Recommendations for Minimal Wi-Fi Capabilities of Terminals

Version 2.0

20 September 2013

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

Security Classification: Non-confidential

Access to and distribution of this document is restricted to the persons permitted by the security classification. This document is confidential to the Association and is subject to copyright protection. This document is to be used only for the purposes for which it has been supplied and information contained in it must not be disclosed or in any other way made available, in whole or in part, to persons other than those permitted under the security classification without the prior written approval of the Association.

Copyright Notice

Copyright © 2013 GSM Association

Disclaimer

The GSM Association ("Association") makes no representation, warranty or undertaking (express or implied) with respect to and does not accept any responsibility for, and hereby disclaims liability for the accuracy or completeness or timeliness of the information contained in this document. The information contained in this document may be subject to change without prior notice.

Antitrust Notice

The information contain herein is in full compliance with the GSM Association's antitrust compliance policy.

Table of Contents

1 Introduction

1.1 Purpose

Wi-Fi or *Wireless Fidelity* has been steadily increasing as a standard feature for radio access in mobile devices (terminals). "Wi-Fi" is a trademark of the Wi-Fi Alliance and the brand name for products using WFA programs based on the IEEE 802.11 family of standards.

However, these terminals have 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 and to create a Permanent Reference Document, as well as inputs to other organisations. 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.

1.2 Scope and Objective

The aim of this document is to consolidate minimum terminal requirements (or references where these have been published already by other groups) for WLAN enabled terminals. It is the intent of this Permanent Reference Document 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
CMN	Cellular Mobile Network
EAP	Extensible Authentication Protocol
EAPoL	Extensible Authentication Protocol over LAN
EDGE	Enhanced Data rates for GSM Evolution
GAN	Generic Access Network
GAS	Generic Advertisement Service
GPRS	General Packet Radio Service

GSM	Global System for Mobile
Hotspot 2.0	Wi-Fi Alliance programme that certifies Passpoint devices
HSPA	High Speed Packet Access
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
I-WLAN	Interworking Wireless LAN
LAN	Local Area Network
LTE	Long Term Evolution
MAC	Media Access Control
MAPIM	Multi Access PDN connectivity and IP flow Mobility
MMS	Multi Media Service
MNSP	3GPP PLMN Service Provider (Also called as an Operator)
OMA	Open Mobile Alliance
Passpoint™	Wi-Fi CERTIFIED Passpoint™
PLMN	Public Land Mobile Network
PMF	Protected Management Frame
QoS	Quality of Service
RADIUS	Remote Authentication Dial In User Service
SIM	Subscriber Identity Module
SCOMO	Software Component Management Object
SMS	Short Message Service
SSID	Service Set Identifier
UICC	Universal Integrated Circuit card
UMA	Unlicensed Mobile Access
UMTS	Universal Mobile Telecommunications System
WEP	Wired Equivalent Privacy
WFA	Wi-Fi Alliance
Wi-Fi	WLAN products which are Wi-Fi Alliance certified
WiMAX	Worldwide Interoperability for Microwave Access
WISP	Wireless Internet Service Provider
WISPr	Wireless Internet Service Provider roaming
WLAN	Wireless Local Area Network
WPA2	Wi-Fi Protected Access Version 2
WPS	Wi-Fi Protected Setup

1.4 Reference Documents

Document Number	Title
Wi-Fi Offload	Wi-Fi Offload Whitepaper Version 1.0 19 April 2010

	Source: www.gsma.com/go/download/?file=wifioffloadwhitepaper.pdf
Passpoint	Wi-Fi Alliance Marketing Requirements Document for Hotspot 2.0: Wi-Fi CERTIFIED Passpoint™ Certification Amendment
Wi-Fi Alliance Certification Programs,	Wi-Fi Alliance Certification Programs, see http://www.wi-fi.org/certification/programs
Wi-Fi Direct	WFA, Wi-Fi CERTIFIED Wi-Fi Direct™: Personal, portable Wi-Fi® technology (2010), https://www.wi-fi.org/register.php?file=wp_Wi-Fi_Direct_20101025_Industry.pdf
OpenCMAPI	Open CM API Requirements Document Release 1.0 – OMA-RD-OpenCMAPI-V1_0-20110712-C.doc / 12, Jul 11 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 24.234-910	3rd Generation Partnership Project; Technical Specification Group Core Network and Terminals; 3GPP System to Wireless Local Area Network (WLAN) Interworking; WLAN User Equipment (WLAN UE) to network protocols; Stage 4 (Release 9) Source: http://www.quintillion.co.jp/3GPP/Specs/24234-910.pdf
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 44.318	Generic Access Network (GAN); Mobile GAN Interface Layer 3 Specification Source: http://www.3gpp.org/ftp/Specs/html-info/44318.htm
3GPP TS 33.234	3rd Generation Partnership Project; Technical Specification Group Services and System Aspects;3G Security;Wireless Local Area Network (WLAN) interworking security
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
IEEE 802.11-2012	IEEE 802.11-2012, Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications.
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://tools.ietf.org/pdf/rfc2460.pdf

RFC 3736	Stateless Dynamic Host Configuration Protocol (DHCP) Service for IPv6 Source: http://tools.ietf.org/html/rfc3736
RFC 3748	Extensible Authentication Protocol (EAP) Source: http://tools.ietf.org/pdf/rfc3748.pdf
RFC 4026	Provider Provisioned Virtual Private Network (VPN) Terminology Source: http://tools.ietf.org/pdf/rfc4026.pdf
RFC 4186	Extensible Authentication Protocol Method for Global System for Mobile Communications (GSM) Subscriber Identity Modules (EAP-SIM) Source: http://tools.ietf.org/pdf/rfc4186.pdf
RFC 4187	Extensible Authentication Protocol Method for 3rd Generation Authentication and Key Agreement (EAP-AKA) Source: http://tools.ietf.org/pdf/rfc4187.pdf
RFC 4443	Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Source: http://tools.ietf.org/html/rfc4443
RFC 4861	Neighbor Discovery for IP version 6 (IPv6) Source: http://tools.ietf.org/html/rfc4861
RFC 4862	IPv6 Stateless Address Autoconfiguration Source: http://tools.ietf.org/html/rfc4862
RFC 4941	Privacy Extensions for Stateless Address Autoconfiguration in IPv6 Source: http://tools.ietf.org/html/rfc4941
RFC 5175	IPv6 Router Advertisement Flags Option Source: http://tools.ietf.org/html/rfc5175
RFC 5247	Extensible Authentication Protocol (EAP) Key Management Framework Source: http://tools.ietf.org/pdf/rfc5247.pdf
RFC 5448	Improved Extensible Authentication Protocol Method for 3rd Generation Authentication and Key Agreement (EAP-AKA') Source: http://tools.ietf.org/pdf/rfc5448.pdf
RFC 6106	IPv6 Router Advertisement Options for DNS Configuration Source: http://tools.ietf.org/html/rfc6106

2 Alignment with Wi-Fi Alliance Certification Programmes

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

2.1 Wi-Fi Alliance Certification Programmes

Terminals are 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.

Terminals should be IEEE 802.11n capable. The majority of smartphones certified by the WFA in the first half of 2012 were certified for IEEE 802.11n. IEEE 802.11n provides higher throughput, and since the radio channel is shared by the Access Point and terminals, the channel capacity improves for all devices.

Terminals shall be Wi-Fi CERTIFIED Passpoint™ [Passpoint]. Passpoint certifies that products implement the technology defined in the Wi-Fi Alliance Hotspot 2.0 Release 1 Technical Specification. This technology enables mobile devices to automatically discover and connect to WLANs, and automatically configures industry-standard WPA2™ security protections without user intervention. Passpoint certification also requires WFA baseline certification as a pre-requisite.

For terminals which are IEEE 802.11n capable, the WFA baseline certification requires terminals to be Wi-Fi CERTIFIED n. In addition, the IEEE 802.11n certification includes WPA2™ (Wi-Fi Protected Access 2) and Wi-Fi Multimedia (WMM) testing.

WPA2™ testing and certification provides WLAN network security - offering government-grade security mechanisms for personal, enterprise and hotspot deployments. The WMM certification provides support for multimedia content over WLAN networks enabling WLAN 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 terminals which are not IEEE 802.11n capable, the WFA baseline consists of two 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.

Terminals need to 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 terminal. Without PMF, this attack could cause the victim terminal, for example, to disassociate from a WLAN network, tear down a QoS flow, etc.

Terminals should support IEEE 802.11r, Fast Transition, in order to significantly reduce the load on a Mobile Network Service Providers (MNSP)'s HLR/HSS. Note that terminals using WPA2-Enterprise with EAP-SIM, EAP-AKA or EAP-AKA' authenticate with their home AAA server *every* time the mobile transitions from one AP to another within the same WLAN network. Terminals using IEEE 802.11r authenticate to their home AAA server only on the first authentication with the WLAN network; all subsequent authentications are handled locally. Example deployments where the use of IEEE 802.11r can dramatically reduce the load on the MNSP's HLR/HSS include high density environments (e.g., sporting venue, train station) or Community WLAN networks (e.g., a user walking down a street would connect to AP after AP in sequence).

Terminals should also support IEEE 802.11k, Radio Resource Measurement. IEEE 802.11k features provide network operators greater capability to manage WLAN to WLAN interference, improve roaming, etc.

The WFA has included certification of IEEE 802.11r and IEEE 802.11k 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 IEEE 802.11r and IEEE 802.11k.

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

Terminals 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 terminal. 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	Terminals SHOULD be IEEE 802.11n capable.
TSG22_R2_WFA_02	Terminals SHALL be Wi-Fi CERTIFIED WPA2™ with Protected Management Frames.
TSG22_R2_WFA_03	Terminals SHALL be Wi-Fi CERTIFIED Passpoint™.
TSG22_R2_WFA_04	Terminals SHOULD be Wi-Fi CERTIFIED Voice-Enterprise.
TSG22_R2_WFA_05	Terminals SHOULD be Wi-Fi CERTIFIED WMM-Power Save.
TSG22_R2_WFA_06	Terminals SHALL 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 WLAN client devices that connect 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 (see www.wi-fi.org/wi-fi_direct.php)

Mobile phones, cameras, printers, PCs, and gaming devices can connect to each other directly to transfer content and share applications quickly and easily. Devices can make a one-to-one connection, or a group of several devices can connect simultaneously. Connecting Wi-Fi Direct devices is easy and simple, in many cases only requiring the push of a button. Moreover, all Wi-Fi Direct™ connections are protected by WPA2™, the latest Wi-Fi security technology. With Wi-Fi Direct™, an AP or internet connection are not required.

Req ID	Requirement
TSG22_R2_WFA_07	Terminals SHOULD support the Wi-Fi Direct™ certification program.

2.3 Supported 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, terminals should support using the 5GHz band.

Req ID	Requirement
TSG22_R2_USE_1	Terminals SHOULD be able to operate in the 2.4GHz band.
TSG22_R2_USE_2	Terminals SHOULD be able to operate in the 5GHz band.

3 WLAN Policy Provisioning

3.1 Operator Policy Provisioning

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 terminal, either through the cellular network or directly over the WLAN access network.

Some operators may also opt to pre-configure operator-controlled APs into terminals.

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

3GPP has, in addition, defined a set of WLAN parameters provisioned into the USIM (see 3GPP TS 31.102) to be used by the terminal. In addition, 3GPP has also defined OTA (Over The Air) mechanisms in order to update the USIM parameters including the WLAN parameters (see 3GPP TS 31.115 and 3GPP TS 31.116).

Req ID	Requirement
TSG22_R2_CM_01	Terminals SHALL support provisioning of WLAN parameters (e.g. network identifiers) using the USIM as specified in 3GPP TS 31.102 and in 3GPP TS 24.234.
TSG22_R2_CM_02	Terminals SHOULD support OMA DM Managed Objects

3.2 User/Manual Provisioning

In most terminals 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 the terminal is in range of an existing WLAN hotspot setup, the connection is automatic.

Req ID	Requirement
TSG22_R2_CM_03	Terminals 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 the terminal, they SHALL be stored in the USIM if the corresponding files are available, otherwise in the terminal.

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 terminals 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 network connections based on the terminal status, connection conditions, operator policies and user profiles associated with these connections.

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

- Turn on and turn off the WLAN (including support of flight mode, where flight mode means that electronic devices SHALL have 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	Terminals SHALL have at least one pre-installed connection management client.
TSG22_R2_CM_06	Terminals SHOULD have programming interfaces/APIs to control and/or manage WLAN connection.
TSG22_R2_CM_07	The pre-installed connection management client on the terminal SHOULD be based on the API offered.
TSG22_R2_CM_08	Terminals SHOULD offer API fully compliant with the OMA [OpenCMAPI] on WLAN management.
TSG22_R2_CM_09	Terminals SHALL support a mechanism that can automatically stop the search for available WLAN access network for the following reasons: – Flight mode enabled – Low battery capacity Terminals have established a connection with an AP

4.2 Network Discovery

Constant scanning for detection of a hotspot may place a heavy toll on the battery life of a Smartphone. Terminals 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	Terminals 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	Terminals SHALL support a WLAN network discovery mechanism that preserves battery life.
TSG22_R2_CM_12	Terminals SHOULD be able to listen & report events to an upper layer (e.g. UI) such as new available network, loss of network.

4.3 WLAN Radio Link and Connection Quality

On most terminal devices, once WLAN is detected, the terminal 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.

Terminals should consider information on AP air interface loading (e.g. BSS load information which may be advertised in beacons), information on backhaul status of a AP (e.g. Passpoint™ WAN metrics information which may be obtained via a ANQP query) and information on radio conditions (e.g. received RSSI level of AP and interference conditions) to avoid connection to a 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 terminal and should include at least a minimum RSSI level, a maximum channel utilisation value for air

interface loading (as defined by BSS load information in IEEE 802.11) and a minimum backhaul bandwidth threshold. The available backhaul bandwidth may be derived from information received in Passpoint™ WAN metrics Information element. These criteria may also be preconfigured by the operator in the terminal 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 terminal may in addition have proprietary schemes to consider additional parameters in order to determine whether the AP is adequate or not.

Once a terminal is connected on a WLAN network it should be able to monitor whether the AP can 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) and switch back to the cellular network if the minimum throughput threshold cannot be satisfied.

Req ID	Requirement
TSG22_R2_CM_13	Terminals SHALL have the capability to monitor the Wi-Fi radio link quality in terms of WLAN Received Signal Strength Indication (RSSI) level.
TSG22_R2_CM_14	Terminals 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 RSSI - IEEE 802.11 BSS load IE - Passpoint™ WAN Metrics IE
TSG22_R2_CM_15	Terminals SHOULD be able to monitor the data throughput level on a selected AP.
TSG22_R2_CM_16	Terminals SHOULD consider the WLAN RSSI and data throughput level on a selected AP when evaluating whether to switch back to the 3GPP network based on default priorities and/or thresholds for those parameters specified by the manufacturer.
TSG22_R2_CM_17	Terminals MAY support provisioning with priorities and/or thresholds related to RSSI, BSS load information, Passpoint™ WAN metrics information and minimum WLAN data throughput level e.g. pre-configured or as part of operator policies.
TSG22_R2_CM_18	Terminals SHOULD use provisioned priorities and /or thresholds by the operator, when present, with higher priority than default manufacturer priorities/thresholds.

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 between 3GPP access (2G/3G/LTE) and WLAN may present usability problems to the terminal which is not properly configured to handle such scenarios.

Hysteresis (meaning that the threshold to switch to a WLAN network is different from the threshold to switch back to a cellular network) mechanisms should be implemented with tuned radio thresholds, so that a terminal switches back quickly to 3GPP access , when the WLAN radio signal strength is fading or throughput is decreased to an unacceptable level.

If no cellular network is available (and the WLAN signal is below the access threshold), WLAN access has to be released.

The network is able to temporarily refuse a WLAN connection, so that the terminal will stay on the cellular network.

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

Req ID	Requirement
TSG22_R2_CM_19	Terminals SHALL have a hysteresis mechanism to prevent them from connecting and disconnecting to/from the same AP within a minimum interval.
TSG22_R2_CM_20	The terminal SHALL limit the number of access retries to the same AP when it receives temporary denied access notification from that AP. (as e.g. RFC 4186 1026 notification with EAPSIM)

4.5 WLAN Access Network Selection

WLAN network selection in the terminal, i.e. based on (U)SIM credentials provided by the 3GPP network operator should take into consideration 3GPP operator policies for WLAN network selection. The operator policies may indicate priority among WLAN networks e.g. based on a pre-configured list of network identifiers or provisioned by the cellular network operator. The cellular network operator policies should have highest priority among all available policies in the terminal for network selection. However, user preference settings should be able to override 3GPP operator policies on WLAN selection.

Terminals should be able to support association on a preferred WLAN network, whether the network identifier is visible or not. Moreover, in order to avoid selection of a WLAN network with poor radio link and/or data connection quality, terminals should evaluate whether a WLAN network is suitable, according to the requirements of Section 4.3 of this PRD. The criteria for determining whether a WLAN network is suitable can be default criteria in the terminals, criteria pre-configured by the operator or provisioned as part of operator policies for WLAN network selection.

In the presence of more than one suitable WLAN network, terminals should select the one prioritised by the cellular operator policy (unless overridden by user preference settings). Terminals should also prefer a WLAN network that is suitable over one that is not suitable, when both networks are allowed by cellular operator policy (even though the WLAN network that is not suitable may be prioritised by the policy).

Req ID	Requirement

TSG22_R2_CM_21	Terminals SHOULD consider user preference settings with highest priority when evaluating inputs for WLAN access technology selection.
TSG22_R2_CM_22	Amongst policies for WLAN network selection within terminal memory, terminals SHOULD consider policies received from the cellular network operator with highest priority (unless overridden by user preference settings).
TSG22_R2_CM_23	Terminals SHALL be able to support the association on a Network Identifier, visible or not.

Note: This version of the specification does not consider the output of the 3GPP Release 12 WLAN Network Selection work item.

4.6 Managing Radio Connections based on Multiple Access Technologies

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

The cellular network operator may provide the terminal with policies (can be subscription specific policies) that indicate, for example, the preferred access technology (e.g. 3GPP cellular vs. WLAN) to use under specific conditions, priority among WLAN networks or how traffic should be distributed between the 3GPP cellular and WLAN access. 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 24.312.

Terminals should adhere to policies received from the cellular network e.g. priority among WLAN networks or between cellular 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 network that is not suitable. The terminal should evaluate whether a WLAN network is suitable according to the principles in Section 4.3 of this PRD. Thus, in presence of more than one suitable WLAN network, terminals should select the one prioritised by the cellular operator policy (unless overridden by user preference settings). Terminals should also prefer a WLAN network that is suitable over one that is not suitable, when both networks are allowed by cellular operator policy (even though the WLAN network that is not suitable may be prioritised by the policy).

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

Req ID	Requirement
TSG22_R2_CM_24	Terminals SHOULD be able to off-load a data flow from 3GPP cellular to WLAN (and vice versa).
TSG22_R2_CM_25	Terminals SHOULD be able to maintain concurrent 3GPP cellular and WLAN connectivity for distributing separate data flows on 3GPP cellular and WLAN.
TSG22_R2_CM_26	Terminals SHOULD consider user preference setting with highest priority when evaluating inputs for multi-access technology selection.
TSG22_R2_CM_27	The hierarchy of the inputs used by the terminal to select the appropriate radio connection for data flows (after user preferences) SHOULD be the following: 1) The policies received from the cellular network operator e.g. ANDSF policies. 2) Information pertaining to the suitability of the selected and/or available radio connection. 3) Information pertaining to the status of the terminal.

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 WLAN access has been performed 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 mechanism keeps 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 hotspot. In this case, the IP layer connectivity stays the same (layer 2 handover only).

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

3. Switch to an AP of a different network, 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 the terminals AP changes, the DHCP function of the terminal 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 proposes to cache information about the network (own IP configuration parameters, MAC and IPs 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 the device retains information about multiple networks, it can also accelerate the return to your private networks. It also helps if the device switches back and forth between two hotspots for some reason.

It is important that it becomes normal practice for all terminals to support IPv6 on their Wi-Fi interface.

In order to improve the IP address utilisation, the terminal shall send DHCP Release message to 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
    1.

Req ID	Requirement
TSG22_R2_CM_28	Terminals SHALL support IPV6 (RFC 2460).
TSG22_R2_CM_29	Terminals SHALL support the ICMPv6 protocol (IETF RFC 4443)
TSG22_R2_CM_30	Terminals SHALL support the Neighbour Discovery Protocol (IETF RFC 4861)
TSG22_R2_CM_31	Terminals SHALL support Stateless Address Auto Configuration (SLAAC, IETF RFC 4862)
TSG22_R2_CM_32	Terminals SHALL support the Privacy Extensions for Stateless Address Autoconfiguration in IPv6 (IETF RFC 4941)
TSG22_R2_CM_33	Terminal SHOULD support (stateless) DHCPv6 client (RFC 3736)
TSG22_R2_CM_34	Terminal SHOULD support Router Advertisement Option for DNS configuration (RFC 6106)
TSG22_R2_CM_35	Terminal SHOULD support IPv6 Router Advertisement Flags Options ([RFC 5175])
TSG22_R2_CM_36	Terminals SHOULD be able to perform Path MTU Discovery according to RFC 1981
TSG22_R2_CM_37	The terminal browser SHALL support IPv6, both for standard HTTP access and standard access with a proxy configuration
TSG22_R2_CM_38	Terminals MAY use DHCPV6 for the IP address assignment.

TSG22_R2_CM_39	Terminals SHOULD be able to use concurrent WLAN and cellular mobile network access for data services.
TSG22_R2_CM_40	Terminal SHALL keep the 3GPP mobile network connection e.g. PDP contexts during WLAN access.
TSG22_R2_CM_41	The terminal SHALL send DHCP Release message to 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	Terminals SHOULD implement the IETF RFC 4436 - Detecting Network Attachment in IPv4 (DNAv4). 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.

5 Security

5.1 Authentication Protocols

5.1.1 EAP-SIM/EAP-AKA/EAP-AKA'

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 networks. GSMA member operators require that (U)SIM based authentication shall be used by a terminal with (U)SIM to authenticate on a WLAN 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 (U)SIM based terminals 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™.

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, terminals 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. More specifically, a terminal with either a USIM or a SIM inserted shall request the authentication method corresponding to the type of smart card it holds when connecting to a WLAN network that has a roaming agreement (either direct or via a VPLMN) with the HPLMN of the (U)SIM. In addition, it shall be possible to configure whether the terminal, with UICC inserted and USIM selected, shall use EAP-AKA or EAP-AKA' when accessing operator WLANnetworks that has a roaming agreement (either direct or via a VPLMN) with the HPLMN of the USIM. In order to cover the case where the HPLMN AAA server does not yet support EAP-AKA, it shall be possible for the operator to configure whether terminals, with UICC inserted and USIM selected, are allowed to use EAP-SIM when connecting to a WLANnetwork that has a roaming agreement (either direct or via a VPLMN) with the HPLMN of the USIM.

Req ID	Requirement
TSG22_R2_SEC_01	Terminals SHALL support EAP-SIM, EAP-AKA and EAP-AKA'.
TSG22_R2_SEC_02	Terminals with SIM inserted and activated SHALL use EAP-SIM to authenticate with a WLAN network that has a roaming agreement (either direct or via a VPLMN) with the HPLMN of the SIM.
TSG22_R2_SEC_03	Terminals with UICC inserted and USIM selected SHALL by default use either EAP-AKA or EAP-AKA' to authenticate with a WLAN network 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 terminals, with USIM inserted and USIM selected, are allowed to use EAP-SIM (when supported by the USIM) when connecting to a WLANnetwork 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.
TSG22_R2_SEC_05	It SHALL be possible for the operator to configure whether terminals with USIM inserted shall use EAP-AKA or EAP-AKA' when connecting to a WLAN network 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.

5.1.2 IEEE 802.1X

This is another key component of the Passpoint™ certification that aims to provide WLAN users a seamless user experience. The terminal requirement is to support IEEE 802.1X.

IEEE 802.1X is an authentication method for PNAC (port-based Network Access Control). It provides an authentication methodology often used by laptops to connect to LAN or WLAN using EAP. In WLANnetworks an AKM (Authentication and Key management) suite needs to be negotiated in order to use IEEE 802.1X for authentication. This is defined as WPA2 Enterprise certification (which is a pre-requisite for Passpoint™ Certification) which mandates the use of IEEE 802.1X authentication methodology.

Req ID	Requirement
TSG22_R2_SEC_06	Terminals SHALL support IEEE 802.1X. Note: IEEE 802.1X is supported by a terminal which is WFA Passpoint™ Certified.

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 network which has the support of an authentication server. To provide a secure means of communication for the terminals over a WLAN air interface, WPA2 Enterprise with PMF is mandatory. WFA also mandates that all Wi-Fi certified devices support 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 terminals (refer to Section 2.1 of this PRD) . .

Req ID	Requirement
TSG22_R2_SEC_07	Terminals SHOULD NOT support WEP.

5.3 Roaming Relationships and IEEE 802.11u

IEEE 802.11u can be used to advertise roaming relationships between Passpoint™ operators, similar to those mechanism used today for cellular access.

Passpoint™ will provide improved WLAN network selection and network access, including the ability to provide network access for visiting users. IEEE 802.11u is used, within Passpoint™, to improve network selection while WPA2 Enterprise (using EAP-SIM or either EAP-AKA or EAP-AKA') will provide automated connectivity and secure network access. It permits the discovery of roaming partners having SSIDs that are unknown to the terminal.

WPA2 Enterprise can be used to authenticate with the home provider for network access (assuming the home operator has a roaming relationship, with the visited operator.)

IEEE 802.11u is included in the Passpoint™ WFA certification [Passpoint].

6 Wi-Fi Protected Setup (WPS)

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 devices and services.

It is often quite challenging for the customer to gain access using their terminal to a WLAN 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 WLANnetworks at home or in a small office environment.

This certification program provides several easy-to-use methods to configure a network and the different terminals to access to 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 terminal.

Req ID	Requirement
TSG22_R2_CM_43	Terminals SHALL support WPS with either PIN or both PIN & Push-Button methods for WLAN.
TSG22_R2_CM_44	Terminals SHALL provide a Registrar capability as Client Device for WPS.
TSG22_R2_CM_45	Terminals SHALL provide a hardware or software button to trigger the WPS wireless protected Setup feature as well as a prompt to enter the PIN.

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.

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

Req ID	Requirement
TSG22_R2_USE_3	Terminals SHALL have an accessible means for toggling the WLAN to on or off.

7.2 Status Information

For better user experience, pertinent terminal 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 WAN link status, WAN uplink and downlink data rates WLAN network name or logo should be displayed when connected to Passpoint™ APs.

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

If the WLAN connection is secure (i.e. AP is Passpoint™ compliant 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 terminal associates with the AP for the first time.

Req ID	Requirement
TSG22_R2_USE_4	Terminals that have a UI (User Interface) SHALL indicate the status of the terminal connection.
TSG22_R2_USE_5	Terminals SHOULD offer programming interfaces providing Status Information to applications.
TSG22_R2_USE_6	Terminals SHOULD offer API fully compliant with the OMA [OpenCMAPI] on Status Information & notifications functions.
TSG22_R2_USE_7	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 terminals could be parameterised with automatic EAP authentication and perform automatic connection attempts to a WLAN network. If the network rejects the access request of the terminal for a repeated number of times due to WLAN barring, the

terminal must stop any other requests 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, there are peculiar 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 these reasons, where authentication frames support Fast Re-authentication procedures, these should be supported in the mobile terminal..

Req ID	Requirement
TSG22_R2_USE_8	Terminals SHALL refrain from attempting an automatic connection when barred due to permanent (and not temporarily) authentication failure or notification after the authentication request is rejected, unless a manual attempt is made. For example, with EAPSIM, according to RFC 41.86 § 10.18 , when receiving the error code 1031 - User has not subscribed to the requested service. (Implies failure, used after a successful authentication.)
TSG22_R2_USE_9	Terminals with a UI (User Interface) SHOULD notify to the user the failure of authentication.
TSG22_R2_USE_10	Terminals SHALL implement fast re-authentication mechanism described in the IETF RFC 4186 - EAP SIM.
TSG22_R2_USE_11	Terminals SHOULD support fast re-authentication mechanism described in the IETF RFC 4187 - EAP AKA/ IETF RFC 5448 - EAP AKA' .

8 Power Management

8.1 Power Save Mechanisms

Mobile devices that present poor battery longevity can present less usefulness to users, due to its mobile nature, such mobile devices can benefit from power save mechanisms.

Req ID	Requirement
TSG22_R2_USE_12	Terminals SHALL have a means of determining low battery level and automatically enabling power save mechanisms.

TSG22_R2_USE_13	Terminals SHALL have a means of notifying the user or application of low battery status.
TSG22_R2_USE_14	Terminals SHOULD make use of Wi-Fi Alliance WMM Power Save mechanisms to preserve battery life.
TSG22_R2_USE_15	Terminals SHOULD have a feature for users to toggle to battery saving mode.
TSG22_R2_USE_16	Terminals SHOULD maintain WLANnetwork connectivity while preserving battery life.

8.2 Idle Power Management

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

Req ID	Requirement
TSG22_R2_USE_17	Terminals SHOULD have a traffic inactivity duration setting that will be indicated by the manufacturer to trigger power save mechanism.
TSG22_R2_USE_18	Terminals MAY use Wi-Fi Alliance WMM Power Save mechanisms to achieve idle power management.

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 cellular 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	Terminals SHALL support a mechanism for Parental Control for access to unsuitable web content for children.
TSG22_R2_USE_20	Terminals SHOULD have their native internet browsers to support parental control.
TSG22_R2_USE_21	Terminals SHOULD restrict download of third party browsers without parental control feature
TSG22_R2_USE_22	Terminals MAY support a mechanism to lock/unlock the unlicensed radio access to the internet.

Note: There is no specification of a standard terminal assisted parental control mechanism currently available in the industry and terminal 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 terminal and/or content filtering norms for the content delivery infrastructure developed by such committees.

Annex A Future Work

WLAN as a standard feature for radio access in mobile devices (terminals) continues to evolve in features and technology.

This section provides guidance on future work; it lists topics which were raised but are not mature enough for (complete) consideration in the main body yet. These topics are expected for further assessment and consideration in future work and following versions:

A.1 Handover between 3GPP Cellular and WLAN networks

Including support for operator network policies, e.g. through use of ANDSF

A.2 WLAN Network Management and Troubleshooting

Through adoption of relevant IEEE Standards, support the gathering and use of diagnostic information, QoS statistics and radio environment measurements to quickly resolve connectivity problems, identify coverage holes in the WLAN network, improve the user experience and enable effective interference management and load balancing.

For large scale WLAN hotspot network deployments, it is important that the hotspot network administrator can collect information from the terminal that can assist with diagnosing connectivity problems, assessing user experience and improving the hotspot network coverage and capacity.

Terminals with WLAN shall be configurable to provide diagnostic information to the network e.g. configuration information as per IEEE 802.11 standards (refer to Section 4.3.13.6 of [IEEE 802.11-2012]) in order to allow the network administrator to troubleshoot connectivity problems.

Moreover, for network monitoring purposes and capacity analysis purposes, terminals shall support the following IEEE 802.11 features:

- IEEE 802.11 Event reporting (Refer to Section 10.23.2.1 of [IEEE 802.11-2012]).
- IEEE 802.11 Triggered STA statistics (Refer to Section 4.3.13.16 [IEEE 802.11-2012]).
- IEEE 802.11 Collocated interference reporting (Refer to Section 4.3.13.5 of [IEEE 802.11-2012]).
- IEEE 802.11 beacon reporting (Refer to Section 10.11.9.1 of [IEEE 802.11-2012]).
- IEEE 802.11 Link Measurement Reporting (Refer to Section 10.11.11 of [IEEE 802.11-2012]).
- IEEE 802.11 channel load measurement (Refer to Section 4.3.8.5 of [IEEE 802.11-2012]).
- IEEE 802.11 STA statistics (Refer to 4.3.8.7 of [IEEE 802.11-2012]).

Another aspect of network management is related to effective management of radio resources to minimise interference in the network, improve user experience and maximise usage of the unlicensed spectrum.

For load balancing purposes, terminals shall support the following features:

- IEEE 802.11 BSS Transition Management (Refer to Section 4.3.13.3 of [IEEE 802.11-2012])
- IEEE 802.11 Neighbour reporting (Refer to Section 4.3.8.10 of [IEEE 802.11-2012])

For interference management purposes, terminals shall support the following features:

- IEEE 802.11 Co-located Interference reporting which can be used to identify and help mitigate interference in the unlicensed bands from non-Wi-Fi transmissions (Refer to Section 4.3.13.5 of [IEEE 802.11-2012]).
- IEEE 802.11 quiet element to assess background interference (Refer to Section 8.4.2.25 of [IEEE 802.11-2012])

Availability of terminal location is also another key element for effective management of large scale networks as well as being an enabler for location based services. Terminals shall support the following feature:

- IEEE 802.11 location reporting (Refer to Section 4.3.8.8 of [IEEE 802.11-2012])

Req ID	Requirement
TSG22_R2_NM_01	Terminals SHALL support IEEE 802.11 diagnostic reporting feature (Refer to 4.3.13.6 of [IEEE 802.11-2012])
TSG22_R2_NM_02	Terminals SHALL support IEEE 802.11 Event reporting feature (Refer to Section 10.23.2.1 of [IEEE 802.11-2012]).
TSG22_R2_NM_03	Terminals SHALL support IEEE 802.11 Triggered station statistics feature (Refer to Section 4.3.13.16 [IEEE 802.11-2012]).
TSG22_R2_NM_04	Terminals SHALL support IEEE 802.11 BSS transition management feature (Refer to Section 4.3.13.3 of [IEEE 802.11-2012])
TSG22_R2_NM_05	Terminals SHALL support IEEE 802.11 Collocated Interference reporting feature (Refer to Section 4.3.13.5 of [IEEE 802.11-2012]).
TSG22_R2_NM_06	Terminals SHALL support IEEE 802.11 beacon reporting feature (Refer to Section 10.11.9.1 of [IEEE 802.11-2012]).
TSG22_R2_NM_07	Terminals SHALL support IEEE 802.11 Link Measurement Reporting feature (Refer to Section 10.11.11 of [IEEE 802.11-2012]).
TSG22_R2_NM_08	Terminals SHALL support IEEE 802.11 channel load measurement feature (Refer to Section 4.3.8.5 of [IEEE 802.11-2012]).
TSG22_R2_NM_09	Terminals SHALL support IEEE 802.11 STA statistics feature (Refer to 4.3.8.7 of [IEEE 802.11-2012]).
TSG22_R2_NM_10	Terminals SHALL support IEEE 802.11 Neighbour reporting feature (Refer to Section 4.3.8.10 of [IEEE 802.11-2012]).

TSG22_R2_NM_12	Terminals SHALL support IEEE 802.11 quiet element feature (Refer to Section 8.4.2.25 of [IEEE 802.11-2012]).
TSG22_R2_NM_13	Terminals SHALL support IEEE 802.11 location reporting (Refer to Section4.3.8.8 of [IEEE 802.11-2012]).

A.3 WLAN Antenna Performance

Ensure common antenna performances through the alignment on requirements for the Minimum Total Radiated Power (MTRP) and the Maximum Total Radiated Sensitivity (MTRS) for WLAN terminals.[1]

A.4 (Partial) Support for 3GPP TS 24.234

To facilitate the Provisioning and Storage of policies in the USIM or Terminal.

A.5 Updates driven in related standardisation bodies such as 3GPP, OMA, WFA etc.

Please note that above list should not be considered as complete or final list but is subject to market and technology developments, inputs received from work driven in related organisations and inputs provided by the members of the GSMA TSG group.

[1] Progress will also be subject to work driven by other industry groups such as the Wi-Fi Alliance Convergence Wireless Group (CWG).

Annex B Network/Connectivity Use Cases

B.1 WPA2, IEEE 802.1X (EAPOL), EAP

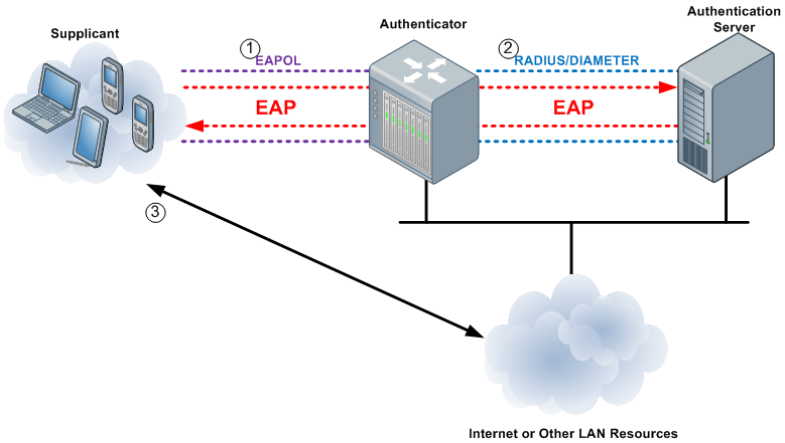

Figure 1: Example EAP Network Architecture

B.1.1 Description

Krishna is leisurely walking around the commercial district when she notices a WLAN hotspot provided by her operator. She chooses the hotspot and her device connects to it successfully. She begins to browse to her favourite websites.

B.1.2 Background

In this use case the multiple layer of security provided by WPA2, IEEE 802.1X and EAP.

B.1.3 Sequence of Events

1. User chooses to connect to the hotspot.
2. Mobile device connects and uses WPA2 to encrypt the communication channel to the hotspot.
3. EAPoL is used additionally to connect securely to the authenticator to facilitate the EAP authentication.
4. Device then authenticates using EAP and connects to the authenticator and authentication server.
5. System authenticates the device and permits the connection.

B.2 IEEE 802.11u

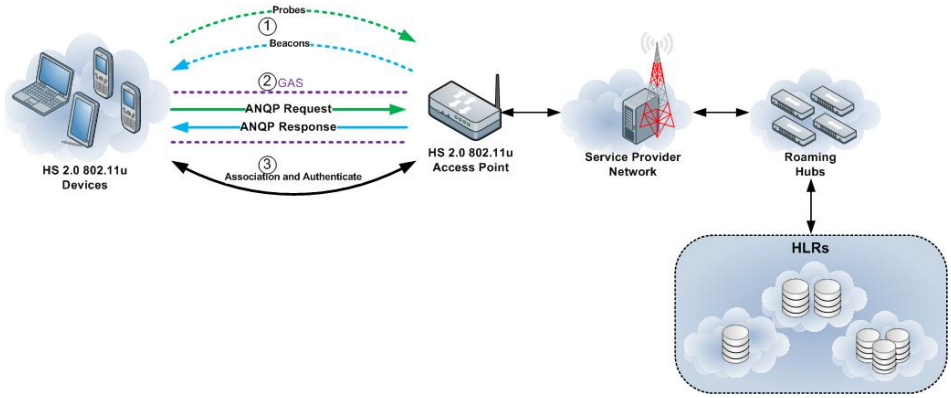

Figure 2: Example IEEE 802.11u Network Architecture

B.2.1 Description

Raymond is at a restaurant when he notices that it offers WLAN provided by his operator. His phone detects the hotspots available and proceeds to connect to the hotspot provided by his operator. The device successfully connects and the device proceeds to authenticate on the network.

B.2.2 Background

This use case attempts to show the convenience that IEEE 802.11u provides to the user when connecting to an IEEE 802.11u-enabled WLAN network. This alleviates the user from punching in security keys for WPA2 and selects the appropriate hotspot/network for the user based on provisioned network details.

B.2.3 Sequence of Events

1. Users choose to connect to WLAN.
2. Device scans for hotspots available.
3. IEEE 802.11u GAS (Generic Advertisement Service) is used to provide for Layer 2 transport of an advertisement protocol's frames between a terminal and a server in the network prior to authentication.
4. IEEE 802.11u ANQP (Access Network Query Protocol) is used to discover different features and available services of the network.
5. Device then proceeds to the authentication process.

B.3 Home (3G) Switch to Home (WLAN)

User decides to switch from 3G, which is provided by the user's home operator, to WLAN, which is also provided by the user's home operator.

B.3.1 Description

Clara is in the suburbs when she walks by a coffee shop. She notices that the place offers WLAN provided by her home network. She connects to the hotspot and starts uploading her pictures.

B.3.2 Background

This use case illustrates the process on how users/devices connect to a hotspot provided by the home operator.

B.3.3 Sequence of Events

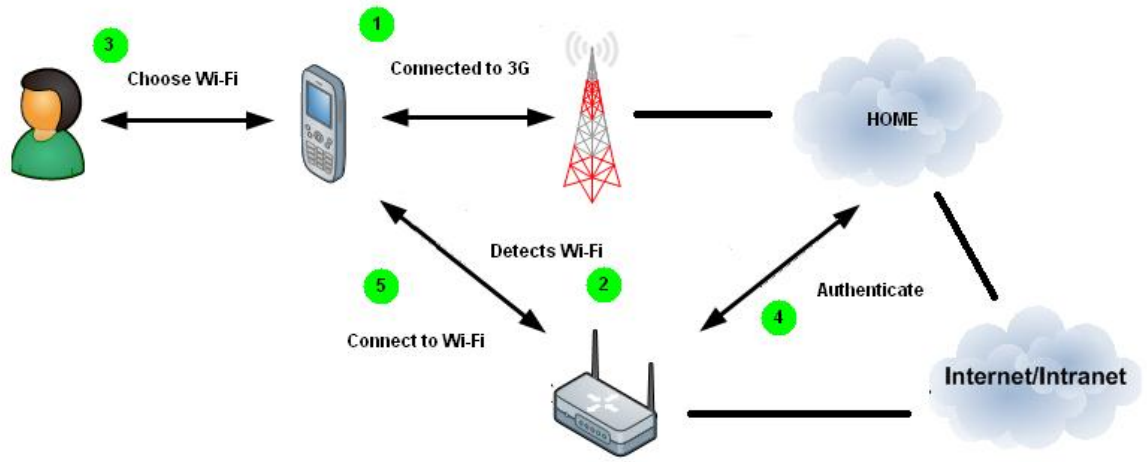

Figure 3: Example 1 - Radio Access Network Connection Switching

1. Mobile device is connected to the user's home operator network and is currently in 3G.
2. Mobile device detects a WLAN network provided by the user's home operator.
3. User decides to switch to the WLAN network.
4. Mobile device is authenticated and authorized to use the WLAN network by the home operator.
5. Mobile device is now connected to the WLAN network.

B.4 Visited (3G) to Visited (WLAN)

User decides to switch from 3G, which is provided by the visited operator, to WLAN, which is also provided by the visited operator.

B.4.1 Description

Lea arrived at the airport for a week-long vacation. Turning her phone on, the phone connects to the roaming network. Incidentally her WLAN radio is on and the device prompted her that a WLAN network is available. It is a network provided by the same visited network. She opted to connect to the WLAN and began to browse her social network account for updates.

B.4.2 Background

This use case illustrates the process on how users/devices connect to a hotspot provided by the visited operator while roaming into a visited 3G network.

B.4.3 Sequence of Events

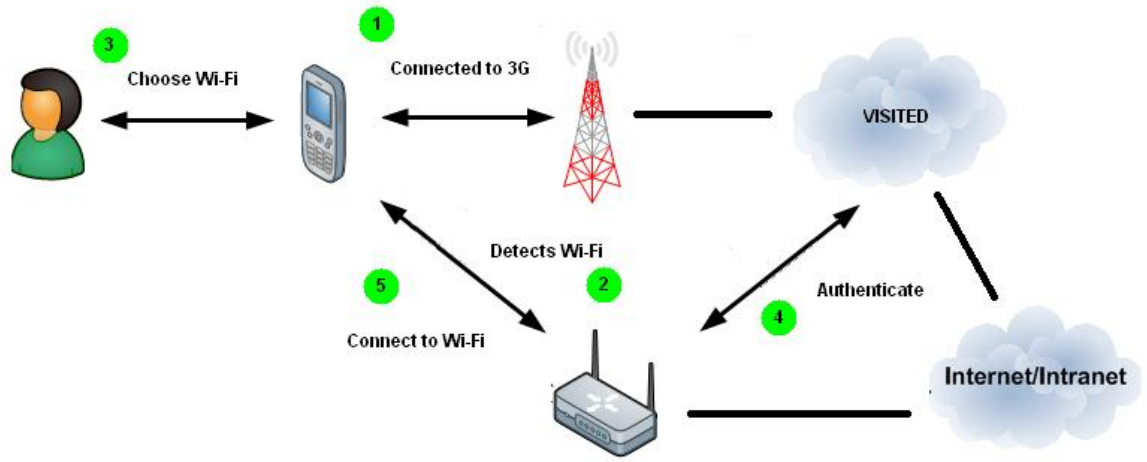

Figure 4: Example 2 - Radio Access Network Connection Switching

1. Mobile device is connected to a visited operator's network and is currently in 3G.
2. Mobile device detects a WLAN network provided by the visited operator.
3. User decides to switch to the WLAN network.
4. Mobile device is authenticated and authorized to use the WLAN network by the visited operator.
5. Mobile device is now connected to the WLAN network.

B.5 Visited (3G) to Home (WLAN)

User decides to switch from 3G, which is provided by the visited operator, to WLAN, which is provided by the user's home operator.

B.5.1 Description

Cheryl recently migrated to another country and was still using her old phone and subscription from her home country. She was walking around when a familiar logo greets her. The sign indicated a WLAN service provided by the operator from her home country. Knowing she can connect to the hotspot easily by using her old phone, she proceeds to do so and starts using the WLAN service to chat with her friends.

B.5.2 Background

This use case illustrates the process on how users/devices connect to a hotspot provided by the home operator while roaming into a visited 3G network.

B.5.3 Sequence of Events

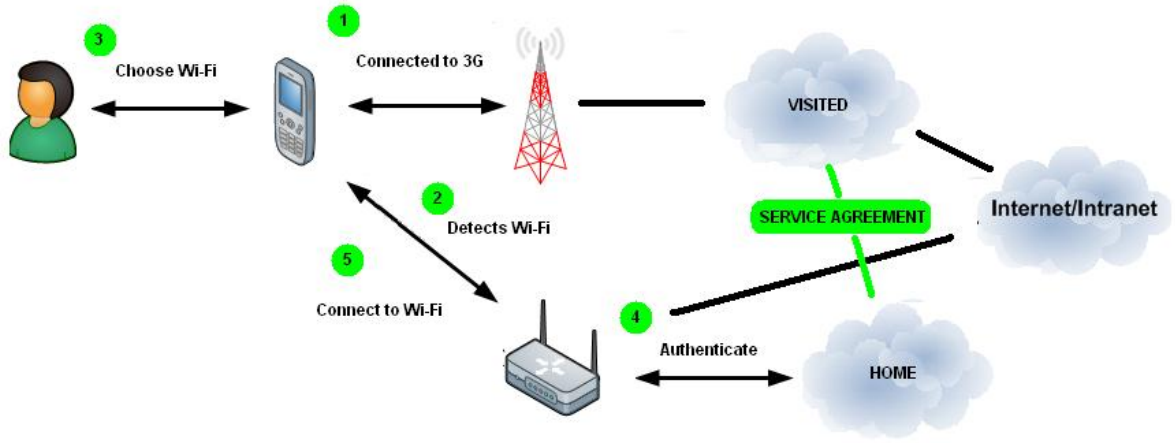

Figure 5: Example 3 - Radio Access Network Connection Switching

1. Mobile device is connected to the visited operator's network and is currently in 3G.
2. Mobile device detects WLAN network provided by the visited operator.
3. User decides to switch to the WLAN network.
4. Mobile device is authenticated and authorized to use the WLAN network by the home operator through a service agreement with the visited operator.
5. Mobile device is now connected to the WLAN network.

B.6 Home (3G) to WLAN (Provider) with Service Agreement

User decides to switch from 3G, which is provided by the user's home operator, to WLAN.

B.6.1 Description

Llorana has a phone subscribed to Smarty Networks and a WLAN subscription service to TwoTone which she uses for her laptop. She goes shopping and remembers she needed to send out an important email. She brings out her phone and sees a list of available hotspots. Seeing TwoTone is available, she opts to use WLAN to connect to the internet and sends out her email and continues shopping.

B.6.2 Background

This use case illustrates the process on how users/devices connect to a hotspot provided by a WLAN provider while in a home 3G network.

B.6.3 Sequence of Events

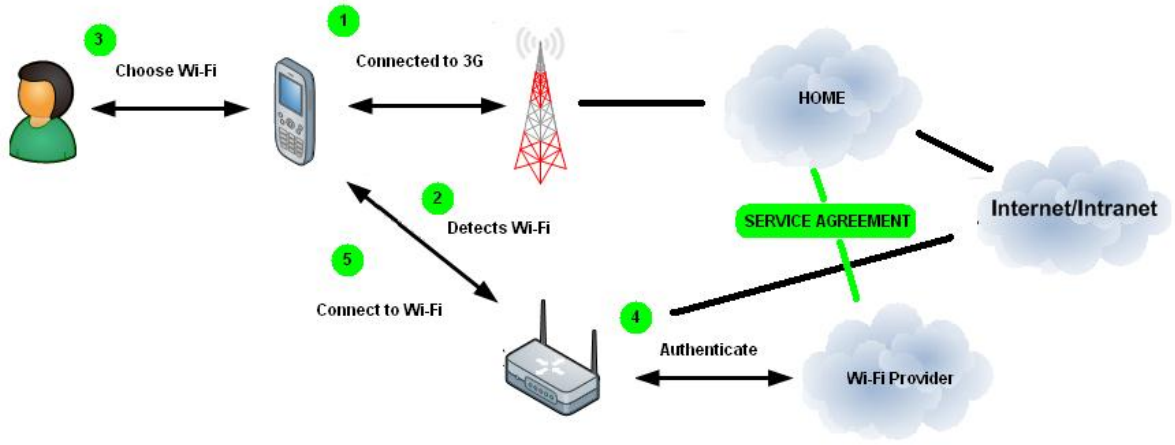

Figure 6: Example 4 - Radio Access Network Connection Switching

1. Mobile device is connected to the user's home operator network and is currently in 3G.
2. Mobile device detects WLAN network with which the user has an account.
3. User decides to switch to the WLAN network.
4. Mobile device is authenticated and authorized to use the WLAN network by the WLAN provider though a service agreement with the home operator.
5. Mobile device is now connected to the WLAN network.

B.7 Home (3G) to WLAN (Provider) with No Service Agreement

B.7.1 Description

Kristine lives in a small community wherein a number of coffee shops offer WLAN accounts to their loyal customers. Her phone is subscribed to Smarty networks and is not affiliated to any WLAN provider. Being a coffee shop enthusiast, she usually hangs around the shops a few hours in a day and this gives her maximum use of her WLAN account.

B.7.2 Background

This use case illustrates the process on how users/devices connect to a hotspot provided by a WLAN provider while in the home 3G network which has no service agreement.

B.7.3 Sequence of Events

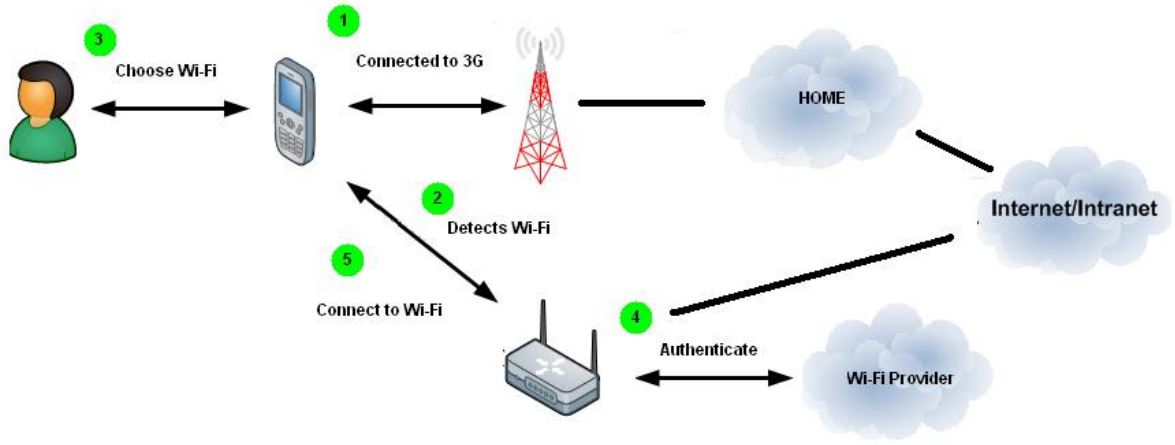

Figure 7: Example 5 - Radio Access Network Connection Switching

2.

1. Mobile device is connected to the visited operator's network and is currently in 3G.
2. Mobile device detects WLAN network with which the user has an account.
3. User decides to switch to the WLAN network.
4. Mobile device is authenticated and authorized to use the WLAN network by the WLAN provider.
5. Mobile device is now connected to the WLAN network.

B.8 Visited (3G) to WLAN (Provider) with Service Agreement

User decides to switch from 3G, which is provided by the visited operator, to WLAN

B.8.1 Description

Louella is heavy internet user and prefers to use WLAN to connect whenever she can. She is subscribed to PingPing, a WLAN provider available in many countries. On her usual business trip to another country, her phone connects to the 3G PingPong network. PingPong network and PingPing is known to have a service agreement. She notices the PingPing logo offering WLAN services, she opts to use WLAN and starts to check her emails.

B.8.2 Background

This use case illustrates the process on how users/devices connect to a hotspot provided by a WLAN provider while in a visited 3G network.

B.8.3 Sequence of Events

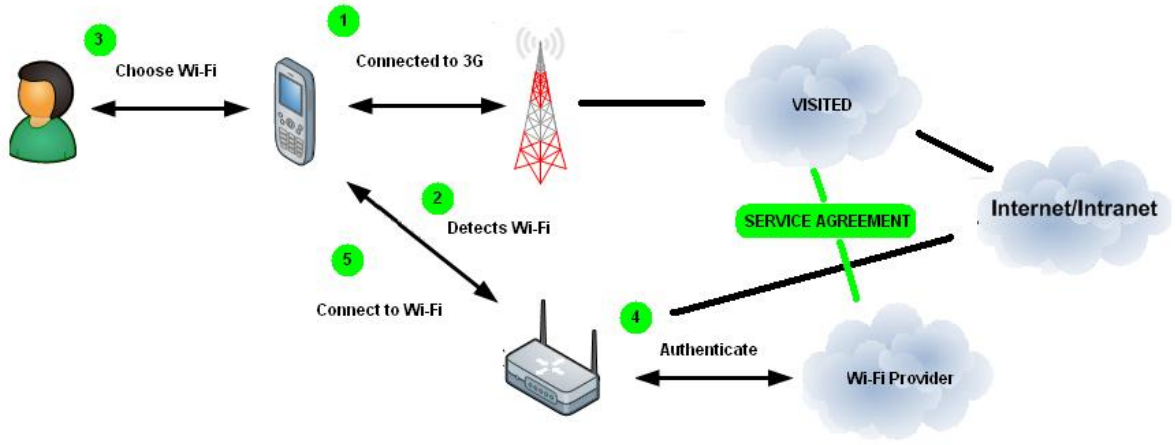

Figure 8: Example 6 - Radio Access Network Connection Switching

1. Mobile device is connected to the visited operator's network and is currently in 3G.
2. Mobile device detects WLAN network.
3. User decides to switch to the WLAN network.
4. Mobile device is authenticated and authorized to use the WLAN network by the WLAN provider through a service agreement with the visited operator.
5. Mobile device is now connected to the WLAN network.

B.9 Visited (3G) to WLAN (Provider) with No Service Agreement

B.9.1 Description

Rizaden frequently travels abroad and uses the internet frequently. She is subscribed to Looper, a WLAN Service Provider. She usually looks for a Looper hotspot so she can sign in and use the internet.

B.9.2 Background

This use case illustrates the process on how users/devices connect to a hotspot provided by a WLAN provider while in a visited 3G network with no service agreement.

B.9.3 Sequence of Events

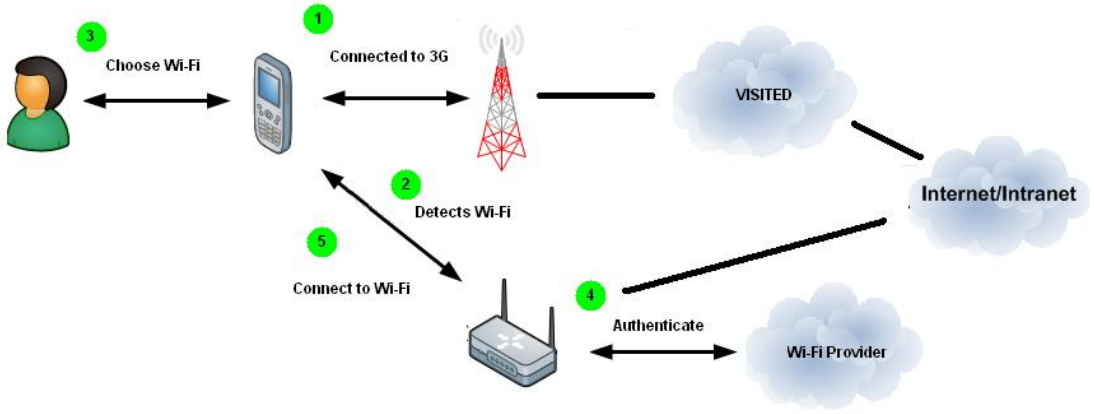

Figure 9: Example 7 - Radio Access Network Connection Switching

1. Mobile device is connected to the visited operator's network and is currently in 3G.
2. Mobile device detects WLAN network.
3. User decides to switch to the WLAN network.
4. Mobile device is authenticated and authorized to use the WLAN network by the WLAN provider.
5. Mobile device is now connected to the WLAN network.

B.10 Device concurrently connected with cellular network and WLAN

B.10.1 Description

An operator may decide to perform selective offload to WLAN traffic that provides little or null revenues which will keep using cellular networks to exchange traffic providing higher revenues. Nevertheless, the user experience concerning the offloaded traffic should not be affected, therefore the quality of the WLAN link needs to be taken into account.

B.10.2 Background

This use case illustrates the process on how the device connects concurrently to WLAN and cellular networks and exchanges traffic through both accesses concurrently.

B.10.3 Sequence of Events

1. User and network operator provides the device with their traffic routing policies (e.g. the operator indicate to the device to use WLAN for http traffic to a media content server X)
2. Mobile device is connected to the cellular network.
3. WLAN network is detected.
4. Mobile device is authenticated and authorized to use the WLAN network.
5. Mobile device is now connected to the WLAN network while keeping the connection with cellular network.
6. (optionally) Mobile device checks that WLAN link and network capability is good enough for http traffic to a media content server.
7. Mobile device routes traffic to the media content server X through WLAN and uses the cellular network for all the other traffic.

Annex C Usability Use Cases

C.1 Use Case: Connect to a Home Service Provider's hotspot with no intervention

C.1.1 Description

Charles, a happy iConnect subscriber, is going back home after a long day at work. His terminal has been connected all day to various hotspots. He wants to show some pictures stored in his mobile terminal on the home DLNA TV screen, and play some music in the background. His terminal connects automatically (without any action from Charles) to the home AP. Later Charles will look for a video and will display it on his mobile terminal.

C.1.2 Background

This use case aims to show that at home a user must be connected to his private access hotspot which offers the access to the home LAN service, with the highest speed, the lowest price, and hopefully privacy and security.

C.1.3 Sequence of Events

1. The mobile device scans and detects a home SP's hotspot in the area.
2. The hotspot's connection policy is assessed by the mobile device's connection manager.
3. The connection manager determines that the mobile device has the needed credentials to connect to the hotspot.
4. Based on the connection policy, the connection manager decides on the specific actions needed in order to connect to the hotspot.
5. It could be possible that the terminal will look first for the last connected AP (for instance a public AP found in the street in front of his house) then in the next scan, it will connect straight to the private access hotspot.

C.2 Use Case: Connect to a HSP hotspot with no intervention

C.2.1 Description

Dave, an existing iBonanza subscriber, is at his university. He needs to create a paper for his Sociology class. To gather references, he decides to look on the internet. Dave's laptop detects an iBonanza hotspot in the university. It connects to the hotspot securely and automatically. Dave browses the internet and finds what he needs.

C.2.2 Background

This use case aims to show that once a user avails of a hotspot service from a provider, there will be no need for them to enter their credentials manually to access the SP's hotspots in any location. The user should also be assured of security during associating and usage.

C.2.3 Sequence of Events

1. The device scans and detects a home SP's hotspot in the area.
2. The hotspot's connection policy is assessed by the mobile device's connection manager.
3. The connection manager determines that the mobile device has the needed credentials to connect to the hotspot.

4. Based on the connection policy, the connection manager decides on the specific actions needed in order to connect to the hotspot.
5. The mobile device is given the hotspot's provider name which the mobile device may display along with any additional information.

C.3 Use Case: Informed Network Selection based on Network Information when in several Hotspots

C.3.1 Description

Allan has an account with his home Service Provider. He is in the park and wants to teach his dog new tricks. He remembers a video in the internet which shows tutorials. Allan decides to stream some of the videos. However, in order to do so, Allan's mobile device should connect to a hotspot which has sufficient bandwidth to support video streaming. Allan's device scans and connects to such a hotspot and is now able to view videos.

C.3.2 Background

This use case aims to show how Allan's mobile device automatically chooses the appropriate hotspot based on network information when in the presence of multiple hotspots.

C.3.3 Sequence of Events

1. Device scans and detects multiple hotspots in the area.
2. Device determines the best suited hotspot by analysing each of the hotspot's network information against the requirements for video streaming.
3. Device finds an AP which has enough bandwidth for video streaming.
4. Device connects to the said AP.
5. User is able to stream videos.

C.4 Use Case: Informed Network Selection based on HSP policies when in several Hotspots

C.4.1 Description

Bobby is taking a vacation in Hong Kong and wants to check his email. However there is no hotspot in the area which belongs to his Home SP. As a result, he decides on availing WLAN services from iBonanza to check his email.

After his vacation, he flies back to Japan. At the airport, he decides to check his email once more. However, the mobile device is within the range of two WLAN providers, iBonanza and his Home SP. However, since his device has been provisioned with his Home SP policies, the mobile device connects to his Home SP network. After checking his email, he leaves the airport and takes a cab home.

Later, Bobby goes to a nearby coffee shop and orders a drink. While relaxing he decides to check the news but the coffee shop's hotspot is in the Home SP exclusion list. Hence the mobile device did not automatically connect to it. Bobby then decides to manually connect to the hotspot and was able to check the news.

C.5 Background

This use case aims to show how Bobby's mobile device automatically chooses the appropriate hotspot based on Home SP policies provisioned in the mobile device when in the presence of multiple hotspots.

C.5.1 Sequence of Events

1. The device is provisioned with the Home SP policies. This makes the mobile advice able to connect to preferred networks based on the policies whenever it detects them.
2. Device scans and detects multiple hotspots in the area.
3. When the device identifies a preferred network after it organizes the hotspots, it tries to connect to the preferred network.
4. However, when the device does not identify a preferred network in the list, it checks the list for hotspots in the home SP policies' exclusion list.
5. If a hotspot is in the home SP's exclusion list, the mobile device will not automatically associated to it unless the user manually chooses to connect.
6. Use Case: Informed Network Selection based on user preference when in several Hotspots

C.5.2 Description

Casey is in the mall with her friends. After doing some shopping, Casey and her friends decide to watch a movie. However, they could not decide between two movies. Therefore, she decides to look for reviews of the movies on the internet. Upon scanning, the mobile device discovers three networks in the area, the mall's hotspot, her home SP's hotspot, and iBonanza hotspot. Since she has an account with iBonanza and has configured her phone to prioritize connection to it, the mobile phone automatically is associated and connects to the iBonanza hotspot. Casey was able to read the reviews.

C.5.3 Background

This use case aims to show how Casey's mobile device automatically chooses the appropriate hotspot based on Caseys configured hotspot preference when in the presence of multiple hotspots.

C.5.4 Sequence of Events

1. The user configures and prioritizes a list of user preferred hotspots and a list of security credentials to use on the mobile device.
2. Device scans and detects multiple hotspots in the area.
3. The connection manager determines which hotspot to associate with based on the user configured list of preferred hotspots.
4. Device evaluates the required security credentials and connects to the hotspot with the allowed credentials based on the configured user list of security credentials.

C.6 Use Case: Network Hierarchy and Selection

C.6.1 Description

Marianne moved out of their house and transferred to a condominium near her school. Every Wednesday of the week, she usually watches her favourite TV show. It happens that her favourite TV show can also be streamed on the internet. Marianne has an option to watch it through her mobile device by the service of the local cellular network. She also has an option to use a WLAN enabled broadband router which is supplied by a local cellular operator or by another SP since her condominium is beside a coffee shop who offers internet to customers. Another option of Marianne is to use the neighbour's WLAN enabled broadband router which is managed by the residential owner.

C.6.2 Background

This use case aims to discuss on how the service will be delivered to the user. Through the network selection policy, the more preferred network will be chosen by the device. Example is when cellular data is in use then there is a hotspot detected. Hotspot will be chosen due to better performance based on different factors.

C.6.3 Sequence of Events

1. User utilizes the mobile device to watch his/her favourite streaming TV show
2. The mobile device has an option to access the internet thru various WLAN APs or thru cellular networks.
3. The residential (private) WLAN hotspot will be chosen as the preferred delivery network.
4. User can now watch his/her favourite TV show

C.7 Use Case: Manual Provisioning and Online sign-up

C.7.1 Description

Denize is a frequent customer of a certain coffee shop near her office. She really loves their specialty drinks and usually finishes her overtime work there. One thing she does not like with the coffee shop is that it has no free public hotspot. Her favourite coffee shop operates a secure hotspot and she needs to pay for it. After the procedure, Denize's mobile device is securely provisioned with the appropriate credentials and configuration to access the hotspot. Denize can now access the internet to check her emails.

C.7.2 Background

This use case aims to determine the process for obtaining an account and access from a secured hotspot. This process includes Discovery, Registration, Provisioning, and Access. In order for the user to gain access from the secured hotspot, the user should perform an online sign-up and give their credentials to gain access to a secured hotspot. After the process of signing-up, the credentials will be authenticated and authorized to give access to the account of the user.

C.7.3 Sequence of Events

1. User's mobile device detects a secured hotspot
2. User will register for the online sign-up and provide her credentials
3. After registration, his/her mobile device will be given access to the internet

C.8 Use Case: 3G/WLAN Mobility

C.8.1 Description

Leigh wanted to cruise the city. Knowing the city is blanketed with WLAN hotspots, she turns on her device and wanted to listen to music from her favourite streaming radio channel. She tunes in to her favourite channel and plugs the device into her car entertainment system. While travelling, her device changes from one network AP to the next hotspot to maintain connectivity. After a few miles, she reaches the expressway and noticed a stutter in the music. Her device beeps and blinks an icon changing from a WLAN antenna to a 3G lettered icon. Upon entering the next expressway exit, she again hears a beep and blinking icon from 3G to WLAN. She continues her cruising adventure in the next city with her streaming music in the background.

C.8.2 Background

The intent of this use-case is to illustrate sections on network handover, WLAN link quality, and intermittent WLAN connectivity. Some smartphones have the capability to switch to and from cellular and WLAN networks with minimal to no intervention from the user.

C.8.3 Sequence of Events

1. Device connects to a preferred hotspot that was provisioned beforehand.
2. Device encounters and scans periodically for new hotspots.
3. When the signal is fading from the hotspot, the device connects to the next available hotspot to continue connectivity.
4. When there is a fading signal and no other hotspots are available, the device falls back to cellular.
5. While still connected to the cellular, the device opportunistically scans for hotspots in the location.
6. Device finds a suitable hotspot and connects to it.
7. User continues to enjoy “seemingly” uninterrupted service.

C.9 Use Case: WPS

C.9.1 Description

Liza got her new mobile device with WLAN capability. Upon getting home she happily opens up the device and tries to connect to her WLAN home network. Her device prompted for the pre-shared key to access the network. She totally forgot about her pre-shared key and did not want to reset it since her siblings were also using it. She opened the manual of the mobile device and found out it had a WPS feature. She went to her WLAN router, pressed the WPS button and accessed the WPS feature on her mobile device. A few moments later she was able to connect and start surfing with her new mobile device.

C.9.2 Background

This use case illustrates the convenience that WPS presents to the user in connecting to a hotspot that has security measures such as WPA2.

C.9.3 Sequence of Events

1. User presses the WPS button on the WLAN router/hub.
2. User uses the WPS feature on the device.
3. Device and router/hub agree based on the WPS connection mechanisms.
4. Router/hub allows device to connect.
5. Device is now connected

C.10 Use Case: WLAN Management APIs

C.10.1 Description

Natalia is a programmer for Smarty Networks. She was tasked to create an application to be pre-installed on their next generation of handset offerings. Due to the lack of an integrated system to manage their devices, she created an application to pull the list of network identifier that Smarty Networks uses and update the list on the handsets thru the application.

The device begins by checking the update server for new data every week. Once an update is found, the application downloads the data and parses through it. The application then

updates the network identifier list on the device using management APIs available on the device.

C.10.2 Background

In the world of software and hardware, APIs are paramount in the burgeoning amount of applications available. Though some APIs should understandably be limited to operators and vendors, others are safe to expose to third party developers.

The intent of this use-case is to illustrate the ability for operators to build their own applications that require management of WLAN capabilities. This alleviates vendors from implementing varying and often conflicting needs of different operators.

C.10.3 Sequence of Events

1. Programmer builds an app to utilize the available management APIs.
2. Application calls management APIs.
3. Device appropriately performs the task and produces the desired result.

C.11 Use Case: Status Information, Function Accessibility, Power Management

C.11.1 Description

Faith is a techie that constantly uses her mobile device to chat and watch videos on the internet. She walks into a coffee shop and notices free WLAN for customers. She turns on the WLAN radio in one click on the device home screen and starts to use the WLAN to watch videos. She noticed the WLAN connection to be faster according to the status bar on her device.

After an hour, her device bleeps, enables battery saving mode and dims her display. She wanted the display to be brighter due to the dark lighting of the coffee shop. She pops up the device settings and disables the battery saving mode. After another hour, she notices she was running out of battery power and decides to turn off her WLAN and enable battery saving.

C.11.2 Background

The intent of this use-case is to focus aspects on usability such as WLAN function accessibility and power management.

Some smartphones have one-click implementations of turning off the WLAN on “power bars” or as checkboxes on the home screen menus. Status information such as connectivity type is also evident in most devices in the form of icons as an antenna or letters “3G.”

Usability aspects of terminals are in most cases for user intuitiveness and ease-of-use. Users accustomed to one device interface are likely to encounter an initial difficulty in performing simple tasks such as turning off the WLAN radio or checking what is the status of their connection. Having a more cohesive usability behaviour and interface generally benefits the user.

C.11.3 Sequence of Events

1. User turns on WLAN with a few clicks and connects to a hotspot.
2. Device successfully associates itself with the hotspot and updates icons and some text on the device for the user to see.
3. Network speeds are displayed and updated by the device at intervals.

4. Upon reaching a certain battery level threshold, the device notifies the user through beeps or icons the low battery level and implements battery saving measures.
5. User disables the battery saving mode through an application or device setting interface.
6. User continues using the device at low battery levels.
7. User decides to enable battery saving and turn off the WLAN from the device interfaces.

C.12 Use Case: Child-safe Online Content

C.12.1 Description

Abigail just got her new mobile device from her mother as a birthday gift. She immediately, connected to 3G, set up her chats and social networking accounts and sent a shout-out to her friends. A naughty friend of hers sent her a link and asked her to open it and check it out. She clicked it and was surprised that it displayed a page informing her that she is not allowed to access the content. She tried to browse her accounts on several social networking sites but encountered no such problem.

She decided to go to nearby fast-food chain and connect to the free WLAN. She tries to browse the link given to her but was still unable to do so.

Beforehand, her mother knowing she is a tech-savvy, turned on the parental control on the device before wrapping it up.

C.12.2 Background

The intent of this use case is to illustrate the possible mechanisms to implement parental control. The implementations need not be network and device at the same time but may be either to enforce it appropriately depending on the circumstances.

Due to geographical/regional regulations, some Mobile Network Operators required a form content or network control to access content. Some operators implement a blacklist of sites in their network systems, implementing a network controlled interface for content filtering.

Several browsers already have a system of plug-ins for filtering non-child-safe sites using blacklists hosted on their own servers.

C.12.3 Sequence of Events

1. The device detects that is in a cellular connection.
2. A URL is requested by the device to the network with a key indicating the parental control is turned on, e.g. a crafted http-header.
3. The operator system crosschecks the URL with a list of filtered sites.
4. It is determined that the site is not allowed when parental control is turned on.
5. The device receives a page notification that access to the page is not allowed..
6. On the succeeding occasion that the device is connected to a WLAN hotspot, the browser checks for the blacklisted sites in a local cache to see if the content is allowed or not.
7. Some browsers have a plug-in that caches the list and is updated regularly by the authors/host of the content filtering components.

C.13 Use Case: Quality of Service Access managed by the network

C.13.1 Description

Charles-Antoine, a happy iConnect subscriber, always expects to get the best connection from his telecom operator, whatever his location and the time of connection, between WLAN, 3G, and 4G bearers. Charles wants in particular to watch his video in live streaming.

C.13.2 Background

The throughput on WLAN access depends on several factors, such as hotspot backbone connectivity (ADSL, fibber, etc.), radio field strength, available bandwidth granted to private access versus public access.

Hence a dynamic access control mechanism managed by the network should be used to guarantee a better customer experience.

The network must be able to refuse temporarily a connection, so that the terminal will stay on the 3G network or on a current hot spot without displaying any message to the customer. A limited retry scheme has to be defined, to avoid network overload (for instance: two retries separated by 60 seconds)

If the terminal detects another hotspot, then it will launch another connection request

For example, this mechanism could rely on the usage of existing error causes described in the RFC 4186. at § 10.18. AT_NOTIFICATION

C.13.3 Sequence of Events

1. The mobile device scans and detects a home SP's hotspot in the area.
2. The hotspot's connection policy is assessed by the mobile device's connection manager.
3. The terminal sends a connexion request
4. The hotspot considers that the radio condition or the Quality of connection is not good enough and sends an error message to the terminal to block any connexion
5. While still connected to the cellular network, the device scans for hotspots in the location.
6. After a while the device found another hotspot and send a new request
7. The hotspot accept the connection
8. The terminal switches to WLAN on that hotspot

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

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.