failure, it shall support automatic recovery without service disruption.

5.6. The equipment shall be maintainable, supporting in-service software upgrades and diagnostics for quick fault localization and rectification.

5.7. Hardware

5.7.1. The system hardware shall be modular in design and shall permit growth in steps. The arrangement shall be such that failure/ deterioration of service shall not occur when implementing the growth.

5.7.2. The system hardware shall not pose any problem, due to changes in date and time caused by events such as changeover of leap year etc., in the normal functioning of the system

5.8. Input-Output devices

5.8.1. The communication facilities provided for exchange of information between the elements of core and the maintenance and operating personnel shall include facilities to perform various management functions

5.8.2. Adequate number of man-machine interfaces shall be available.

5.8.3. A suitable alarm and display system at OMC shall be provided for a continuous indication of the system status.

5.9. Equipment Practice

5.9.1. Suitable test access points and displays shall be provided for facilitating maintenance. Test access points shall be located on the front side of the bay. All visual display devices shall be located in a position attracting immediate attention of the operation and maintenance personnel.

5.9.2. For chassis-based systems, it shall be indicated whether printed board connectors are of edge-type or plug-and-socket type. They shall not be easily damaged during replacements and removals. The contact particulars as well as life test performance on contact resistance for each type of connector shall be supplied.

5.9.3. All components and material used in the equipment shall be non-inflammable or in absence of it, self-extinguishable. They shall be fully tropicalized

5.9.4. The buses, if any, shall be suitably protected against electrical and magnetic interference from neighboring systems (like electromechanical systems, fluorescent tubes, motors, etc.)

5.9.5. For chassis-based systems, the different plug-in cards shall have suitable mechanical safeguards to prevent damage due to accidental interchange of cards

5.9.6. The system shall provide for human isolation and protection from accidental high voltage power contact.

5.10. Software

5.10.1. The software shall be written in a High-Level Language.

5.10.2. The software shall be modular and structured.

5.10.3. The software shall include the following characteristics:

a. The design of the software shall be such that the system is easy to handle both during installation and normal operations as well as during extensions.

b. The design shall be such that propagation of software faults is contained.

c. Test programs shall include fault tracing for detection and localization of system faults.

5.11. Software Maintenance

5.11.1. All software updates, for a period as specified, shall be supplied on continuing basis. These updates shall include new features and services and other maintenance updates.

5.11.2. Integration of software updates without posing any problem to the existing

functionality shall be possible.

CHAPTER 6

6. Quality Requirements

6.1. The manufacturer shall furnish the MTBF values. Minimum value of MTBF shall be specified by the purchaser. The calculations shall be based on the guidelines given in either QA document No. QM-115 {January 1997} "Reliability Methods and Predictions" or any other international standards.

6.2. The equipment shall be manufactured in accordance with international quality management system ISO 9001:2015 or any other equivalent ISO certificate for which the manufacturer should be duly accredited. A quality plan describing the quality assurance system followed by the manufacturer would be required to be submitted.

6.3. The equipment shall conform to the requirements for Environment specified in TEC QA standards QM-333 {Issue- March, 2010} (TEC 14016:2010) "Standard for Environmental testing of Telecommunication Equipment" or any other equivalent international standard, for operation, transportation and storage. The applicable environmental category A or B to be decided by the purchaser based on the use case. (This requirement is applicable only for hardware-based solutions.)

CHAPTER 7

7. Safety, Security and EMI/EMC Requirements

7.1. Safety Requirements

The equipment shall conform to relevant safety requirements as per (IS/IEC 62368-1:2018 or Latest & IS 10437: 2019/IEC 60215: 2016) as prescribed under Table no. 1 of the TEC document 'SAFETY REQUIREMENTS OF TELECOMMUNICATION EQUIPMENT": TEC10009: 2024. (These requirements are applicable for purposely built hardware or a physical entity only).

7.2. Security Requirements

The WLAN interworking gateway functions mentioned in this GR, shall comply to the security requirements mentioned in the applicable Indian Telecommunication Security Assurance Requirements (ITSAR) as and when notified by National Centre for communication Security (NCCS)

7.3. EMI/EMC Requirements

These requirements are applicable for purposely built hardware or a physical entity only. (These requirements shall be as per TEC Standard No. TEC11016:2016 as modified/ amended from time to time(These requirements are applicable for purposely built hardware or a physical entity only).).

Clause	Parameter	Standard
1.	Conducted and Radiated Emission	CISPR 32 Class-A
2.	Immunity to Electrostatic discharge: Contact discharge level 2 {± 4 kV}	IEC-61000-4-2 Performance Criteria-B, Clause 9
3.	Immunity to Electrostatic discharge: Air discharge level 3 {± 8 kV}	IEC-61000-4-2 Performance Criteria-B, Clause 9
4.	Immunity to radiated RF: a) Radio Frequency: 80 MHz to 1 GHz, Electromagnetic field:	IEC 61000-4-3 (2010);

	3V/m b) Radio Frequency: 800 MHz to 960 MHz, Electromagnetic field: 10V/m c) Radio Frequency: 1.4 GHz to 6 GHz, Electromagnetic field: 10V/m	
5.	Immunity to fast transients (burst): Test Level 2: a) 1 kV for AC/DC power port b) 0. 5 kV for signal / control / data / telecom lines.	IEC 61000- 4- 4 {2012); Performance Criteria-B, Clause 9
6.	Immunity to surges: AC/DC ports a) 2 kV peak open circuit voltage for line to ground b) 1kV peak open circuit voltage for line to line	IEC 61000-4-5 (2014) Performance Criteria-B, Clause 9
7.	Immunity to surges: Telecom ports a) 2 kV peak open circuit voltage for line to ground coupling. b) 2 kV peak open circuit voltage for line-to-line coupling.	IEC 61000-4-5 (2014) Performance Criteria-C, Clause 9
8.	Immunity to conducted disturbance induced by Radio frequency fields: Under the test level 2 {3 V r.m.s.} in the frequency range 150 kHz-80 MHz for AC / DC lines and Signal /Control/telecom lines.	IEC 61000-4-6 (2013) Performance Criteria-A, Clause 9
9.	Immunity to voltage dips & short interruptions (applicable to only ac mains power input ports, if any):	IEC 61000-4-11 (2004): a) Performance Criteria B for Reduction of Supply 30% for

	Limits: - a) a voltage dip corresponding to a reduction of the supply voltage of 30% for 500ms (i.e., 70% supply voltage for 500ms) b) a voltage dip corresponding to a reduction of the supply voltage of 60% for 200ms; (i.e.,40% supply voltage for 200ms) c) a voltage interruption corresponding to a reduction of supply voltage of > 95% for 5s. d) a voltage interruption corresponding to a reduction of supply voltage of >95% for 10ms.	500ms or Dip to reduction of 60% for 100ms b) Performance Criteria C for Reduction of 60% for 200ms c) Performance criteria C for Voltage Interruption>95% for 5 s (Note: In case of Battery back-up performance criteria A is applicable). d) Performance Criteria B for Voltage Interruption >95% duration :10ms (Note: In case of Battery back-up Performance Criteria A is applicable for above conditions.)
10	Immunity to voltage dips & short interruptions (applicable to only DC power input ports, if any): a) Voltage Interruption with 0% of supply for 10ms. b) Voltage Interruption with 0% of supply for 30ms, 100ms, 300ms and 1000ms. c) Voltage dip corresponding to 40% & 70% of supply for 10ms, 30 ms. d) Voltage dip corresponding to 40% & 70% of supply for 100ms, 300 ms and 1000 ms.	IEC 61000-4-29(2000) a) Applicable Performance Criteria shall be B. b) Applicable Performance Criteria shall be C. c) Applicable Performance Criteria shall be B. d) Applicable Performance Criteria shall be C. Applicable Performance Criteria shall be B.

	e) Voltage variations corresponding to 80% and 120%of supply for 100 ms to 10s as per Table 1c of IEC 61000-4-29.	

CHAPTER 8

8. Information for the procurer of product

8.1. The procurer can specify the type and quantity of the WLAN interworking gateway as per their requirement based on the deployment scenario.

8.2. Interfaces and features which are optional needs to be examined by the procurer and suitably specified in the tender conditions as per their requirement based on the deployment scenario specific to the procurer.

ABBREVIATIONS

3GPP	3rd Generation Partnership Project
AAA	Authentication, Authorization and Accounting
AMF	Access and Mobility Management Function
APN	Access Point Name
CSCF	Call Session Control Function
DN	Data Network
eDNS	Enhanced Domain Name System
ePDG	Evolved Packet Data Gateway
EPC	Evolved Packet Core
ER	EAP Re-authentication
ESP	Encapsulating Security Payload
GTP	GPRS Tunnelling Protocol
HSS	Home Subscriber Server
ICSR	Inter Chassis Session Recovery
IE	Information Element
IEEE	Institute of Electrical and Electronics Engineers
IMS	IP Multimedia Subsystem
IP	Internet Protocol
IPSec	Internet Protocol Security
IKEv2	Internet Key Exchange Version 2
LI	Lawful Interception
LTE	Long Term Evolution
MAC	Media Access Control
MCM	Multiple Connectivity Mode
MME	Mobility Management Entity
MOBIKE	Mobility and Multihoming Protocol
NAS	Non-Access Stratum
NAT	Network Address Translation
NGCN	Next Generation Core Network
N3IWF	Non-3GPP InterWorking Function

NWu	Non-3GPP Wireless Untrusted Access Interface
NWt	Non-3GPP Wireless Trusted Access Interface
OCSP	Online Certificate Status Protocol
PAA	PDN Address Allocation
P-CSCF	Proxy Call Session Control Function
PCRF	Policy and Charging Rules Function
PDN	Packet Data Network
PDU	Protocol Data Unit
PGW	Packet Data Network Gateway
PMIPv6	Proxy Mobile IPv6
QoS	Quality of Service
RFC	Request for Comments
SA	Security Association
SCTP	Stream Control Transmission Protocol
SGW	Serving Gateway
SMF	Session Management Function
SWm	Reference Point between ePDG and AAA server
SWu	Reference Point between UE and ePDG
STa	Reference Point between TWAG and AAA server
TCP	Transmission Control Protocol
TNAN	Trusted Non-3GPP Access Network
TNAP	Trusted Non-3GPP Access Point
TNGF	Trusted Non-3GPP Gateway Function
TWAG	Trusted WLAN Access Gateway
UE	User Equipment
UPF	User Plane Function
VoIP	Voice over Internet Protocol
VoLTE	Voice over LTE
WLAN	Wireless Local Area Network
WLCP	WLAN Control Plane Protocol