Recommendations for Minimum Wi-Fi ® Capabilities of Terminals

Version 6.0

04 December 2018

This is a Non-binding Permanent Reference Document of the GSMA

Security Classification: Non-confidential

Copyright Notice

Disclaimer

Antitrust Notice

Table of Contents

1 Introduction

1.1 Purpose

Wi-Fi has been steadily increasing as a standard feature for radio access in a device.

However, a device has varying degrees of Wireless Local Area Network (WLAN) support which poses a number of risks in the market such as different implementations of WLAN confusing end-users, which results in a reluctance to use it. The different WLAN implementations and requirements also cause interoperability issues and create fragmentation that impacts its use in the market.

The GSMA TSG (Terminal Steering Group) has established a dedicated work item for operators and vendors to share existing WLAN experiences from operators, to assess relevant industry activities, to gather input from other organisations, and to create a PRD (Permanent Reference Document). The outcome shall help drive and standardise WLAN implementation of MNOs and OEMs and facilitate support of WLAN functionality and usability for users of WLAN services on operator networks.

Note that the Annexes containing the Use Cases from which the original requirements for this PRD were derived have been deprecated in V3.0 of this document, as they became obsolete as the requirements were modified and expanded with the changing industry.

1.2 Scope and Objective

The aim of this document is to consolidate minimum device requirements (or references where these have been published already by other groups) for a WLAN enabled device. It is the intent of this PRD to facilitate alignment of operator WLAN requirements and to enhance the WLAN functionality and usability for users of WLAN services on operator networks.

This PRD does not exclude the possibility for support of additional WLAN capabilities not mentioned in this document.

1.3 Definition of Terms

Term	Description
3GPP	Third Generation Partnership Project
ANDSF	Access Network Discovery and Selection Function
ANQP	Access Network Query Protocol
AP	Access Point
API	Application Programming Interface
APN	Access Point Name
BSS	Basic Service Set
EAP	Extensible Authentication Protocol
EPC	3GPP Enhanced Packet Core
ePDG	Evolved Packet Data Gateway
EPS	Evolved Packet System
ESS	Extended Service Set

Term	Description
GSM	Global System for Mobile Communications
GTP	GPRS Tunnelling Protocol
Hotspot 2.0	Wi-Fi Alliance programme that certifies a Hotspot 2.0 device
HPLMN	Home Public Land Mobile Network
IE	Information Element
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
IMS	IP Multimedia Subsystem
LAN	Local Area Network
LTE	Long Term Evolution
MAC	Media Access Control
MAPCON	Multi Access PDN Connectivity
MME	Mobility Management Entity
MNO	Mobile Network (i.e. 3GPP PLMN) Operator
MNS	Mobile Network (i.e. 3GPP PLMN) Service
NAI	Network Access Identifier
NFC	Near Field Communications
OMA	Open Mobile Alliance
OMA DM	OMA Device Management
OTA	Over the air
Passpoint™	Wi-Fi CERTIFIED Passpoint™
P-CSCF	Proxy Call Session Control Function
PDN	Packet Data Network
PDN GW	Packet Data Network GateWay
PIN	Personal Identification Number
PLMN	Public Land Mobile Network
PMF	Protected Management Frame
OEM	Original Equipment Manufacturer
QoS	Quality of Service
PDN	Packet Data Network
PRD	Permanent Reference Document
RAT	Radio Access Technology
RSSI	Receive Signal Strength Indication
S2b	The name of a 3GPP architecture reference point
SaMOG	S2a Mobility Based on GTP (GPRS Tunnelling Protocol)
SIM	Subscriber Identity Module
SIP	Session Initiation Protocol
SMS	Short Message Service

Term	Description
SSID	Service Set Identifier
SWu	The name of a 3GPP architecture reference point
SWw	The name of a 3GPP architecture reference point
TKIP	Temporal Key Integrity Protocol
TWAG	Trusted Wireless Access Gateway
UI	User Interface
UICC	Universal Integrated Circuit card
UMTS	Universal Mobile Telecommunications System
USIM	Universal SIM
VPLMN	Visited Public Land Mobile Network
WEP	Wired Equivalent Privacy
WFA	Wi-Fi Alliance
Wi-Fi	WLAN products which are usually Wi-Fi Alliance certified
WLAN	Wireless Local Area Network
WMM	Wireless Multi-Media
WPA2	Wi-Fi Protected Access Version 2
XCAP	XML Configuration Access Protocol (XCAP)
XML	Extensible Markup Language

1.4 Reference Documents

Document Number	Title
Passpoint	Wi-Fi Alliance Hotspot 2.0 (Release 2) Technical Specification Package Source: https://www.wi-fi.org/downloads-registered-guest/Hotspot_2-0_%2528R2%2529_Technical_Specification_Package_v1-4_0.zip/29728
Wi-Fi Alliance Certification Programs	Wi-Fi Alliance Certification Programs See: http://www.wi-fi.org/certification/programs
Wi-Fi Direct	Wi-Fi Alliance, Peer to Peer (P2P) Technical Specification v1.7 Source: https://www.wi-fi.org/downloads-registered-guest/Wi-Fi%2BP2P%2BTechnical%2BSpecification%2Bv1.7.pdf/29559
OpenCMAPI	Open CM API Requirements Document Release 1.0 Source: http://www.openmobilealliance.org/Technical/release_program/docs/CopyrightClick.aspx?pck=OpenCMAPI&file=V1_0-20110712-C/OMA-RD-OpenCMAPI-V1_0-20110712-C.pdf
3GPP TS 23.060	3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; General Packet Radio Service (GPRS); Service description; Stage 2

Document Number	Title
	Latest version of: http://www.3gpp.org/ftp/specs/archive/23_series/23.060/
3GPP TS 23.401	3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; General Packet Radio Service (GPRS) enhancements for Evolved Universal Terrestrial Radio Access Network (E-UTRAN) access (Release 12) Latest version of: http://www.3gpp.org/ftp/specs/archive/23_series/23.401/
3GPP TS 23.402	3rd Generation Partnership Project; Technical Specification Group Core Network; Architecture enhancements for non-3GPP accesses Latest version of: http://www.3gpp.org/ftp/specs/archive/23_series/23.402/
3GPP TS 24.234	3rd Generation Partnership Project; Technical Specification Group Core Network; 3GPP System to WLAN Interworking; UE to Network Protocols Latest version of: http://www.3gpp.org/ftp/specs/archive/24_series/24.234/
3GPP TS 24.302	3rd Generation Partnership Project; Technical Specification Group Core Network and Terminals; Access to the 3GPP Evolved Packet Core (EPC) via non-3GPP access networks; Stage 3 Latest version of: http://www.3gpp.org/ftp/specs/archive/24_series/24.302/
3GPP TS 24.312	3rd Generation Partnership Project; Technical Specification Group Core Network and Terminals, Access Network Discovery and Selection Function (ANDSF) Management Object (MO) Latest version of: http://www.3gpp.org/ftp/specs/archive/24_series/24.312/
3GPP TS 31.102	3rd Generation Partnership Project; Technical Specification Group Core Network and Terminals; Characteristics of the Universal Subscriber Identity Module (USIM) application. Latest version of: http://www.3gpp.org/ftp/specs/archive/31_series/31.102/
3GPP TS 31.115	3rd Generation Partnership Project; Technical Specification Group Core Network and Terminals; Secured packet structure for (Universal) Subscriber Identity Module (U)SIM Toolkit applications. Latest version of: http://www.3gpp.org/ftp/specs/archive/31_series/31.115/
3GPP TS 31.116	3rd Generation Partnership Project; Technical Specification Group Core Network and Terminals; Remote APDU Structure for (U)SIM Toolkit applications. Latest version of: http://www.3gpp.org/ftp/specs/archive/31_series/31.116/
3GPP TS 33.234	3rd Generation Partnership Project; Technical Specification Group Services and System Aspects;3G Security; Wireless Local Area Network (WLAN) interworking security Latest version of: http://www.3gpp.org/ftp/specs/archive/33_series/33.234/
3GPP TS 33.402	3rd Generation Partnership Project; Technical Specification Group Services and System Aspects;3GPP System Architecture Evolution (SAE); Security aspects of non-3GPP accesses Latest version of: http://www.3gpp.org/ftp/specs/archive/33_series/33.402/
3GPP TS 36.304	3rd Generation Partnership Project; Technical Specification Group Radio Access Network; Evolved Universal Terrestrial Radio Access (E-UTRA); User Equipment (device) procedures in idle mode Latest version of: http://www.3gpp.org/ftp/specs/archive/36_series/36.304/
3GPP TS 25.304	3rd Generation Partnership Project; Technical Specification Group Radio Access

Document Number	Title
	Network; User Equipment (device) procedures in idle mode and procedures for cell reselection in connected mode Latest version of: http://www.3gpp.org/ftp/specs/archive/36_series/25.304/
3GPP TS 25.331	3rd Generation Partnership Project; Technical Specification Group Radio Access Network; Radio Resource Control (RRC); Protocol specification Latest version of: http://www.3gpp.org/ftp/specs/archive/36_series/25.331/
3GPP TS 36.331	3rd Generation Partnership Project; Technical Specification Group Radio Access Network; Radio Resource Control (RRC); Protocol specification Latest version of: http://www.3gpp.org/ftp/specs/archive/36_series/36.331/
IEEE 802.11-2016	IEEE 802.11-2016, Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications. Source: https://standards.ieee.org/findstds/standard/802.11-2016.html
IEEE 802.11 HT	Enhancements for High Throughput (HT) were first defined in Amendment 802.11n™, and have since been incorporated into 802.11-2016 [IEEE 802.11-2016] in clause 20.
IEEE 802.11 VHT	Enhancements for Very High Throughput (VHT) for Operation in Bands below 6 GHz, is existing Amendment 802.11ac™ to 802.11-2016 [IEEE 802.11-2016]
IEEE 802.11 Legacy PHY	IEEE 802.11 legacy Physical Layer (PHY) Amendments 802.11a™, 802.11b™, and 802,11g™ were first defined as amendments to 802.11-1999, and have since been incorporated into 802.11-2007 and beyond.
IEEE 802.11 Fast BSS Transition	Fast Basic Service Set (BSS) Transition was first defined in Amendment 802.11r™, and has since been incorporated into 802.11-2016 [IEEE 802.11-2016] in clause 12.
IEEE 802.11 RRM	Radio Resource Measurement (RRM) for Wireless LANs was first defined in Amendment 802.11k™, and has since been incorporated into 802.11-2016 [IEEE 802.11-2016] in clause 10.
RFC 1981	Path MTU Discovery for IP version Source: http://www.ietf.org/rfc/rfc1981.txt
RFC 2460	Internet Protocol, Version 6 (IPv6) Source: http://www.ietf.org/rfc/rfc2460.txt
RFC 3736	Stateless Dynamic Host Configuration Protocol (DHCP) Service for IPv6 Source: http://www.ietf.org/rfc/rfc3736.txt
RFC 3748	Extensible Authentication Protocol (EAP) Source: http://www.ietf.org/rfc/rfc3748.txt
RFC 4186	Extensible Authentication Protocol Method for Global System for Mobile Communications (GSM) Subscriber Identity Modules (EAP-SIM) Source: http://www.ietf.org/rfc/rfc4188.txt
RFC 4187	Extensible Authentication Protocol Method for 3rd Generation Authentication and Key Agreement (EAP-AKA) Source: http://www.ietf.org/rfc/rfc4187.txt
RFC 4436	Detecting Network Attachment in IPv4 (DNAv4) Source: http://www.ietf.org/rfc/rfc4436.txt
RFC 4443	Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6)

Document Number	Title
	Source: http://www.ietf.org/rfc/rfc4443.txt
RFC 4861	Neighbour Discovery for IP version 6 (IPv6) Source: http://www.ietf.org/rfc/rfc4861.txt
RFC 4862	IPv6 Stateless Address Autoconfiguration Source: http://www.ietf.org/rfc/rfc4862.txt
RFC 4941	Privacy Extensions for Stateless Address Autoconfiguration in IPv6 Source: http://www.ietf.org/rfc/rfc4941.txt
RFC 5175	IPv6 Router Advertisement Flags Option Source: http://www.ietf.org/rfc/rfc5175.txt
RFC 5247	Extensible Authentication Protocol (EAP) Key Management Framework Source: http://www.ietf.org/rfc/rfc5247.txt
RFC 5448	Improved Extensible Authentication Protocol Method for 3rd Generation Authentication and Key Agreement (EAP-AKA') Source: http://www.ietf.org/rfc/rfc5448.txt
RFC 6106	IPv6 Router Advertisement Options for DNS Configuration Source: http://www.ietf.org/rfc/rfc6106.txt
OMA Device Management Bootstrap	Device Management Bootstrap Source: http://technical.openmobilealliance.org/Technical/release_program/docs/copyrightclick.aspx?pck=DM&file=V1_2_1-20080617-A/OMA-TS-DM_Bootstrap-V1_2_1-20080617-A.pdf
Wireless Broadband Alliance Wi-Fi Calling – Opportunities and Challenges towards 5G	WBA Wi-Fi Calling – Opportunities and Challenges towards 5G

2

Alignment with Wi-Fi Alliance Certification Programmes

It is essential for a device with WLAN capabilities to support Wi-Fi Alliance certifications to ensure that devices and network elements from multiple vendors are interoperable.

2.1 Wi-Fi Alliance Certification Programmes

A device is expected to support the certification requirements listed in this subsection in order to achieve the following objectives:

- Interoperability with public WLANs (hotspots) including scalability of authentication systems,
- Interoperability with consumer/residential networks,
- Interoperability with enterprise networks.

IEEE 802.11n™ [IEEE 802.11 HT], which operates in the 2.4 and 5 GHz bands, provides high performance over legacy specifications 802.11a™, 11b™ and 11g™ [IEEE 802.11 Legacy PHY]. IEEE 802.11ac™ [IEEE 802.11 VHT], the very latest version of Wi-Fi in 5 GHz, pushes Wi-Fi performance past the gigabit-per-second data rate for network capacity. Since the radio channel is shared by an AP and a device, increasing performance results in improved channel capacity for a device.

A device shall be IEEE 802.11n capable for 2.4 GHz operation and IEEE 802.11ac capable for 5 GHz operation.

For a device which is IEEE 802.11n capable, the Wi-Fi Alliance baseline certification requires the device to be Wi-Fi CERTIFIED n™. For a device which is IEEE 802.11ac capable, the Wi-Fi Alliance baseline certification requires the device to be Wi-Fi CERTIFIED ac™. In addition, both certifications include WPA2™ (Wi-Fi Protected Access 2) and Wi-Fi Multimedia (WMM) testing.

WPA2 testing and certification provides WLAN access network security - offering government-grade security mechanisms for personal, enterprise and hotspot deployments. The WMM certification provides support for multimedia content over WLAN access networks enabling WLAN access networks to prioritize traffic generated by different applications using Quality of Service (QoS) mechanisms. WMM® certifies products which implement technology defined in the WMM® Technical Specification.

For a device which is not IEEE 802.11n or 802.11ac capable, the Wi-Fi Alliance baseline consists of separate certifications: the IEEE 802.11 certification for radio types of IEEE 802.11a, IEEE 802.11b, IEEE 802.11g with WPA2 and the WMM® certification.

A device shall be Wi-Fi CERTIFIED WPA2 with Protected Management Frames (PMF), which provides a WPA2-level of protection for unicast and multicast management action frames. Protection of management frames prevents attacks in which a wireless attacker forges frames (mimicking an AP) and transmits them to a victim device. Without PMF, this attack could cause the victim device, for example, to disassociate from a WLAN access network, tear down a QoS flow, etc.

A device shall be Wi-Fi CERTIFIED Passpoint™ [Passpoint]. Passpoint certifies that products implement the technology defined in the Wi-Fi Alliance Hotspot 2.0 Technical Specification. This technology enables advertisement of roaming relationships between the Passpoint operators, similar to those mechanisms used today for 3GPP access, allowing the device to automatically discover and connect to WLANs. It also automatically configures WPA2-Enterprise level security (using EAP-SIM, EAP-AKA or EAP-AKA') without user intervention.

Passpoint certification requires Wi-Fi Alliance baseline certification as a pre-requisite.

A device should support Fast BSS Transition [IEEE 802.11 Fast BSS Transition], in order to significantly reduce the load on a Mobile Network Service Providers (MNSP)'s HLR/HSS. Note that a device using WPA2-Enterprise with EAP-SIM, EAP-AKA or EAP-AKA' authenticates with its home AAA server every time the device transitions from one AP to another within the same WLAN access network. A device using Fast BSS Transition authenticates to its home AAA server only on the first authentication with the WLAN access

network; all subsequent authentications are handled locally. Example deployments where the use of Fast BSS Transition can dramatically reduce the load on the MNSP's HLR/HSS include high density environments (e.g., sporting venue, train station) or Community WLAN access networks (e.g., a user walking down a street would connect to AP after AP in sequence).

A device should also support IEEE 802.11 Radio Resource Measurement (RRM) [IEEE 802.11 RRM]. RRM features provide network operators greater capability to manage WLAN to WLAN interference, improve roaming, etc.

The Wi-Fi Alliance has included certification of Fast BSS Transition and RRM capabilities within the Voice-Enterprise certification. Although portions of this certification, which include performance testing using simulated VoIP streams are not required by this PRD, Voice-Enterprise is currently the only certification option for Fast BSS Transition and RRM.

A device should be Wi-Fi CERTIFIED WMM-Power Save™. This certification program provides power savings for delivering multimedia content over WLAN access networks – it helps conserve battery life while using voice and multimedia applications by managing the time the device spends in sleep mode. Testing has shown 37 - 73% power savings versus legacy power save mechanisms.

A device shall be Wi-Fi CERTIFIED Wi-Fi Protected Setup™. This certification program facilitates easy set-up of security features using a Personal Identification Number (PIN) or other defined methods within the device. Wi-Fi Protected Setup certifies products which implement technology defined in the Wi-Fi Simple Configuration Technical Specification.

Req ID	Requirement
TSG22_R2_WFA_01	A device SHALL be IEEE 802.11n for 2.4 GHz and 5GHz operation and IEEE 802.11ac capable for 5 GHz operation.
TSG22_R2_WFA_02	A device SHALL be Wi-Fi CERTIFIED WPA2 with Protected Management Frames.
TSG22_R2_WFA_03	A device SHALL be Wi-Fi CERTIFIED Passpoint.
TSG22_R2_WFA_04	A device SHOULD be Wi-Fi CERTIFIED Voice-Enterprise.
TSG22_R2_WFA_05	A device SHOULD be Wi-Fi CERTIFIED WMM-Power Save.
TSG22_R2_WFA_06	A device SHOULD be Wi-Fi CERTIFIED Wi-Fi Protected Setup.

The Wi-Fi Alliance certification programs are located at http://www.wi-fi.org/certification/programs

2.2 Wi-Fi CERTIFIED Wi-Fi Direct ®

Wi-Fi CERTIFIED Wi-Fi Direct [Wi-Fi Direct] is a certification mark for a WLAN client device that connects directly without use of an AP, to enable applications such as printing, content sharing, and display. Wi-Fi Direct certifies products which implement technology defined in the Wi-Fi Alliance Peer-to-Peer Technical Specification [Wi-Fi Direct].

Mobile phones, cameras, printers, PCs, and gaming devices can connect to each other directly to transfer content and share applications quickly and easily. A device can make a one-to-one connection, or a group of several devices can connect simultaneously. Connecting a Wi-Fi Direct device is easy and simple, in many cases only requiring the push of a button.

Wi-Fi Direct certification requires a device to implement WPA2-Personal level security. Some Wi-Fi Direct devices maintain an infrastructure connection concurrently with a Wi-Fi Direct connection, and it is possible for the device to provide cross-connect capabilities which allows a Wi-Fi Direct peer to access a network through another associated peer. As infrastructure Wi-Fi deployments require the more stringent WPA2-Enterprise level security this could compromise the infrastructure network, allowing the device which is not authenticated with the network to have network access. To avoid this potential security breach, a Wi-Fi Direct capable device needs to provide the capability to disable infrastructure connections when connecting over Wi-Fi Direct.

Note: this section may be modified at a later date if clarifying technical information on Wi-Fi Direct™ is received from the Wi-Fi Alliance.

Req ID	Requirement
TSG22_R2_WFA_07	A device SHOULD support the Wi-Fi Direct certification program.
TSG22_R3_WFA_08	A device which supports Wi-Fi Direct SHOULD provide the user with the ability to prevent cross connect between a Wi-Fi Direct connection and an access network connection.

2.3 Dual-band Support Bands

The 2.4GHz band is widely deployed and in many areas can become congested due to both the number of APs in an area as well as the number of users trying to receive a service in that area.

The 5GHz band is now becoming more widely deployed by both operators and in home networks. Consequently, a device should support the use of the 5GHz band. It is advantageous for a device to support dual-band operations, working in either the 2.4 GHz band or the 5 GHz band. This allows a device to use all available APs (regardless of band), and allows dual-band APs to balance the load of the device, across bands.

Req ID	Requirement
TSG22_R2_USE_02	VOID
TSG22_R3_USE_03	A device SHOULD support dual-band operation in the 2.4 GHz and 5 GHz bands.

2.4 3GPP Release 12 specifications

Within this document the terms: pre-release 12, release 12 and post-release 12 devices refer to devices, which meet 3GPP specifications.

WLAN Policy Provisioning

3.1 Operator Policy Provisioning

3 Expanded service of operators through service agreements and partnerships can significantly increase the coverage and list of network identifiers (e.g. SSID) within a user's subscription. An update mechanism shall be in place to broker the inclusion of new parameters and data (e.g. SSIDs) within the user's subscription, together with the exclusion or removal of irrelevant ones. OMA DM can provide a means to configure a device, either through the 3GPP network or directly over the WLAN access network or some operators may pre-configure a device to select operator controlled APs. In order for the OMA DM client in the device to be able to access the OMA DM server, it is necessary to bootstrap the device with at least the address of the OMA DM server (e.g. URL of the OMA DM server) and the credentials (e.g. username and password) for the OMA DM client to authenticate to the OMA DM Server.

OMA DM Bootstrap specification v1.2 [OMA Device Management Bootstrap] provides three options for configuring the bootstrap information in the device:

1. At the factory, during the device personalization for instance;
2. Via an OMA Push message from the OMA DM server; or,
3. From the information stored in the UICC (in the EF Bootstrap file).

OMA DM provides a means to provision a device at the initialisation phase from the UICC (see [OMA Device Management Bootstrap]). When bootstrap information is stored in the UICC bootstrap file, according to OMA Device Management Bootstrap specification, a device is required to use the information from the EF Bootstrap file, as the device is a GSM device.

3.1.1 3GPP ANDSF Policy Provisioning

For ANDSF operation, the ANDSF policies are provided to the device as defined in TS 23.402 [3GPP TS 23.402], TS 24.302 [3GPP TS 24.302] and TS 24.312 [3GPP TS 24.312].

3.1.2 3GPP RAN assisted WLAN interworking

In RAN assisted WLAN interworking for E-UTRAN the RAN assistance information defined in TS 36.304 [3GPP TS 36.304] clause 5.6 and TS 24.312 [3GPP TS 24.312] clause 5.7.21B34 (OPI) are provided to the device by the E-UTRAN as specified in TS 36.331 clause 5.6.12. For UTRAN the RAN assistance information defined in TS 25.304 [3GPP TS 25.304] clause 5.10 and TS 24.312 [3GPP TS 24.312] clause 5.7.21B34 (OPI) are provided to the device by the UTRAN as specified in TS 25.331 [3GPP TS 25.331].

RAN rules may be used to support the selection of WLAN for performing the handover of one or more "off loadable" PDN connections. The RAN rules have been defined in TS 36.304 [3GPP TS 36.304] clause 5.6.2. The use of the RAN rules on the device has been defined in TS 23.402 [3GPP TS 23.402] and TS 24.302 [3GPP TS 24.302].

For traffic steering via RAN rules, the MME may provide information to the device indicating which PDN Connection can be offloaded to WLAN as specified in TS 23.401 [3GPP TS 23.401] clause 4.3.23. As specified in the same clause, traffic steering decisions using RAN rules are not applicable to non-seamless WLAN offload.

3.1.3 3GPP Operator policy coexistence

The WLAN access selection and the traffic routing behaviour of a device using SIM credentials within a single PLMN shall be controlled either by the ANDSF rules or by the RAN rules not by both. The device can be provisioned with both policies, and the device shall select the policy to be used as defined in TS 23.402 [3GPP TS 23.402] clause 4.8.6.4 and TS 24.302 [3GPP TS 24.302] clause 6.10.

3GPP Home Operator and/or Visited Operator policies may be used to assist the device in selecting a WLAN access point and in steering traffic between 3GPP and WLAN accesses.

For WLAN selection, according to TS 24.302 [3GPP TS 24.302] clause 5.1.3.2.3, the following applies:

- When the network uses RAN rules with a release 12 or post-release 12 device as defined in TS 23.401 [3GPP TS 23.401] clause 4.3.23 and TS 23.060 [3GPP TS 23.060] clause 5.3.21, a list of WLAN identities (e.g. SSID, HESSID) as part of RAN Assistance parameters may be sent by the 3GPP RAN to the device.
- When the network uses ANDSF rules with a release 12 or post-release 12 device as defined in TS 23.402 [3GPP TS 23.402] clause 4.8.2.1.6, the Home and Visited Operator WLAN Selection Policies (WLANSP) that include a list of Preferred Roaming Partners defined in WFA HS 2.0 [Passpoint] and identified by their PLMN identifiers or NAI Realms as specified in IEEE 802.11-2016 [IEEE 802.11-2016] and, for authentication purposes, a list of Preferred SSID may be sent to the device via OMA DM.

A device may be pre-provisioned by necessary subscription information (e.g. SSIDs and accompanying security keys) for connection to operator-owned WLAN access networks.

3GPP has, in addition, defined a set of I-WLAN parameters provisioned into the USIM [3GPP TS 31.102] to be used by the device. In addition, 3GPP has also defined OTA (Over The Air) mechanisms in order to update the USIM parameters including the WLAN parameters [3GPP TS 31.115] [3GPP TS 31.116]. However, as stated in TS 24.234 [3GPP TS 24.234] “WLAN Network Selection supersedes I-WLAN for device WLAN selection as specified in 3GPP TS 24.302 from Rel-12 onwards”. This means that WLAN selection and associated PLMN selection are non-backward compatible between Release 12 and pre-Release 12. This also means that Release 12 features are not supported by devices that use I-WLAN feature for WLAN selection and associated PLMN selection.

Req ID	Requirement
TSG22_R2_CM_01	A pre-Release 12 device SHALL support provisioning of WLAN parameters (e.g. network identifiers) using the USIM as specified in 3GPP TS 31.102 [3GPP TS 31.102] and 3GPP TS 24.234 [3GPP TS24.234]. However, as stated in TS 24.234 [3GPP TS 24.234] “WLAN

Req ID	Requirement
	Network Selection supersedes I-WLAN for device WLAN selection as specified in 3GPP TS 24.302 from Rel-12 onwards", no such requirement exists for Release 12 and post-Release 12 devices.
TSG22_R3_CM_49	A device that supports OMA DM Management Objects SHOULD support mandatory features of OMA DM Bootstrap as defined in [OMA Device Management Bootstrap] and the conditional features of OMA DM Bootstrap relevant to a GSMA device described in this document.
TSG22_R4_CM_50	A Release 12 or post-release 12 device SHOULD support provisioning of WLAN parameters (e.g. network identifiers) using the USIM via 3GPP ANDSF as specified in TS 23.402 [3GPP TS 23.402] , TS 24.302 [3GPP TS 24.302] clauses 5.1.3.2.3, 6.8 and 6.10 and TS 24.312 [3GPP TS 24.312].
TSG22_R4_CM_51	A Release 12 or post-release 12 device SHOULD support provisioning of WLAN parameters (e.g. network identifiers) using the USIM via 3GPP RAN Rules provisioned by E-UTRAN/UTRAN as specified in TS 23.401 [3GPP TS 23.401], TS 23.060 [3GPP TS 23.060], TS 36.304 [3GPP TS 36.304] clause 5.6, TS 36.331 [3GPP TS 36.331] clause 5.6.12, TS 25.304 [3GPP TS 25.304] clause 5.10, TS 25.331 [3GPP TS 25.331].

3.2 User/Manual Provisioning

In most devices today, manual provisioning is already available. This will often be the case for hotspots that the operator does not own and in home network setups. The facility often exists to store profiles so that every time a device is in range of an existing WLAN hotspot setup, the connection is automatic.

Req ID	Requirement
TSG22_R2_CM_03	A device SHALL allow the user to provision network identifiers (e.g. SSID), credentials and priorities.
TSG22_R2_CM_04	If the user manually provisions configurations in a device, they SHALL be stored in the USIM if the corresponding files are available, otherwise in the device.

4

Connection Management

4.1 Connection Management Client

Connection management clients interface between several layers providing an intuitive means of managing connectivity, preferences and networks. The implementation will vary per operating system and manufacturer but most of the work of the client should be to use API calls rather than issuing low level calls itself. This will make the build of clients easier and more uniform throughout devices and operating systems.

Connection management clients are in charge of managing all connections. In the context of this document, the connection management client, or application manages different WLAN access network connections based on a device status, connection conditions, operator policies and user profiles associated with these connections.

The following are examples of connection management APIs that a device could implement to improve WLAN management:

- Turn on and turn off the WLAN (including support of flight mode, where flight mode means that a device has the functionality to turn off wireless modules in case the transmitting and receiving of the wireless signals impacts the safety of aircraft flight.)
- Query if WLAN functionality is on or off
- Interact with the connection manager to connect to and disconnect from APs
- Use the operator predefined list of preferred network identifiers (e.g. SSID)
- Add, delete, modify and manage WLAN profiles, including information such as network identifiers (e.g. SSID), secured or open network, discover security methods and authentication credentials.
- Access to detailed information per network identifier, such as the WLAN signal strength per network identifier (e.g. SSID – active or inactive), WLAN channel physical rate, backhaul capability (if available), security methods and authentication credentials used, known or unknown network)
- Access to the list of available network identifiers (e.g. SSID)
- Support automatic & manual connection modes
- Force the association to a specific network identifier (e.g. SSID), visible or not.
- Listen to the WLAN events such as new available network, loss of network, successful association on a specific network identifier (e.g. SSID).
- Access to information on an active session using a specific network identifier (e.g. a SSID) such as IP address, MAC Address, Subnet Address
- Modify information on WLAN connection such as IP address, Subnet Address

Req ID	Requirement
TSG22_R2_CM_05	A device SHALL have at least one pre-installed connection management client.
TSG22_R2_CM_06	A device SHOULD have programming interfaces/APIs to control and/or manage WLAN connections.
TSG22_R2_CM_07	VOID
TSG22_R2_CM_08	A device SHOULD offer an API compliant with the OMA [OpenCMAPI] for WLAN management.
TSG22_R3_CM_46	The connection manager SHALL provide an API to turn on and turn off the WLAN including support of flight mode, where flight mode means that a device SHALL have the functionality to turn off wireless modules.
TSG22_R5_CM_63	A device SHOULD prefer a 5 GHz connection over a 2.4 GHz connection when both are available for the same specific network identifier.

4.2 Network Discovery

Constant scanning for detection of a hotspot may place a heavy toll on the battery life of a Smartphone. A device should implement periodic scanning algorithms that preserve battery life. The scanning algorithm should take into account Passpoint network discovery.

Req ID	Requirement
TSG22_R2_CM_10	A device SHALL be able to provide detailed information per network identifier discovered (such as signal strength, security methods, type of authentication credentials used, known or unknown network) to the user and/or application.
TSG22_R2_CM_11	A device SHALL support a WLAN access network discovery mechanism.
TSG22_R2_CM_12	A device SHOULD be able to listen & report events to an upper layer (e.g. UI) such as new available network, loss of network.
TSG22_R3_CM_47	A device's WLAN access network discovery mechanism SHALL preserve battery life.

4.3 WLAN Radio Link and Connection Quality

On most devices, once a WLAN is detected, a device defaults to use the WLAN connection to provide data connectivity to applications. Unfortunately, being connected to the AP does not necessarily mean that there is data connectivity to the Internet or that the connectivity will provide adequate user experience. For the purpose of WLAN access network selection (See Section 4.5) and management of multiple radio connections on the device (See Section 4.6), consideration of the WLAN radio link and connection quality are important to avoid poor user experience.

A device should consider over the air utilization of the WLAN AP (e.g. WLAN channel utilization which may be advertised in beacons), backhaul status of an AP (e.g. Wi-Fi Alliance Hotspot 2.0 WAN metrics information which may be obtained via an ANQP request), WLAN signal strength (e.g. WLAN Beacon RSSI as specified in TS 36.304 [3GPP TS 36.304] clause 5.6.2 for ANDSF and RAN rules) to avoid connection to an AP with no connectivity or which is not suitable to provide basic connectivity. The criteria defining a suitable AP may be default criteria in the device and should include at least a minimum signal strength level (e.g. WLAN Beacon RSSI), a maximum channel utilisation value for air interface loading (as defined by WLAN channel utilization in IEEE 802.11) and a minimum backhaul bandwidth threshold. The minimum backhaul bandwidth may be derived from information received in Wi-Fi Alliance Hotspot 2.0 WAN metrics Information element. These criteria may also be preconfigured by the operator in the device or provisioned as part of operator policy. If criteria (e.g. as defined by priorities and/or thresholds) are pre-configured or provisioned by the operator, they should be considered with higher priority than default values. The device may in addition have proprietary schemes to consider additional parameters in order to determine whether the AP is adequate or not.

Once a device is connected on a WLAN access network it should be able to monitor whether the AP can continue to provide adequate throughput (as defined by a default minimum throughput threshold criterion, preconfigured operator policy on minimum throughput threshold or operator provisioned policy containing a minimum throughput threshold). If the minimum throughput threshold cannot be satisfied, the device should be able to switch its connection to another AP or to a 3GPP network.

Req ID	Requirement
TSG22_R2_CM_13	A device SHALL have the capability to monitor the WLAN signal strength (e.g. WLAN Beacon RSSI).
TSG22_R2_CM_14	A device SHOULD consider the following parameters, when available, in selection of a AP, based on default priorities and/or thresholds for those parameters specified by the manufacturer: - WLAN signal strength (WLAN Beacon RSSI) - IEEE 802.11 Channel Utilization IE - Wi-Fi Alliance Hotspot 2.0 WAN Metrics IE
TSG22_R2_CM_15	A device SHOULD be able to monitor the data throughput level on the serving AP.
TSG22_R2_CM_16	A device SHOULD have the ability to switch their network connection away from a serving AP which is not providing adequate throughput (as defined by a minimum throughput threshold criterion, which is default, preconfigured by operator policy, or provisioned by operator policy) to another AP, or to a 3GPP network.
TSG22_R2_CM_17	A device MAY support provisioning with priorities and/or thresholds related to WLAN signal strength and quality, WLAN Beacon RSSI, Wi-Fi Alliance Hotspot 2.0 WAN metrics information and minimum WLAN data throughput level e.g. pre-configured or as part of operator policies.
TSG22_R2_CM_18	A device SHOULD use provisioned priorities and /or thresholds by the operator, when present, with higher priority than default manufacturer priorities/thresholds.
TSG22_R4_CM_52	A release 12 and post-release 12 device, SHALL use 3GPP operator policies and RAN assistance parameters as defined in TS 23.402 [3GPP TS 23.402] clause 4.8, TS 24.302 [3GPP TS 24.302] clauses 5.4, 6.8 and 6.10 and TS 24.312 [3GPP TS 24.312] for ANDSF and in TS 23.401 [3GPP TS 23.401] clause 4.3.23, TS 23.060 [3GPP TS 23.060] clause 5.3.21, TS 36.304 [3GPP TS 36.304] clause 5.6 , TS 36.331 [3GPP TS 36.331] clause 5.6.12, in TS 25.304 [3GPP TS 25.304] clause 5.10 and TS 25.331 [3GPP TS 25.331] for RAN rules.

4.4 Intermittent WLAN Connectivity

Users would like to be connected to the best available resource as much as possible with minimum interruption to usability.

Maximising available resources such as switching to higher bandwidth WLAN presents an attractive alternative to users. However, minimum interruption should be ensured.

Automatically switching from WLAN access to another WLAN or to 3GPP access (2G/3G/LTE) may present usability problems to a device if it is not properly configured to handle such scenarios.

Hysteresis (meaning that the threshold to switch to WLAN access is different from the threshold to switch away from that access) mechanisms should be implemented with tuned radio thresholds, so that a device which is experiencing signal strength or throughput degradation from its serving AP can determine when to switch to another AP or to 3GPP access.

The device should have a defined access threshold at which it will release its connection to the serving AP, even if there is no other WLAN or 3GPP access network available.

In some cases, WLAN access could be temporarily denied from the network for technical or marketing reasons, without displaying any message to the customer. A device in this situation should avoid network overload by too many successive request attempts.

Req ID	Requirement
TSG22_R2_CM_19	A device SHALL have a hysteresis mechanism to prevent disconnect followed by connection or re-connection in a minimal interval with no improvement in connection conditions.
TSG22_R2_CM_20	A device SHALL limit the number of access retries to the same AP when it receives temporary denied access notification from that AP, according to a limit which may be defined by an operator. (e.g. 1026 notification with EAP-SIM in RFC 4186 [RFC 4186])

4.5 WLAN Access Network Selection

WLAN access network selection in a pre-release 12 device should take into consideration 3GPP operator policies for WLAN access network selection. The operator policies may indicate priority among WLAN access networks e.g. based on a pre-configured list of network identifiers or provisioned by the 3GPP operator. The 3GPP operator policies should have highest priority among all available policies in the device for network selection. However, user preference settings should be able to override 3GPP operator policies on WLAN selection.

A device should be able to support association on a preferred WLAN access network, if the SSID is broadcast. Moreover, in order to avoid selection of a WLAN access network with poor radio link and/or data connection quality, a device should evaluate whether a WLAN access network is suitable, according to the requirements of Section 4.3 of this PRD. The criteria for determining whether a WLAN access network is suitable can be default criteria in the device, a criteria pre-configured by the operator or provisioned as part of operator policies for WLAN access network selection.

In the presence of more than one suitable WLAN access network, a device should select the one prioritised by the 3GPP operator policy (unless overridden by user preference settings). A device should also prefer a WLAN access network that is suitable over one that is not

suitable, when both networks are allowed by 3GPP operator policy (even though the WLAN access network that is not suitable may be prioritised by the policy).

4.5.1 3GPP WLAN Access Network Selection

Per TS 23.402 [3GPP TS 23.402] clause 4.8.6.4, WLAN access network selection in a release 12 or post-release 12 device is based either on ANDSF policies as defined in TS 23.402 [3GPP TS 23.402] clause 4.8, or on RAN rules as defined in TS 23.401 [3GPP TS 23.401] clause 4.3.23 and TS 23.060 [3GPP TS 23.060] clause 5.3.21. Both ANDSF policies and RAN rules are provided by the 3GPP operator. The operator policies may indicate priority among WLAN access networks provisioned by the 3GPP operator. The 3GPP operator policies should have highest priority among all available policies in the device for network selection. However, user preference settings should be able to override 3GPP operator policies on WLAN selection.

A WLAN can provide the device with EPC access in two different flavours: either the WLAN is considered by the operator as a “Trusted access network” per TS 23.402 [TS 23.402] clause 4.3.1.2 and the Trusted WLAN (TWAN) can access a PDN GW via S2a interface, or the WLAN is considered by the operator as an “Untrusted access network” per TS 23.402 [TS 23.402] clause 4.3.1.2 and the device can connect to an Evolved Packet Data Gateway (ePDG) in order to access a PDN GW via S2b interface.

Req ID	Requirement
TSG22_R2_CM_22	A 3GPP device SHOULD consider policies for WLAN access network selection received from a 3GPP operator with the highest priority (unless overridden by user preference settings).
TSG22_R2_CM_23	A device SHALL be able to support the association to a WLAN access network where the SSID is not broadcast.
TSG22_R4_CM_59	A release 12 and post-release 12 device, SHALL consider policies received from the 3GPP operator i.e. either ANDSF policies including the support of RAN Assistance parameters as defined in TS 23.402 [3GPP TS 23.402] clause 4.8, or RAN rules as defined in TS 23.401 [3GPP TS 23.401] clause 4.3.23 and TS 23.060 [3GPP TS 23.060] clause 5.3.21 with highest priority (unless overridden by user preference settings).
TSG22_R4_CM_60	A release 12 or post-release 12 device, when provisioned with both ANDSF and RAN rules, SHALL select the policy to be used as defined in TS 23.402 [3GPP TS 23.402] clause 4.8.6.4 and TS 24.302 clause 6.10.
TSG22_R4_CM_61	A release 12 or post-release 12 device, when using ANDSF, SHALL select a WLAN as defined in TS 23.402 [3GPP TS 23.402] clause 4.8, TS 24.302 clauses 5.1.3.2.3, 6.8 and 6.10 and TS 24.312 [3GPP TS 24.312].
TSG22_R4_CM_62	A release 12 or post-release 12 device, when using RAN Rules, SHALL select a WLAN as defined in TS 36.304 [3GPP TS 36.304] clause 5.6 and in TS 36.331 [3GPP TS 36.331] clause 5.6.12 for E-UTRAN, in TS 25.304 [3GPP TS 25.304] clause 5.10 and in TS 25.331 [3GPP TS 25.331] for UTRAN.

4.6 Managing Radio Connections based on Multiple Access Technologies

3GPP operators would like to effectively manage the distribution of data traffic between the 3GPP and WLAN access networks in order to maximise the overall system capacity whilst not compromising the user experience. In order to achieve those objectives, it is required that a device can offload a data flow from 3GPP to WLAN as well as switch the data flow back from WLAN to 3GPP. If the device has more than one data flow e.g. from different applications running in parallel on the device, it is also required that the device can maintain both the 3GPP connection and WLAN connection to allow distribution of the separate flows on different access technologies.

The 3GPP operator may provide a device with policies (e.g. subscription specific policies) that indicate, for example, the preferred access technology (e.g. 3GPP vs. WLAN) to use under specific conditions, priority among WLAN access networks or how traffic should be distributed between the 3GPP and WLAN access networks. The conditions for applying specific policies such as location and time and the rules for distributing traffic between access technologies may be based on policy management solutions, for example, ANDSF (Access Network Discovery and Selection Function) as defined in 3GPP TS 23.402 [3GPP TS 23.402], 3GPP TS 24.302 [3GPP TS 24.302] and TS 24.312 [3GPP TS 24.312].

A device should adhere to policies received from the 3GPP network e.g. priority among WLAN access networks or between 3GPP and WLAN, unless this would conflict with user preference settings (which should be considered with highest priority) or would result in selection of a WLAN access network that is not suitable. The device should evaluate whether a WLAN access network is suitable according to the principles in Section 4.3 of this PRD. Thus, in presence of more than one suitable WLAN access network, a device should select the one prioritised by the 3GPP operator policy (unless overridden by user preference settings). A device should also prefer a WLAN access network that is suitable over one that is not suitable, when both networks are allowed by 3GPP operator policy (even though the WLAN access network that is not suitable may be prioritised by the policy).

A device may also consider the status of a device e.g. battery life for choosing not to connect to a WLAN access network (and connect to 3GPP), provided that no 3GPP operator policy is available that prioritises WLAN over 3GPP or 3GPP operator policy prioritises WLAN, but the available WLAN access networks (that can be accessed according to operator policy) are not suitable. Alternatively, a device may connect to a WLAN access network that is not suitable if there is no other connectivity option available i.e. the 3GPP network or another suitable WLAN access network that the device is allowed to access according to operator policy or a WLAN access network prioritised by user preference.

Req ID	Requirement
TSG22_R2_CM_24	A device SHOULD be able to off-load a data flow from 3GPP to WLAN (and vice versa).
TSG22_R2_CM_25	A device SHOULD be able to maintain concurrent 3GPP and WLAN connectivity.
TSG22_R2_CM_26	VOID
TSG22_R2_CM_48	VOID

TSG22_R3_CM_50	A device SHALL enable the selection of the appropriate access technology based on the following priority order: 1) User Preference 2) Operator Policy 3) Device status and heuristics

4.7 Traffic management across RATs

Maintaining network operator services across varying network technologies provides better network performance through offloading. However, disruption of services should be kept at a minimum when switching between different network technologies e.g. switching from 3G to WLAN.

It is important that the mobile network connection be kept when a device switches between network technologies for the following reasons:

- For core network capacity (i.e. no new PDP context establishment on 3GPP on every AP connection).
- Charging tickets processing load
- Transparent user interface

It is important that network inactivity timer mechanisms keep working as normal. When a device attaches to a new AP, the following scenarios may apply (in networks configured via DHCP or with static IP configuration):

1. Switch between APs within the same BSS. In this case, the IP layer connectivity stays the same (layer 2 handover only).

2. Switch between APs of different BSSs within the same ESS. Depending on the implementation, IP connectivity may stay the same, but may also change.

3. Switch to an AP of a different ESS, the AP/network is known and configured, and the old lease is not outdated. For example, in private networks, leases can be in the range of days or even static and therefore this situation is not uncommon.

If a devices AP changes, the DHCP function of a device should issue a DHCP request to the new AP even if the identity or network identifier (e.g. SSID) of the AP does not change. However, this process could be slow since the device needs to go through a complete DHCP exchange before it is able to communicate. RFC 4436 [RFC 4436] proposes to cache information about the network (own IP configuration parameters, MAC and IP addresses of test node(s) in the network) and to probe them quickly using (unicast) ARP after the link comes up.

If the probing confirms that the network looks the same, there is no need to re-acquire the IP address via DHCP. The device simply continues to use its current lease. Nevertheless, it is recommended to do DHCP in parallel, to avoid additional delays if the probes result in a negative answer.

If a device retains information about multiple networks, it can also accelerate the return to your private networks. It also helps if a device switches back and forth between two hotspots for some reason.

In order to improve the IP address utilisation, a device shall send DHCP Release message to an AP to release its IP address in the following circumstances:

1. Users disconnect from applications
2. Users switch from the current network identifier to another
3. Users turn WLAN off
4. Users turn Flight Mode on when one network identifier is connected

3GPP signaling procedures for moving PDN connections between 3GPP and WLAN accesses while ensuring IP address preservation are specified in TS 23.402 [3GPP TS 23.402] for “untrusted WLAN” (based on SWu and S2b) and in TS 23.402 [3GPP TS 23.402] clause 16 signaling procedures for “trusted WLAN” (based on SWw and S2a).

The decision to move certain traffic between 3GPP access and WLAN is taken by the device, based on policy rules and assistance provided by the network, measurements performed by the device and local operating environment information. For 3GPP devices, using USIM credentials for authentication, these policy rules may be either ANDSF traffic steering rules per TS 23.402 [3GPP TS 23.402] clause 4.8, TS 24.302 [3GPP TS 24.302] clauses 5.4, 6.8 and 6.10 and TS 24.312 [3GPP TS 24.312], or 3GPP RAN traffic steering rules per TS 23.401 [3GPP TS 23.401] clause 4.3.23, TS 23.060 [3GPP TS 23.060] clause 5.3.21, TS 36.304 clause 5.6 [3GPP TS 36.304], TS 36.331 [3GPP TS 36.331] clause 5.6.12, TS 25.304 [3GPP TS 25.304] clause 5.10 and TS 25.331 [3GPP TS 25.331].

Both ANDSF and RAN rules may use RAN assistance parameters as described in these clauses. ANDSF additionally uses OPI RAN Assistance parameter as defined in TS 24.312 [3GPP TS 24.312] clause 5.7.21B34. Coexistence between ANDSF and RAN rules is described in TS 23.402 [3GPP TS 23.402] clause 4.8.6.4.

Req ID	Requirement
TSG22_R2_CM_39	VOID
TSG22_R2_CM_40	A device SHALL keep the 3GPP mobile network connection e.g. PDP contexts during WLAN access.
TSG22_R2_CM_41	A device SHALL send a DHCP Release message to an AP to release its IP address in the following circumstances: 1. Users disconnect from applications 2. Users switch from the current network identifier to another 3. Users turn WLAN off 4. Users turn Flight Mode on when one network identifier is connected
TSG22_R2_CM_42	A device SHOULD implement the Detecting Network Attachment in Ipv4 (DNAv4) [RFC 4436]. When implemented, the mechanism SHALL be applied every time a radio link to a new AP is established, even if the identity or network identifier (e.g. SSID) of the AP does not change.

TSG22_R2_CM_43	VOID
TSG22_R2_CM_44	VOID
TSG22_R2_CM_45	VOID
TSG22_R4_CM_46	Release 12 and post-release 12 devices SHOULD implement ANDSF traffic steering rules including the support of RAN Assistance parameters per TS 23.402 clause 4.8 (Inter-System Routing Policy and Inter-APN Routing Policy), TS 24.302 [3GPP TS 24.302] clauses 5.4, 6.8 and 6.10 and TS 24.312 [3GPP TS 24.312].
TSG22_R4_CM_47	Release 12 and post-release 12 devices SHOULD implement traffic steering using RAN rules per TS 23.401 clause 4.3.23, TS 23.060 [3GPP TS 23.060] clause 5.3.21., TS 36.304 [3GPP TS 36.304] clause 5.6 and TS 36.331 [3GPP TS 36.331] clause 5.6.12 for E-UTRAN, TS 25.304 [3GPP TS 25.304] clause 5.10 and TS 25.331 [3GPP TS 25.331] for UTRAN.
TSG22_R4_CM_48	Release 12 and post-release 12 devices SHOULD implement 3GPP Rel-12 procedures for the support of moving PDN connections between 3GPP access and trusted WLAN where the device IP address is preserved.
TSG22_R4_CM_49	Release 12 and post-release 12 devices SHOULD implement 3GPP procedures for the support of moving PDN connections between 3GPP access and untrusted WLAN where the device IP address is preserved.

4.8 IP Version Support

Increasingly Wi-Fi networks are supporting IPv6 and it is important that support of IPv6 becomes widespread and mandatory for all new devices.

The following device requirements are considered the minimum needed to enable universal support of the set of IPv6 features in networks and a device. This is also consistent with the IPv6 device requirements of a device using 3GPP networks.

Req ID	Requirement
TSG22_R2_CM_28	A device SHALL support IPv6 [RFC 2460]
TSG22_R2_CM_29	A device SHALL support the ICMPv6 protocol [RFC 4443]
TSG22_R2_CM_30	A device SHALL support the Neighbour Discovery Protocol [RFC 4861]
TSG22_R2_CM_31	A device SHALL support Stateless Address Auto Configuration (SLAAC) [RFC 4862]
TSG22_R2_CM_32	A device SHALL support the Privacy Extensions for Stateless Address Autoconfiguration in IPv6 [RFC 4941]
TSG22_R2_CM_33	A device SHOULD support (stateless) DHCPv6 client [RFC 3736]
TSG22_R2_CM_34	A device SHOULD support Router Advertisement Option for DNS configuration [RFC 6106]
TSG22_R2_CM_35	A device SHOULD support IPv6 Router Advertisement Flags Options [IETF RFC 5175]

Req ID	Requirement
TSG22_R2_CM_36	A device SHOULD be able to perform Path MTU Discovery [RFC 1981]
TSG22_R2_CM_37	A device browser SHALL support IPv6, both for HTTP access and access with a proxy configuration.
TSG22_R2_CM_38	A device MAY use DHCPv6 for the IP address assignment.

5 Security

5.1 Authentication Protocols

In order to support a seamless authentication experience in WLAN, it is a requirement to provide consistent support for the appropriate authentication mechanisms. There are (U)SIM-based and non-(U)SIM-based authentication mechanisms available to authenticate on WLAN access networks. GSMA member operators require that (U)SIM based authentication shall be used by a device with (U)SIM to authenticate on a WLAN access network that has a roaming agreement (either direct or via a VPLMN) with the HPLMN of the (U)SIM.

GSMA operators believe that (U)SIM-based authentication can increase WLAN usage. Furthermore, Passpoint requires that a (U)SIM based device shall support (U)SIM-based authentication for WLAN access [Passpoint].

Among non-(U)SIM based authentication mechanisms, EAP-TLS and EAP-TTLS have been identified as mandatory mechanisms according to Passpoint.

5.1.1. (U)SIM based EAP methods and 3GPP Service Provider selection

The EAP (Extensible Authentication Protocol) is an authentication framework that provides for the transport and usage of cryptographic keys and parameters generated by the EAP-methods. To mirror the security and authentication for GSM, UMTS and LTE, a device shall support EAP-SIM, EAP-AKA and EAP-AKA' for IEEE 802.1X-based WLAN access according to 3GPP TS 33.234 [3GPP TS 33.234] and 3GPP TS 33.402 [3GPP TS 33.402]. This support includes the mechanism for identify privacy, which is used to avoid sending clear-text permanent subscriber identification information. Identity privacy in EAP-SIM, EAP-AKA and EAP-AKA' is based on temporary identities, or pseudonyms, which are defined in 3GPP TS 33.234 [3GPP TS 33.234].

A device shall request the available EAP methods, to determine if they correspond to the type of SIM/UICC it holds, when connecting to a WLAN access network. The response will enable the device, based on its configuration, to determine which EAP method to use.

A device with:

- a SIM inserted and selected shall use EAP-SIM to authenticate with a WLAN that has a roaming agreement (either direct or via a VPLMN) with the HPLMN of the SIM.
- a UICC inserted and a USIM selected shall, by default, use either EAP-AKA or EAP-AKA' to authenticate with a WLAN that has a roaming agreement (either direct or via a VPLMN) with the HPLMN of the USIM. However, in order to cover the case where the HPLMN AAA server does not yet support EAP-AKA or EAP-AKA', it shall be possible for the operator to configure the device to use EAP-SIM when connecting to

a WLAN access network that has a roaming agreement (either direct or via a VPLMN) with the HPLMN of the USIM.

For the authentication procedure, the device shall include the root NAI when the device attempts to authenticate directly to its HPLMN or the decorated NAI when the device attempts to authenticate to the HPLMN via a VPLMN.

For pre-release 12, release 12 and post release 12 devices, the selection of a 3GPP Service Provider, which is required to construct the NAI, has been specified by 3GPP as follows:

Pre-Release 12 devices, procedures are specified in TS 24.234 [3GPP TS 24.234] clause 5.2.

Release 12 and post-release 12 devices, procedures are specified in TS 24.302 [3GPP TS 24.302] clause 5.2.3.2.

Req ID	Requirement
TSG22_R2_SEC_01	VOID
TSG22_R2_SEC_02	A device with a SIM inserted and selected SHALL use EAP-SIM to authenticate with a WLAN that has a roaming agreement (either direct or via a VPLMN) with the HPLMN of the SIM.
TSG22_R2_SEC_03	A device with a UICC inserted and a USIM selected SHALL by default use either EAP-AKA or EAP-AKA' to authenticate with a WLAN that has a roaming agreement (either direct or via a VPLMN) with the HPLMN of the USIM.
TSG22_R2_SEC_04	It SHALL be possible for the operator to configure whether a device, with a USIM inserted and a USIM selected, is allowed to use EAP-SIM (when supported by the USIM) when connecting to a WLAN that has a roaming agreement (either direct or via a VPLMN) with the HPLMN of the USIM. This might be, for example, in the factory or by another method. Note: This is to cover the case where the HPLMN AAA does not support EAP-AKA or EAP-AKA'.
TSG22_R2_SEC_05	It SHALL be possible for the operator to configure whether a device, with a USIM inserted and a USIM selected, shall use EAP-AKA or EAP-AKA' when connecting to a WLAN that has a roaming agreement (either direct or via a VPLMN) with the HPLMN of the USIM. This might be, for example, in the factory or by another method.
TSG22_R2_SEC_06	VOID
TSG22_R3_SEC_09	A device SHALL support identity privacy mechanisms described in EAP-SIM [RFC 4186] / EAP-AKA [RFC 4187] / EAP-AKA' [RFC 5448]
TSG22_R3_SEC_10	A device, with a USIM inserted and a USIM selected, SHALL store the pseudonym, re-authentication identities and related parameters used in the identity privacy mechanism and in the fast re-authentication mechanism, respectively, in the UICC when the corresponding files are present as specified in [3GPP TS 31.102], so that it can be maintained across reboots.

Req ID	Requirement
TSG22_R4_SEC_11	A pre-release 12 device, with a USIM inserted and a USIM selected, SHALL support PLMN selection procedure as specified in TS 24.234 [3GPP TS 24.234] clause 5.2.
TSG22_R4_SEC_12	A release 12 or post-release 12 device, with a USIM inserted and a USIM selected, SHALL support 3GPP Service Provider selection as defined in TS 24.302 [3GPP TS 24.302] clause 5.2.3.2.
TSG22_R6_SEC_13	It SHALL be possible for a device to request the available EAP methods, to determine if they correspond to the type of SIM/UICC it holds, when connecting to a WLAN access network.

5.1.2. (U)SIM based EAP methods error handling

The (U)SIM based EAP methods (EAP-SIM, EAP-AKA and EAP-AKA') define various error codes for terminal authentication, as AT Notification Codes [RFC 4186/RFC 4187]. The following table defines terminal behaviour for these codes:

AT Notification Code	Description	Terminal Behaviour
0	General failure after authentication	Advise user about error indicating that authentication has succeeded but error occurred afterwards. User is advised to check with service provider about their subscription.
1026	User has been temporarily denied access	Advise user about error and prompt for retry or automatically retry within MAX_RETRY_VALUE. The default value shall be "Retry every 20 seconds up to 3 attempts".
1031	User has not subscribed to the requested service	Advise user about error, for example remediation, and provide assistance about their subscription. Also see section 7.3.
16384	General failure	Advise user about error.
32768	Success	Authentication is successful.

5.2 WLAN Over the Air Security

Wi-Fi Protected Access 2 Enterprise (WPA2-Enterprise) with Protected Management Frames (PMF) is the latest version of the security protocol and security certification

programme developed by the Wi-Fi Alliance to secure the access to a WLAN access network which has the support of an authentication server. To provide a secure means of communication for a device over a WLAN air interface, WPA2-Enterprise with PMF is mandatory. The Wi-Fi Alliance also mandates that a Wi-Fi CERTIFIED device supports the WPA2-Personal mode of operation which offers similar level of security over the air without the need for an authentication server (depending on the strength of the user defined passphrase). Support for older and non-secure security mechanism (e.g. WEP) should be discontinued in favour of newer and more secure mechanisms. For both operators and customers, using the (U)SIM card for authentication and security is a convenient means to simplify the process for subscribers.

WPA2-Enterprise with PMF (and WPA2-Personal) is a mandatory requirement for a device (refer to Section 2.1 of this PRD).

Req ID	Requirement
TSG22_R2_SEC_07	A device SHALL NOT support WEP.
TSG22_R5_SEC_13	A device SHALL NOT support TKIP.

Wi-Fi Protected Setup

6 Some technologies require a level of technological skill or background to setup or utilise. By providing an easier means for connecting through hotspots, setup becomes easier for non-technically adept users, providing a broader reach for a device and services.

It is often quite challenging for the customer to gain access using their device to connect to a WLAN access network at home or in a small office environment as they must access the right network identifier (e.g. SSID) and enter the correct security key without any errors.

Wi-Fi Protected Setup is an optional certification program in Wi-Fi Alliance designed to ease this process and set up of security-enabled WLAN access networks at home or in a small office environment.

This certification program provides several easy-to-use methods to configure a network and different devices to access it:

- Push-Button Configuration
- PIN / numeric code
- Near Field Communication (NFC) method in which a customer touches a token or a card with his NFC enabled device.

Req ID	Requirement
TSG22_R2_SEC_08	An NFC enabled device SHOULD support Wi-Fi CERTIFIED Wi-Fi Protected Setup NFC.

7

User Interface

7.1 WLAN On/Off Function Accessibility

Turning off the WLAN radio on intervals when it is not used can increase battery life.

A device has a means of turning off the WLAN radio from an application or setting that is accessible through a menu or application icons. Accessibility to this feature should be as easy as possible for the user.

Req ID	Requirement
TSG22_R2_USE_03	A device SHALL have an accessible means for the user to toggle the WLAN radio on or off.

7.2 Status Information

For better user experience, pertinent device status information should be provided to the user using a consolidated or convenient interface such as icons and or status notifications.

Status information, such as network coverage, signal level and battery strength, byte counter, connection manager, network identity, encryption status, shall be provided through an application or operating system information. Additional information from Passpoint can also be provided, such as WLAN link status, WLAN uplink and downlink data rates. WLAN access network name or logo should be displayed when connected to Passpoint APs.

Status about authentication success and failure may also be indicated on a device. If the WLAN connection is insecure, a notification message should be displayed to the user when a device associates with an AP for the first time.

If the WLAN connection is secure (i.e. AP is Passpoint certified or supports WPA2-Enterprise and EAP authentication over IEEE 802.1X), an icon indicating a secure connection should be visible to the user (e.g. padlock layered on WLAN signal strength icon). If the WLAN connection is insecure, a notification message should be displayed to the user when a device associates with the AP for the first time.

Req ID	Requirement
TSG22_R2_USE_04	A device that has a UI SHALL indicate the status of the device connection.
TSG22_R2_USE_05	A device SHOULD offer programming interfaces providing Status Information to applications.
TSG22_R2_USE_06	A device SHOULD offer an API compliant with the OMA [OpenCMAPI] for Status Information & notifications functions.
TSG22_R2_USE_07	Link status information from a Passpoint AP MAY be used to improve link status information presented to the user or applications.

7.3 Authentication Architecture Overload Data Prevention

In some networks, EAP authentication could be reserved for some tariff plans for marketing reasons (e.g. no WLAN access for basic offers).

Hence, some devices could be parameterised with automatic EAP authentication and perform automatic connection attempts to a WLAN access network. If the network rejects the access request of a device for a repeated number of times due to WLAN barring, the device must stop any other request until a manual attempt is made. Otherwise, this could lead to some core network overload.

Frequent attempts to connect to barred APs will have a detrimental effect on usability and battery life.

According to the relevant IETF RFCs, certain EAP-enabled authentication frames support Fast Re-authentication methods. These are enabled by the Authentication Server providing Fast Re-Authentication Identity and other parameters to the WPA™ supplicant instantiated on the end-user device, as part of normal Full Authentication procedure. When the WPA supplicant requires authentication subsequent to a given Full Authentication, it can optionally use a Fast Re-authentication procedure.

Note:

- compared to Fast Re-authentication, Full Re-Authentication places a number of additional loading factors on service-provider access and core-network resources;
- compared to 3GPP mobile data RAN infrastructure, challenges to predicting and engineering against WLAN attachment/detachment scenarios. When Full Authentication is required for each device re-attachment, the additional load becomes difficult to predict.
- For example, with EAP-SIM, according to RFC 4186 clause 10.18, when receiving the error code 1031 – User has not subscribed to the requested service.

For these reasons, where authentication frames support Fast Re-authentication procedures, these should be supported in a device.

Req ID	Requirement
TSG22_R2_USE_08	A device SHALL refrain from attempting an automatic connection when barred due to permanent (and not temporary) authentication failure or notification after the authentication request is rejected, unless a manual attempt is made.
TSG22_R2_USE_09	A device with a UI SHALL notify to the user the failure of authentication.
TSG22_R2_USE_10	A device SHALL implement the fast re-authentication mechanism described in the RFC 4186 – EAP SIM.
TSG22_R2_USE_11	A device SHALL support fast re-authentication mechanism described in the EAP AKA [RFC 4187] / EAP AKA' [RFC 5448].

7.4 Access to U/SIM When 3GPP Radio is in Flight Mode

There is the potential use case for a terminal to have its Wi-Fi radio enabled but its 3GPP radio is off, such as the 3GPP radio being in flight mode. One such case may be in an aircraft where use of the Internet via an on board Wi-Fi network is permitted but the use of cellular radio is still banned. Some customers turn off their 3GPP connections when roaming and their devices should still be able to use Passpoint based authentication when roaming.

If the WLAN is Passpoint enabled, then the terminal needs to be able to access the U/SIM credentials for authentication on the WLAN even though the 3GPP radio is off or in flight mode.

Req ID	Requirement

TSG22_R3_USE_12	Terminals SHOULD allow Passpoint authentication using U/SIM credentials even though the 3GPP radio is off or in flight mode.

Power Management

8.1 Power Save Mechanisms

8 A mobile device that presents poor battery longevity can result in less usefulness to users, due to its mobile nature; such a device can benefit from power save mechanisms.

Req ID	Requirement
TSG22_R2_USE_12	VOID
TSG22_R2_USE_13	VOID
TSG22_R2_USE_14	VOID
TSG22_R2_USE_15	VOID
TSG22_R2_USE_16	A device SHOULD maintain WLAN access network connectivity while preserving battery life.

8.2 Idle Power Management

A device, although idle, may be using power due to the requirement for network connections to be kept open.

Req ID	Requirement
TSG22_R2_USE_17	A device SHOULD have a traffic inactivity duration setting to trigger power save mechanism.
TSG22_R2_USE_18	VOID

9

Parental Control

Some Mobile Network Operators require parental control or content policing due to regulatory requirements.

Mobile operators are able to filter web content inappropriate for children (under-age people) when browsing the Internet using 3GPP data. WLAN is ubiquitous and can be operated by individuals without the need for a license to operate the AP, thus there is no obligation for these individuals to enforce policies such as adult content filtering.

Req ID	Requirement
TSG22_R2_USE_19	A device SHALL support a mechanism for Parental Control for access to unsuitable web content for children.
TSG22_R2_USE_20	A device SHOULD have their native internet browsers to support parental control.

TSG22_R2_USE_21	A device SHOULD restrict download of third party browsers without parental control feature.
TSG22_R2_USE_22	A device MAY support a mechanism to lock/unlock the unlicensed radio access to the internet.

NOTE: There is no specification of a standard device assisted parental control mechanism currently available in the industry and device implementations are expected to track the outcome of on-going and completed work in this area between a number of high-profile industry and regulatory bodies including, in Europe, the European Commission. The requirements on the characteristics of a parental control mechanism in this document are guidelines and may be superseded or complemented by industry norms on parental control mechanisms for the device and/or content filtering norms for the content delivery infrastructure developed by such committees.

IMS Services

10

There are existing GSMA PRDs that are relevant to service support on terminals. They should be considered in conjunction with this document. With respect to the support of IMS based services being delivered over WLAN, the relevant GSMA PRDs are:

- IR.51 IMS Profile for Voice, Video and SMS over untrusted Wi-Fi access, Version 6.0, 01 May 2018
- IR.61 Wi-Fi Roaming Guidelines, Version 12.0, 27 September 2017
- IR.92 IMS Profile for Voice and SMS, Version 12.0, 02 May 2018
- IR.94 IMS Profile for Conversational Video Service, Version 12.0, 12 June 2017

With the deployment of Passpoint networks, the development of Carrier Wi-Fi as well as presence of Wi-Fi in many homes, operators are now wishing to deploy services that make use of the Wi-Fi networks to deliver services to their customers. An example of such is IMS based service over Wi-Fi, in particular voice (Wi-Fi Calling) and SMS.

Terminals using Wi-Fi requiring to use these services, must be able to access the EPC via WLAN, either trusted WLAN or untrusted WLAN, as defined in 3GPP TS 23.402.

The terminals need to support the following aspects:

- IMS basic capabilities and supplementary services for telephony
- Real-time media negotiation, transport, and codecs
- Wi-Fi wireless technology (as described in this document GSMA PRD TS.22) and (evolved) packet core capabilities
- Functionality that is relevant across the protocol stack and subsystems.

A terminal compliant to this profile must support IMS-based telephony as detailed in the GSMA PRD IR.51 which defines a voice and video over Wi-Fi IMS profile by profiling a number of Wi-Fi, (Evolved) Packet Core, IMS core, and terminal features. These features are considered essential to launch interoperable IMS based voice and video over Wi-Fi. GSMA PRD IR.51 is based on the IMS Voice and SMS profile described in GSMA PRD IR.92 and on the IMS Profile for Conversational Video Service profile described in GSMA PRD IR.94. The defined profile is compliant with 3GPP specifications.

GSMA PRD IR.51 also references this document, GSMA PRD TS.22, which outlines the Wi-Fi wireless technology and packet core feature set. Consequently, the two documents need to be considered in unison.

Reference also needs to be made to GSMA PRD IR.61, which describes some of the network and terminal requirements for the support of SWu, SWw and S2b interfaces.

The terminal needs to be able to support a PDN connection as defined in 3GPP TS 23.402 [3GPP TS 23.402] to the EPC over the Wi-Fi wireless interface to access IMS based voice, SMS and video services.

NOTE: Emergency calls over EPC-integrated Wi-Fi is not specified in 3GPP.

This document only provides details of access to the EPC using untrusted Wi-Fi networks as supported by terminals and networks.

If the terminals support either IMS-based voice or SMS or video services, (or a combination), the following requirements must be met by the terminal.

Req ID	Requirement
TSG22_R3_SVC_01	Terminals MAY support IMS based voice, or SMS, or video service, over Wi-Fi.

10.1 Support of Access to EPC via Untrusted WLAN on Terminals

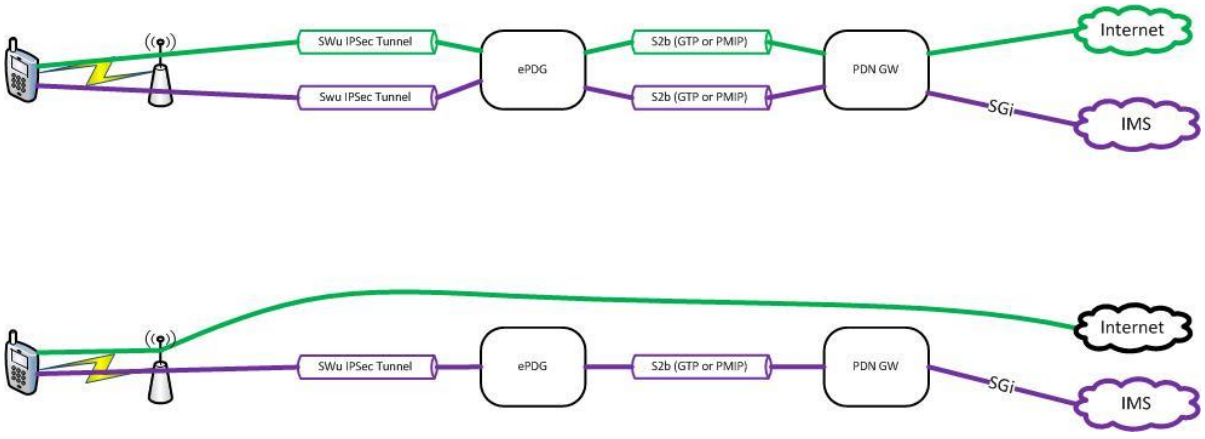

Figure 1: VoWiFi on untrusted WLAN based on SWu and S2b – two possible options

Terminals shall support the SWu interface for connection to the Evolved Packet Data Gateway, ePDG, for access to the EPC. The ePDG is connected to the PDN GW, via the S2b interface. This will allow for delivery of IMS based services over untrusted Wi-Fi networks.

Req ID	Requirement

TSG22_R3_SVC_02	If terminals meet requirement TSG22_R3_SVC_01, then terminals SHALL support SWu to connect to the ePDG.
TSG22_R3_SVC_03	VOID

10.2 Support of PDN Connections

If the terminals support either IMS based voice or SMS or video services, (or any combination), then the terminal must support the PDN connections described in this section.

The terminal needs to be able to support PDN connections, ePDG and P-CSCF discovery, as defined in GSMA PRD IR.51 clauses 4.7 and 4.9 respectively.

10.2.1 Multiple PDN connections

The terminal must support multiple PDN connections, see GSMA PRD IR.51 clause 4.5. For APN considerations of SIP signalling and XCAP see GSMA PRD IR.51 clause 4.6.

NOTE: For Multi Access PDN Connectivity (MAPCON), see clause 6.5 in GSMA PRD IR.61.

Req ID	Requirement
TSG22_R3_SVC_04	Terminals SHALL support multiple PDN connections.
TSG22_R3_SVC_05	Terminals SHALL be able to select an ePDG dynamically, as specified in 3GPP TS 23.402 clause 4.5.4.
TSG22_R3_SVC_06	Terminals SHALL support being configured with static ePDG IP addresses.
TSG22_R3_SVC_07	Terminals SHALL support the procedures for P-CSCF discovery via EPC via WLAN, as described in 3GPP TS 24.229, Annex R.2.2.1 option III.
TSG22_R3_SVC_08	Terminal MAY use 3GPP TS 24.229, Annex R.2.2.1 option I, If no P-CSCF contact information is available from configuration.

10.3 Support of IMS Profile for Voice, Video and SMS over Wi-Fi

If the terminals support either IMS based voice or SMS or video services, (or any combination thereof), then the terminals shall support the profiles defined in GSMA PRD IR 51 (IMS Profile for Voice, Video and SMS over Wi-Fi).

Req ID	Requirement
TSG22_R3_SVC_09	Terminals SHALL support the profiles defined in PRD IR 51 (IMS Profile for Voice, Video and SMS over Wi-Fi).

10.4 Wi-Fi Calling/VoWiFi

Wi-Fi calling/VoWiFi is a service that is now deployed by numerous mobile operators to extend the service reach for their customers. In order to provide a similar experience and service availability across as many WLAN as possible, a minimum set of requirements for the terminals has been created. WBA created these requirements in its WBA Wi-Fi Calling

document [WBA Wi-Fi Calling – Opportunities and Challenges towards 5G] so WLAN operators can also ensure their networks support the Wi-Fi calling service for their users.

These requirements do not include over the top voice services installed as non-operator applications on “smartphone” terminals.

Wi-Fi calling and VoLTE can be complimentary and it is possible for operators to provide service continuity to its customers whilst they switch between these network types using the native voice services on their terminals.

However there are still some limitations to Wi-Fi calling including the support of emergency calling, these limitations are being examined by standardisation bodies including the IEEE.

The set of requirements are listed below:

Req ID	Requirement
TSG22_R6_SVC_10	Terminals SHALL be capable of providing a single and integrated user interface for any mobile service that is delivered over both cellular and Wi-Fi access networks.
TSG22_R6_SVC_11	Terminals SHALL provide a UI that enables the user to change the Wi-Fi Calling settings (e.g., to change the Wi-Fi vs. Cellular preferred setting, or to enable/disable Wi-Fi Calling). Note, disabling Wi-Fi Calling functionality changes the connection setting of the terminal to Cellular only mode.
TSG22_R6_SVC_12	Terminals SHALL enable Wi-Fi Calling by default when the terminal first boots up and no user preferences have been set.
TSG22_R6_SVC_13	Terminals SHALL allow users to select one of the calling options: Wi-Fi only (e.g., when international roaming), Wi-Fi preferred, cellular preferred and cellular only.
TSG22_R6_SVC_14	Terminals SHALL use Wi-Fi preferred profile by default when Wi-Fi Calling is enabled
TSG22_R6_SVC_15	When Wi-Fi preferred is enabled by the user (and Wi-Fi preferred is allowed by the provider policy) and the terminal is within range of an available Wi-Fi network, the terminal SHALL access Wi-Fi Calling services irrespective of availability of the cellular network.
TSG22_R6_SVC_16	When Wi-Fi preferred is enabled and no Wi-Fi network is available, the terminal SHALL use the cellular network (if available) for all services while continuing to monitor for Wi-Fi.
TSG22_R6_SVC_17	When Wi-Fi only is enabled (i.e. don’t use Cellular), the terminal SHALL switch off the cellular radio and it SHALL access Wi-Fi Calling services when Wi-Fi is available.
TSG22_R6_SVC_18	When Wi-Fi only is enabled (i.e. don’t use Cellular), the terminal SHALL route all non IMS data traffic over Wi-Fi.
TSG22_R6_SVC_19	When Wi-Fi only is enabled (i.e. don’t use Cellular), and if no qualified Wi-Fi networks are available, the terminal SHALL not try to scan/enable/connect

Req ID	Requirement
	to the cellular network.
TSG22_R6_SVC_20	If Wi-Fi Calling is disabled while Wi-Fi only is enabled, then the Wi-Fi only behaviour SHALL no longer apply (i.e., the terminal can use cellular access to support voice calling).
TSG22_R6_SVC_21	When cellular preferred is enabled, the terminal SHALL select an available cellular network for access to calling services when both cellular and Wi-Fi are available.
TSG22_R6_SVC_22	When cellular preferred is enabled and a cellular network is not available or cellular coverage is poor, the terminal SHALL access Wi-Fi Calling services over an available Wi-Fi network.
TSG22_R6_SVC_23	When cellular preferred is enabled, the terminal SHALL not try to handover active Wi-Fi Calling sessions from cellular to Wi-Fi when good cellular coverage is available.
TSG22_R6_SVC_24	When cellular preferred is enabled, the terminal SHALL seamlessly handover active Wi-Fi Calling sessions from cellular to Wi-Fi if cellular coverage becomes poor.
TSG22_R6_SVC_25	When cellular only is enabled, the terminal SHALL access all Wi-Fi Calling services (e.g., voice, video, text) over cellular. The terminal SHALL provide data services (e.g., internet browsing) over available Wi-Fi. For example, when cellular-only is enabled, and there is no cellular coverage or poor cellular coverage, the terminal will behave as if there were no Wi-Fi Calling; i.e., it will always attempt to use cellular for Wi-Fi Calling services, and it will not attempt to provide mobile voice and text over Wi-Fi after connecting to Wi-Fi.
TSG22_R6_SVC_26	Terminals SHALL provide a user-friendly UI for initiating emergency calls.
TSG22_R6_SVC_27	Terminals SHALL support initiating a Wi-Fi Calling call from the phone's native dialer, contact list, and call logs.
TSG22_R6_SVC_28	Terminals SHALL support receiving a Wi-Fi Calling call using the phone's native interface.
TSG22_R6_SVC_29	Terminals SHALL support Wi-Fi Calling messaging services from the phone's native SMS/MMS application.
TSG22_R6_SVC_30	Terminals SHALL support user browsing of Internet and checking emails and other data connection activities while active in a Wi-Fi Calling call.
TSG22_R6_SVC_31	When the user changes the terminal's Wi-Fi Calling setting from "disabled" to "enabled", the terminal SHALL select an access network based on network availability and network preference settings, and register with the IMS over that access network.
TSG22_R6_SVC_32	When the user changes the terminal's Wi-Fi Calling setting from "enabled" to "disabled", the terminal SHALL de-register with the home IMS.
TSG22_R6_SVC_33	When the terminal is set to Airplane mode and the Wi-Fi is enabled with connectivity, the terminal MAY attempt to register for Wi-Fi Calling based on the operator's policy.
TSG22_R6_SVC_34	If the terminal is in airplane mode and the user enables Wi-Fi, the terminal SHALL follow the connection preferences set in determining connection.

Req ID	Requirement
	The preferences shall not be changed automatically.
TSG22_R6_SVC_35	If the terminal is in airplane mode and Wi-Fi Calling is set to cellular preferred mode and the Wi-Fi is enabled, the terminal SHALL register for Wi-Fi Calling but shall not attempt to search for cellular coverage.
TSG22_R6_SVC_36	While in airplane mode with Wi-Fi enabled (i.e., cellular radio is disabled), the terminal SHALL attempt to access emergency services over Wi-Fi.
TSG22_R6_SVC_37	If the terminal is registered for Wi-Fi Calling and the user disables airplane mode, the IMS registration SHALL be maintained.
TSG22_R6_SVC_38	If the terminal detects a handover trigger during a voice call that is established over Wi-Fi (e.g., low RSSI level), and there are no alternate cellular or Wi-Fi networks available, then the terminal SHALL generate a two tone beep alerting user that the call might drop.
TSG22_R6_SVC_39	Terminals SHALL select either cellular or Wi-Fi access for emergency calls, based on operator policy configured in the terminal or conveyed to the terminal at network attachment time.
TSG22_R6_SVC_40	Terminals SHALL establish emergency calls over an available Wi-Fi network if no cellular network is available.
TSG22_R6_SVC_41	When the terminal is on a Wi-Fi call, the Wi-Fi Calling icon SHALL indicate that the call is on Wi-Fi.
TSG22_R6_SVC_42	If the user attempts to initiate a call while Wi-Fi Calling is disabled, and there is no cellular coverage, then the terminal SHOULD pop up a message that reminds the user to enable Wi-Fi Calling in order to make calls.
TSG22_R6_SVC_43	Terminals SHALL have a capability to update or modify Wi-Fi calling IMS settings based on the SIM Card insert. This allows a user to change MNO or to pass their terminal to a different user who will have an open market-like terminal.

Annex A Document Management

Document History

Version	Date	Brief Description of Change	Approval Authority	Editor / Company
1.0	14 May 2012	Submitted to DAG and EMC for approval, final approval date 7th June 2012	EMC	William S. Yu, Smart Communications Francis A. Tuazon, Smart Communications
1.1	13 October 2012	Addition of agreed, and agreed with minimum changes for version 2 Change Requests (CRs) from October 2012	TSG/PSMC	Stephen McCann, Research in Motion Ellen H. Encinares, Smart Communications
2.0	4 July 2013	Addition of agreed change requests for version 2 from November 2012 – May 2013	TSG/PSMC	John Nickalls, NEC Stephen McCann, Research in Motion Ellen H. Encinares, Smart Communications Carolyn Heide, Ruckus
3.0	21 July 2014	All CRs agreed at previous meetings incorporated The updates within Version 3.0 cover the following topics: • Alignment with Wi-Fi Alliance certification programmes • Policy provisioning • Connection management • Network discovery • Radio Link and Quality • IPv6 support • Security • Flight mode access • IMS Services	TSG	Carolyn Heide, Ruckus, Stephen McCann, BlackBerry
4.0	22 Sept 2015	CRs agreed since v3.0: • VoWiFi • Rel 12 3GPP – WLAN interworking • Alignment of 3GPP Rel 12 with Wi-Fi Alliance Passpoint • EAP-SIM updates	TSG	Dennis Yocum, Intel Stephen McCann, BlackBerry
5.0	6 April 2016	CRs agreed since V4.0	TSG	Stephen McCann, BlackBerry

		• IMS Services • IEEE 802.11 technology and Wi-Fi Alliance updates		
6.0	4th Dec 2018	CRs agreed since V5.0 • Annex A removal • Editorial updates • Wi-Fi Calling • EAP-method error handling	TSG#34	Stephen McCann, BlackBerry

Other Information

It is our intention to provide a quality product for your use. If you find any errors or omissions, please contact us with your comments. You may notify us at prd@gsma.com your comments or suggestions & questions are always welcome.