सत्यमेव जयते

वर्गीय आवश्यकताओं के लिए मानक
टीईसी xxxxx:२०२६
STANDARD FOR GENERIC REQUIREMENTS
TEC 36xxx:2026

वाई-फाई ऑफलोडिंग तकनीकी

Wi-Fi Offloading Technology

ISO 9001:2015

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

Release __: Month, 2026

FOREWORD

Telecommunication Engineering Centre (TEC) is the technical arm of Department of Telecommunications (DOT), Government of India. Its activities include:

- Framing of TEC Standards for Generic Requirements for a Product/Equipment, Standards for Interface Requirements for a Product/Equipment, Standards for Service Requirements & Standard document of TEC for Telecom Products and Services
- Formulation of Essential Requirements (ERs) under Mandatory Testing and Certification of Telecom Equipment (MTCTE)
- Field evaluation of Telecom Products and Systems
- Designation of Conformity Assessment Bodies (CABs)/Testing facilities
- Testing & Certification of Telecom products
- Adoption of Standards
- Support to DoT on technical/technology issues

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 Standard for Generic Requirements contains the generic requirements for Wi-Fi Offloading (Mobile Data Offload – MDO) technology in Indian telecom networks. The document specifies architectural models for trusted and untrusted access along with requirements for authentication, security, QoS, and policy control. It emphasizes interoperability with PM-WANI, global OpenRoaming, and compliance with 3GPP, IEEE, and TEC standards, enabling secure and scalable deployments.

CONTENTS

HISTORY SHEET

S.No.	*Standard/ document No.*	*Title*	*Remarks*
1.	TEC 36xxx:2026	Wi-Fi Offloading Technology	First issue
2.			

REFERENCES

S.No.	*Document No.*	*Title/Document Name*
1)	3GPP TS 23.261	IP flow mobility and seamless Wireless Local Area Network (WLAN) offload
2)	3GPP TS 23.402	Architecture enhancements for non-3GPP accesses
3)	3GPP TS 23.502	5G; Procedures for the 5G System (5GS)
4)	3GPP TS 24.502	Access to the 3GPP 5G Core Network (5GCN) via Non-3GPP Access Networks (N3AN); Stage 3
5)	3GPP TS 24.302	Access to the 3GPP Evolved Packet Core (EPC) via non-3GPP access networks; Stage 3
6)	3GPP TS 33.234	3G Security; Wireless Local Area Network (WLAN) Interworking Security
7)	3GPP TS 33.402	3GPP System Architecture Evolution (SAE); Security aspects of non-3GPP accesses
8)	3GPP TS 33.501	Security Architecture and Procedures for 5G System
9)	3GPP TS 38.413	NG-RAN; NG Application Protocol (NGAP)
10)	RFC 5996	Internet Key Exchange Protocol Version 2 (IKEv2)
11)	RFC 3588	Diameter Base Protocol
12)	ITU-T Y.2250	Mobility management in NGN

CHAPTER-1

1.0 Introduction

Wi-Fi offloading allows seamless mobility of data and IP flow from cellular networks (4G/5G) to Wi-Fi Networks/WLAN, helping to reduce congestion, improve spectrum efficiency, and enhance user experience.

This document contains the Generic Requirements (GR) for Wi-Fi Offloading (Mobile Data Offload - MDO) technology in telecommunication networks. It provides functional, architectural, interoperability, security, and performance requirements for enabling seamless mobile data traffic offloading from cellular networks to Wi-Fi networks.

2.0 Description

Wi-Fi offload essentially enabling the use of Wi-Fi to relieve congestion on the cellular networks or use Wi-Fi as one of the options for in-building solution. 3GPP standard "3GPP TS 23.261" defines specifications for "IP flow mobility and seamless Wireless Local Area Network (WLAN) offload" and outlines how mobile devices can seamlessly transition between cellular networks and Wi-Fi access points for data offloading purposes.

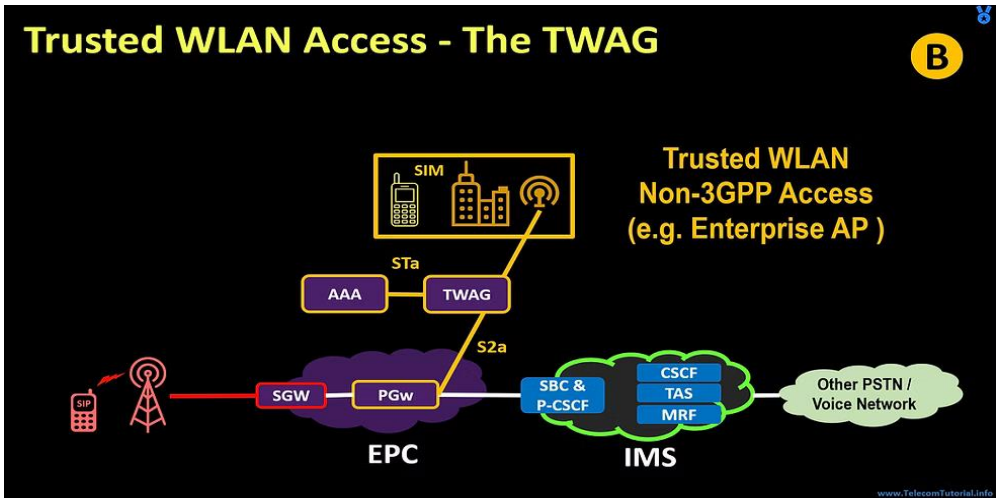
2.1 Architecture

i. The system shall support interworking of Wi-Fi access with both EPC (4G LTE) and 5GC (5G) core networks.

ii. Support for trusted and untrusted access models using TWAG(for trusted)/ePDG(for untrusted) in LTE and TNGF(for trusted)/N3IWF(for untrusted) in 5G. A comparison is described in Annexure-A

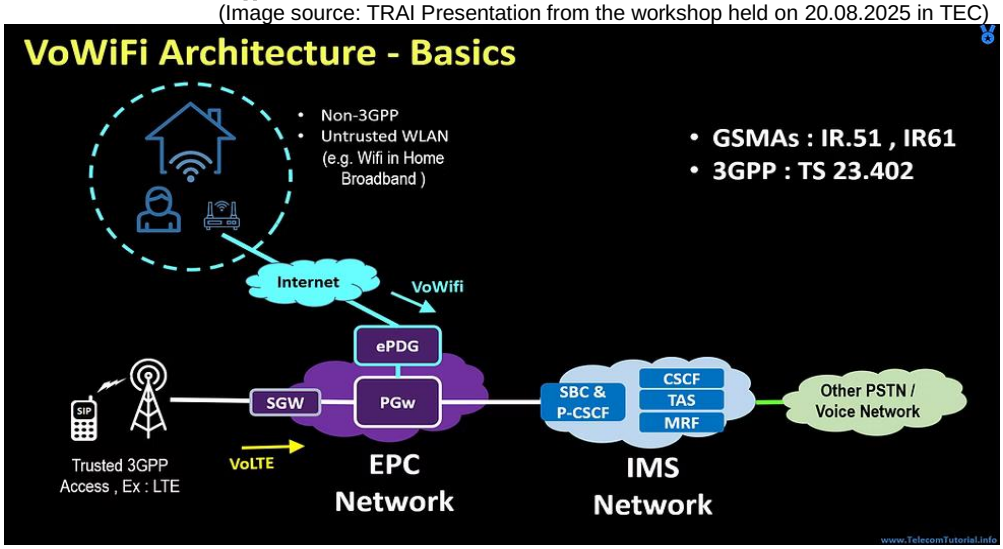
iii. It shall enable IMS-based services (VoWiFi, SMS over IMS) and ensure seamless mobility between LTE (VoLTE) and Wi-Fi (VoWiFi).

iv. Architecture shall allow deployment in edge as well as cloud-based environments for scalability.



(i) Architecture of Trusted Network

(Image source: TRAI Presentation from the workshop held on 20.08.2025 in TEC)



(ii) Architecture of Un-Trusted Network

(Image source: TRAI Presentation from the workshop held on 20.08.2025 in TEC)

3.0 Functional / Operational Requirements

3.1 Authentication Requirements

i. Wi-Fi offloading solutions shall comply with 3GPP standards (TS 23.402, TS 23.501/502) and IEEE Wi-Fi standards (802.11 standards).
ii. The system shall support EAP-SIM, EAP-AKA/AKA′, and 5G-AKA for SIM-based authentication.
iii. For untrusted Wi-Fi, IPSec/IKEv2 tunnels shall be established between UE and ePDG/N3IWF.
iv. For trusted Wi-Fi, authentication shall be directly with AAA/HSS using 802.1X/EAP methods.
v. Passpoint/Hotspot 2.0 (IEEE 802.11u) shall be supported for seamless network discovery, selection, and roaming.
vi. All authentication and data transport mechanisms shall comply with national security directives and lawful interception.

3.2 Policy Control Requirements

i. Mapping of Wi-Fi 802.11e/WMM QoS classes with 3GPP QCI/5QI shall be supported.
ii. PCRF (in LTE) and PCF (in 5G) shall enforce operator-defined policies during Wi-Fi offloading.
iii. Traffic prioritization shall ensure real-time services (voice, video) are not degraded during offload.
iv. Mechanisms shall exist for dynamic bandwidth allocation, policy enforcement, and charging across both access networks.

3.3 Offload Modes (Applicable in case of Trusted Networks)

Operators shall have the ability to configure following offload modes dynamically:

i. Full Offload: All device traffic routed via Wi-Fi.
ii. Selective Offload: Specific application flows (e.g., video, social media) routed via Wi-Fi while others remain on cellular.
iii. Hybrid Connectivity: Simultaneous use of Wi-Fi and cellular networks using MPTCP or ATSSS (Access Traffic Steering, Switching, Splitting).

3.4 Operating Frequency Range For Wi-Fi Networks

i. The operating frequency range for Wi-Fi networks shall be in the unlicensed bands viz. 2.4 GHz, 5 GHz, 6 GHz (any one or combination of these bands) and as applicable as per latest National Frequency Allocation Plan (NFAP) and published WPC GSRs being revised from time to time.

ii. Offload implementations shall comply with DoT spectrum guidelines and TEC equipment certifications.

iii. 6 GHz Wi-Fi (Wi-Fi 6E/7) is recommended for high-density indoor deployments to improve quality of service. (*Note- Use of 6 GHz (Wi-Fi 6E/7) spectrum shall be subject to DoT delicensing notification. Once delicensed, power limits and channelization shall comply with notified conditions).*

4.0 Interconnectivity and Interoperability Requirements

4.1 The system shall support Voice over Wi-Fi (VoWiFi) including emergency calling capabilities, SMS over IMS, and multimedia telephony services.

4.2 The system shall support Seamless handover between VoLTE and VoWiFi shall without call drops.

4.3 The system shall support IoT and M2M use cases where non-critical traffic can be selectively offloaded to Wi-Fi.

4.4 The system shall Support for enterprise deployments using trusted Wi-Fi domains (TNGF/TWAG).

4.5 The system shall Support for large-scale public deployments such as PM-WANI hotspots and smart cities and support integration with PM-WANI framework and enable open roaming across different Public Data Offices (PDOs/PDOAs).

4.6 The system shall Solutions shall provide policy-based routing to ensure lawful interception and billing continuity.

4.7 The system shall enable inter-operator roaming and interoperability for both domestic and international Wi-Fi offload scenarios. Interoperability shall be ensured between different vendors' Wi-Fi APs, AAA servers, ePDG/N3IWF gateways, and mobile cores.

4.8 Interworking with international OpenRoaming standards (WBA/Hotspot 2.0) shall be supported to enable global interoperability.

4.9 Solutions shall allow seamless interoperability between different MNO networks during Wi-Fi offload and roaming.

4.10 Compliance with TRAI and DoT interoperability mandates shall be ensured.

5.0 EMI/EMC Requirements

The equipment used for deploying Wifi offloading technology shall conform to the EMC requirements as per the relevant standards and limits indicated therein TEC Standard 11016:2016(old no.- TEC/SD/DD/EMC-221/05/OCT-16)"Electromagnetic Compatibility Standard for telecommunication Equipment"

6.0 Safety Requirements

The equipment shall conform to relevant safety requirements as per IS 10437 : 2019/ IEC 60215 : 2016 as prescribed under TEC document 'SAFETY REQUIREMENTS OF TELECOMMUNICATIONS EQUIPMENT TEC 10009: 2024'.

7.0 Documentation

Technical literature in English with complete layout and detailed block schematic shall be provided in hard copy. All aspects of installation, operation, maintenance, trouble shooting and replacement shall be covered in this manual wherever applicable. Additionally, a soft copy /QR code on the system in respect of technical literature shall also be provided both in Hindi and English. Label or suitable arrangement for address and telephone numbers of Maintenance center shall also be provided.

CHAPTER-2

8.0 **Information for the procurer of product**

The procurer shall specify the requirements for

8.1 **Standards Compliance**

Specify applicable standards for Wi-Fi offloading such as IEEE 802.11 (relevant versions), ANDSF (Access Network Discovery and Selection Function), 3GPP Release specifications (e.g., Release 13/14 for LTE-WLAN aggregation), and relevant IETF standards.

8.2 **Application Environment:** Indoor, Outdoor, or Both.

8.3 **Frequency Bands Supported:** Specify operational frequency bands (2.4 GHz, 5 GHz, 6 GHz) as per applicable clauses or requirements.

8.4 **MIMO and Throughput Requirements:** Specify MIMO configurations (e.g., 2x2, 4x4) and minimum throughput targets.

8.5 **Integration with Cellular Core Networks:** Specify compatibility with cellular core network elements, e.g., PGW (Packet Gateway), MME (Mobility Management Entity), or EPC (Evolved Packet Core).

8.6 **Device Type & Functionality:** Specify if the product acts as:

- Wi-Fi Offload Gateway
- Access Controller with offload capabilities
- Client device with offload features

8.7 **Roaming and Mobility Support:** Requirements for seamless handover between Wi-Fi and cellular networks, and support for hotspots roaming

8.8 **Compliance with National or International Certifications:** Wi-Fi CERTIFIED™, WANI compliance, or other regulatory requirements

8.10 **Environmental and Deployment Requirements:** IP rating (for outdoor), temperature range, and ruggedness

8.11 **Validation and Interoperability Testing:** Specify any validation requirements for interoperability with specific cellular operators or network equipment.

Abbreviations

i. MDO – Mobile Data Offload
ii. VoWiFi – Voice over Wi-Fi
iii. TWAG – Trusted WLAN Access Gateway
iv. ePDG – Evolved Packet Data Gateway
v. N3IWF – Non-3GPP Interworking Function
vi. TNGF – Trusted Non-3GPP Gateway Function
vii. ATSSS – Access Traffic Steering, Switching, and Splitting
viii. PM-WANI – Public Wi-Fi Access Network Interface
ix. QoS/QCI/5QI – Quality of Service parameters
x. AKA – Authentication and Key Agreement
xi. EAP – Extensible Authentication Protocol
xii. MPTCP – Multipath Transmission Control Protocol
xiii. ANDSF – Access Network Discovery and Selection Function
xiv. OFDMA – Orthogonal Frequency Division Multiple Access
xv. WLAN- Wireless Local Area Network

Annexure-A

Table (1)-Comparison of Trusted vs. Untrusted Wi-Fi Offload(4G)

Feature/Aspect	ePDG (Untrusted)	TWAG (Trusted)
Network Type	Untrusted Non-3GPP (public Wi-Fi)	Trusted Non-3GPP (operator Wi-Fi)
Security	IPSec tunnels	No IPSec needed
Authentication	EAP-based via AAA servers	EAP-based via RADIUS/AAA
Core Network Interface	Connects to PGW	Connects to PGW
Traffic Handling	Securely tunnels user data	Aggregates/forwards user data
Mobility Support	Seamless handover across 3GPP/untrusted Wi-Fi	Seamless handover across LTE/trusted Wi-Fi
Policy Enforcement	Limited	Supports QoS and policy enforcement

Table(2)- Features of N3IWF and TNGF(5G)

Feature/Aspect	N3IWF (Untrusted Wi-Fi)	TNGF (Trusted Wi-Fi)
Network Type	Untrusted non-3GPP	Trusted non-3GPP
UE Tunnel	Yes, IPSec/IKEv2	No, optional
Authentication	UE authenticates via tunnel	UE authenticates via AP directly
Security Enforcement	N3IWF handles UE security	Trusted AP, optional tunnel
QoS Enforcement	Limited, best-effort	Full QoS support
UE Complexity	Higher (manages tunnel)	Lower (transparent)
Mobility	Supports handover	Supports seamless handover