Recommendations for Minimal Wi-Fi Capabilities of Terminals

Version 1.1

18 December 2012

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

Security Classification: Non-confidential

Copyright Notice

Disclaimer

Antitrust Notice

Table of Contents

1 Introduction

1.1 Purpose

Wi-Fi 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 the IEEE 802.11 family of standards.

However these terminals have varying degrees of Wi-Fi support and this poses a number of risks in the market such as the confusion created by the different implementations of the Wi-Fi to end-users hence making them resistant in using it and there are also the interoperability issues of Wi-Fi. The different Wi-Fi implementations and requirements create fragmentation that impacts its use in the market.

The, GSMA TSG (Terminal Steering Group) has created a document which will help standardize Wi-Fi implementation of MNOs and OEMs. The document was created by consolidating and deliberating all MNOs and OEMs Wi-Fi requirements.

1.2 Scope

1.3 Objective

The aim of this document is to consolidate terminal requirements and existing Wi-Fi experiences from various operators. It is the intent of this document to become a tool to help operators align their Wi-Fi requirements.

This document details features or items not previously discussed in other Wi-Fi related documents such as out-of-the-box configurations. The consolidated features and requirements pertain to device/terminal aspects, and outlines a minimum set of Wi-Fi capabilities to be supported by Wi-Fi enabled terminals but does not exclude the possibility for additionally support of other Wi-Fi capabilities not mentioned in this document.

1.4 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
HS2.0	Wi-Fi Hotspot 2.0 Program
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
PLMN	Public Land Mobile Network
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
WFN	Wi-Fi Network
Wi-Fi	Wireless network using IEEE 802.11 standards
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

1.5 Reference Documents[1]

Document Number	Title
	Wi-Fi Offload Whitepaper Version 1.0 19 April 2010 Source: www.gsma.com/go/download/?file=wifioffloadwhitepaper.pdf
	Wi-Fi Alliance Marketing Requirements Document for Hotspot 2.0: Wi-Fi CERTIFIED Passpoint™ Certification Amendment
	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
RFC 4026	Provider Provisioned Virtual Private Network (VPN) Terminology Source: http://tools.ietf.org/pdf/rfc4026.pdf
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
24234-910	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
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 5448	Improved Extensible Authentication Protocol Method for

[1] These are relevant as and only if made available

	3rd Generation Authentication and Key Agreement (EAP-AKA') Source: http://tools.ietf.org/pdf/rfc5448.pdf
RFC 5247	Extensible Authentication Protocol (EAP) Key Management Framework Source: http://tools.ietf.org/pdf/rfc5247.pdf
RFC 3748	Extensible Authentication Protocol (EAP) Source: http://tools.ietf.org/pdf/rfc3748.pdf

2 Security

2.1 Authentication Protocols

2.1.1 EAP-SIM/EAP-AKA/EAP-AKA'

In order to support a more seamless authentication experience in Wi-Fi, it is a requirement to provide consistent support for the appropriate authentication mechanisms. Operators believe that SIM-based authentication is one of the key requirements to increasing Wi-Fi usage and a fundamental requirement of WFA's Hotspot 2.0 initiative. Requirement is that SIM based terminals must support SIM-based authentication.

The EAP (Extensible Authentication Protocol) is an authentication framework that provides the transport and usage of cryptograph keys and parameters generated by the protocol. To mirror the security and authentication for GSM and UMTS, it is recommended that EAP methods: EAP-SIM and EAP-AKA (assumed to also include EAP-AKA') be supported by terminals.

In Wi-Fi networks, the standard usage of EAP-SIM and EAP-AKA is supported by WPA2 Enterprise. The main advantage of using these EAP methods is that the same security processes are then used for Cellular and Wi-Fi networks, preventing unauthorized connections to those networks.

Req ID	Requirement
TSG22_SEC_01	Terminals SHALL support EAP-SIM when SIM or USIM is used.
TSG22_SEC_02	Terminals SHALL support either EAP-AKA or EAP-AKA' when USIM is used.
TSG22_SEC_03	Terminals SHOULD support legacy authentication.

2.1.2 IEEE 802.1X

This is another key component of the HS2.0 initiative that aims to provide Wi-Fi users a more seamless user experience. Requirement is to support IEEE 802.1X for terminal.

IEEE 802.1X, also known as EAPoL 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 Wi-Fi networks 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.

Req ID	Requirement
TSG22_SEC_04	Terminals SHALL support IEEE 802.1X.

2.1.3 Authentication Priorities

Several Authentication mechanisms can be used or should be supported by the terminal. The preference would be for the terminal always to be authenticated using the SIM/USIM.

There are SIM-based and non-SIM-based Authentications mechanisms available to authenticate a user on a Wi-Fi hotspot network. TSG work defines that for GSMA member operators SIM-based authentication is recommended as first priority as it is within GSMA's remit to define and maintain essential security, certification hence implementation aspects. TLS and TTLS are identified as optional mechanisms, with reference to WBA and WFA documentation for further information on implementation details.

Req ID	Requirement
TSG22_SEC_05	Terminals with a valid (U)SIM SHALL have an authentication priority mechanism with EAP-SIM and either EAP-AKA or EAP-AKA' as highest priority.

2.2 Air Link Security

Wi-Fi Protected Access II Enterprise (WPA2 Enterprise) is the latest version of the security protocol and security certification programs developed by the Wi-Fi Alliance to secure the access to a WLAN. To provide a secure means of communication for the terminals, WPA2 Enterprise is Mandatory.

Support for older and non-secure security mechanism must be discontinued in favour of newer and more secure mechanisms. For both operators and customers, using the SIM card for authentication and security is a convenient means to simplify the process for subscribers.

Req ID	Requirement
TSG22_SEC_06	Terminals SHALL support WPA2 Enterprise and WPA2-Personal.
TSG22_SEC_07	Terminals SHOULD NOT support WEP.

2.3 IEEE 802.11u

IEEE 802.11u can be used to advertise roaming relationships between HS2.0 operators, similar to those mechanism used today for cellular access.

HS2.0 will provide improved Wi-Fi network selection and network access, including the ability to provide network access for visiting users. IEEE 802.11u will be used 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.)

Req ID	Requirement
TSG22_SEC_08	Terminals SHOULD support IEEE 802.11u features within WFA's Hotspot 2.0.

3 Connection Management

3.1 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 Wi-Fi network connections based on the terminal status, connection conditions, operator policies and user profiles associated with these connections.

Some Connection Management APIs that terminals would have to manage the Wi-Fi better would be the following:

- Turn on and turn off the Wi-Fi (including support of flight mode)
- Query if Wi-Fi functionality is on or off
- Interact with the connection manager to connect/disconnect to/from Wi-Fi APs
- Use the operator predefined list of preferred network identifiers (e.g. SSID)
- Add, delete, modify and manage Wi-Fi profiles (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 Wi-Fi signal strength per network identifier (e.g. SSID - active or inactive), Wi-Fi 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 on a specific network identifier (e.g. SSID), visible or not.
- Listen to the Wi-Fi 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 Wi-Fi connection such as IP address, Subnet Address

Req ID	Requirement
TSG22_CM_09	Terminals SHALL have a pre-installed connection management client.
TSG22_CM_10	Terminals SHOULD have programming interfaces/APIs to control and/or manage Wi-Fi connection.
TSG22_CM_11	The pre-installed connection management client on the Terminal SHOULD be based on the API offered.
TSG22_CM_12	Terminals SHOULD offer API fully compliant with the OMA OpenCMAPI Release 1.0 on WLAN management.

3.2 Supported Networks

At the onset of growing available wireless hotspots in the world, Wi-Fi is becoming a defining avenue for operators to offload their traffic. This would however entail the use and standardization of dual-network handsets using 3GPP and Wi-Fi technologies. For example, the dual-network handsets can surf the Internet through Wi-Fi networks and receive SMS/MMS through cellular networks simultaneously.

Req ID	Requirement
TSG22_CM_13	Terminals SHALL have dual-network capability for cellular mobile networks and Wi-Fi technologies.

3.2.1 5GHz

The 2.4GHz band is widely deployed and in many areas can become congested due to both the number of AP (Access Points) s 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_USE_14	Terminals SHOULD support 5GHz.

3.3 WLAN Access Network Selection

For WLAN Access Point selection, the following inputs can be used:
Input for Access Point Selection:

- User preferences
- The input on the user preferences shall be considered
- Network policies

A pre-configured list of network identifiers can be used e.g. SSID list for Access Point selection. For example, this list can be downloaded to th device based on operator policy. Network identifiers can be used to identify the user's private network, an enterprise network, an operator network or a public network. In case Access Points are available with different categories of network identifiers, the terminal should use the following hierarchy for Access Point selection with the following priority (highest first): private network, enterprise network, operator network and public network.

- Status and quality of the connection
  It may happen that among the available Wi-Fi networks, there is only one possible Access Point that can be used to exchange data packets or one network is more suitable for the type of application and traffic.
- Status of the terminal
  The status of the device, e.g. location, battery life, can be used to perform network selection.

Req ID	Requirement
TSG22_CM_15	When selecting WLAN access, the terminal MAY select the network and radio connection to use according to the following inputs: User preference settings The policies received from the network. Information to pertain the status of the connection, e.g. Radio environment information, quality of IP connection, application specific requirements. Information to pertain the status of the device.
TSG22_CM_16	Terminals SHOULD consider user preference setting with highest priority when evaluating inputs for access technology selection.
TSG22_CM_17	When selecting WLAN access, the hierarchy of the inputs used by the terminal to select the proper network MAY be the following: 1) The policies received from the network. 2) Information pertaining the status of the device and the connection, e.g. radio environment information, quality of IP connection, application specific requirements
TSG22_CM_18	Terminals SHALL select a Wi-Fi network according to the terminal's pre-configured network identifier (e.g. SSIDs).

TSG22_CM_19	Terminals SHALL be able to perform network selection according to a network hierarchy.
TSG22_CM_20	Terminal network hierarchy selection SHOULD be: 1) Private Network Identifier (WPA2-PSK) e.g. SSID 2) Enterprise Network Identifier (WPA2-Enterprise) e.g. SSID 3) Operator Network Identifier (WPA2-Enterprise) e.g. SSID 4) Public Network Identifier (non-secured) e.g. SSID
TSG22_CM_21	Terminals SHALL be able to force the association on a Network Identifier, visible or not.
TSG22_CM_22	Terminals SHALL be able to identify known Wi-Fi networks and unknown Wi-Fi networks (known networks are network identifiers (e.g. SSID) pre-configured or that have already been used/predefined by the user).
TSG22_CM_23	Terminals SHALL be able to connect to known Wi-Fi networks.
TSG22_CM_24	Terminals SHOULD be able to connect to unknown Wi-Fi networks.
TSG22_CM_25	Terminals SHOULD have the capability to automatically reconnect to a higher prioritised Wi-Fi network when available even when already connected to another Wi-Fi network

3.4 Managing Multiple Radio Connections

Network selection is a process that can take into consideration several inputs. These inputs can be classified in 4 categories

- Operator policies
  The operator can provide the terminal with policies that indicate the preferred network (e.g. 3GPP vs. Wi-Fi) to use under specific conditions. In the case where the terminal can use only one interface among the available ones, the policies can indicate the operator indication on which network the terminal can use. If the terminal can use multiple interfaces the policies can indicate how traffic can be distributed among the active interfaces.
- Status and quality of the connection
  It may happen that among the available networks, there is only one possible network that can be used to exchange data packets or one network is more suitable for the type of application and traffic.
- Status of the terminal
  The status of the device, e.g. location, battery life, can be used to perform network selection.
- User preferences
  The input on the user preferences may be also considered

Req ID	Requirement
TSG22_CM_26	The terminal MAY be endowed with a functionality handling all radio connections including the Wi-Fi.
TSG22_CM_27	The terminal MAY select the network and radio connection to use according to the following inputs: User preference settings. The policies received from the network. Information to pertain the status of the connection, e.g. Radio environment information, quality of IP connection, application specific requirements. Information to pertain the status of the device and the connection.
TSG22_CM_28	Terminals SHOULD consider user preference setting with highest priority when evaluating inputs for access technology selection.
TSG22_CM_29	The hierarchy of the inputs used by the terminal to select the proper network MAY be the following:

	1) The policies received from the network. 2) Information pertaining the status of the device and the connection, e.g. Radio environment information, quality of IP connection, application specific requirements.
TSG22_CM_30	ANDSF MAY be used to provide the terminal with network policies.

3.5 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 HS2.0 network discovery.

Req ID	Requirement
TSG22_CM_31	Terminals SHALL be able to provide detailed information per network identifier discovered (such as signal strength, security methods, authentication credentials used, known or unknown network)
TSG22_CM_32	Terminals SHALL support a Wi-Fi network discovery mechanism that preserves battery life.
TSG22_CM_33	Terminals scanning algorithm SHOULD support HS2.0 discovery mechanisms.
TSG22_CM_34	Terminals SHOULD be able to listen & report events to an upper layer (e.g. UI) such as new available network, loss of network.

3.6 Network Handover

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 Wi-Fi.

It is important that the mobile network connection must be kept when the Wi-Fi access has been performed for the following reasons:

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

Network inactivity timer mechanism keeps working as normal.

If the terminal's AP changes, the DHCP function of the terminal may issue a DHCP request to the new AP, even if the identity or network identifier (e.g. SSID) of the AP doesn't change.

Req ID	Requirement
TSG22_CM_35	Terminals SHOULD have support for IPV6.
TSG22_CM_36	Terminals SHOULD be allowed IP address preservation for session continuity.
TSG22_CM_37	Terminals MAY use DHCP or DHCPV6 for the IP address assignment behaviour.
TSG22_CM_38	Terminals MAY support handover between 3GPP and Wi-Fi networks.

TSG22_CM_39	Terminals MAY make use of concurrent Wi-Fi and cellular mobile network access to allow for handover of network services.
TSG22_CM_40	Terminal SHALL keep the 3GPP mobile network connection e.g. PDP contexts during Wi-Fi access.

3.7 Provisioning

3.7.1 Operator Provisioning

Expanded service of operators through service agreements and partnerships can veritably 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.

HS2.0 defines operator policy features that make use of OMA DM to provide a means to configure a terminal, either through the cellular network or directly over the Wi-Fi access network. Note: HS2.0 also provides a SOAP-XML server as well as an OMA-DM server.

Req ID	Requirement
TSG22_CM_41	Terminal SHALL support provisioning of network identifiers through push or pull mechanisms.
TSG22_CM_42	Terminals SHOULD support OMA DM Managed Objects as defined by HS 2.0. Note:- Some operators may not have an OMA DM server

3.7.2 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 similarly in home network setups. The facility often exists to store profiles so that every time the terminal is in range of an existing Wi-Fi hotspot setup, the connection is automatic.

HS2.0 provides a standardised mechanism for manually provisioning hotspot network access entitled "Online Sign-up." The mechanism allows the terminal to be provisioned with both credentials and policy. There are different types of credentials that can be provisioned, for example username/password and certificates.

Req ID	Requirement
TSG22_CM_43	Terminals SHALL be capable of provisioning credentials, policy and network identifier (e.g. SSID) lists manually by the user
TSG22_CM_44	The terminals SHALL store manually provisioned configurations locally.
TSG22_CM_45	Terminals SHALL prioritize user/manual provisioned over operator provisioned network identifiers.
TSGXX_CM_46	Terminals MAY use HS2.0 for Online Sign-up.

3.8 VPN

In previous years, corporations use expensive leased lines to connect remote locations. Recently, VPN (Virtual Private Network) provided a means for organizations and private entities to utilize public communication infrastructures which still ensure data security, allowing lower communication costs with the same security that is provided by expensive

private leased lines.

Req ID	Requirement
TSG22_CM_47	Terminals SHOULD be able to initiate VPN connections for networks that require it. Note:- Some VPN networks require proprietary VPN software to connect. Installation of this software is out of scope of this document.

3.9 Wi-Fi Protected Setup (WPS)

Some technologies require a level of technological skill or background to setup or utilize. 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 Wi-Fi 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 designed to ease this process and set up of security-enabled Wi-Fi networks 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_CM_48	Terminals SHOULD support WPS with either PIN or both PIN & Push-Button methods for Wi-Fi.
TSG22_CM_49	Terminals SHOULD provide a Registrar capability as Client Device for WPS.
TSG22_CM_50	Terminals SHOULD provide a hardware or software button to trigger the WPS wireless protected Setup feature as well as a prompt to enter the PIN

3.10 Notification Architecture Compatibility

Terminals that use background notification such as mail and news feeds rely on periodic sending of data, “keep-alive” sessions”. These mechanisms are compatible with network firewalls. However, this may not be the case for APs that implement session expiration and hence disconnect the service from the network.

HS2.0 will provide features such as signalling of session expiration (both time based and data limit based) using IEEE 802.11v.

Req ID	Requirement
TSG22_CM_51	Terminals SHALL support a mechanism for providing end users with the appropriate service notifications.

3.11 Wi-Fi Link Quality

On most terminal devices, once Wi-Fi is detected, the data connection defaults to use its available resources. Unfortunately, being connected to the hotspot does not necessarily mean the availability or reliability of a data connection.

User experience and actual network performance based on parameters such as throughput, latency, signal strength etc. should be used for network selection.

Req ID	Requirement
TSG22_CM_52	Terminals SHALL have the capability to monitor the Wi-Fi link quality.
TSG22_CM_53	Terminals SHALL have the capability to switch to the 3GPP network should the Wi-Fi link quality be insufficient to maintain connectivity.
TSG22_CM_54	Terminals MAY have the capability to drop back to the Wi-Fi network should the Wi-Fi link quality be sufficient to maintain connectivity.
TSG22_CM_55	Terminals switching between 3GPP and Wi-Fi networks, or vice-versa, SHOULD NOT impact the user experience.

3.12 Intermittent Wi-Fi Connectivity

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

Maximizing available resources such as switching to higher bandwidth Wi-Fi presents an attractive alternative to users. However, automatically switching from 3GPP (2G/3G) and Wi-Fi may present usability problems to the terminal which is not properly configured to handle such scenarios and minimum interruption should be ensured.

Criteria

While the terminal is connected to Wi-Fi: a fast variation of the Wi-Fi signal strength (up or down) is the minimum criteria to indicate that the terminal is on the move and a handover to a cellular network should be performed.

While the terminal is connected to a cellular network and detects one or more candidate Wi-Fi APs, a short analysis of the Wi-Fi signal strength of candidate APs should be an additional criterion for the terminal to decide to switch from cellular to Wi-Fi. It is recommended that information when available from HS2.0 capable APs such as internet connectivity and WAN throughput is used. Hysteresis mechanisms should be implemented with tuned radio thresholds (hysteresis meaning threshold to access a Wi-Fi network is different from threshold to go back to cellular), so that a terminal switches back quickly to 3G, when Wi-Fi radio signal strength is fading or throughput is decreased to an unacceptable level.

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

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

In some cases, Wi-Fi 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_CM_56	Terminals SHALL have a hysteresis mechanism to prevent them from connecting and disconnecting to/from the same Wi-Fi AP within a minimum interval.

TSG22_CM_57	The terminal SHALL limit the number of access retries to the same Access Point when it receives temporary denied access notification from that Access Point. (as e.g. RFC 4186 1026 notification with EAPSIM)

4 Usability

4.1 User Interface

4.1.1 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 HS2.0 can also be provided, such as WAN link status, WAN uplink and downlink data rates Wi-Fi network name or logo should be displayed when connected to HS2.0 APs.

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

If Wi-Fi connection is secure (i.e. AP is HS2.0 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 Wi-Fi signal strength icon). If the Wi-Fi connection is insecure, a notification message should be displayed to the user if a terminal associates with the Wi-Fi AP for the first time.

Req ID	Requirement
TSG22_USE_59	Terminals that have a UI (User Interface) SHALL indicate the status of the terminal connection.
TSG22_USE_60	Terminals SHOULD offer programming interfaces providing Status Information to applications.
TSG22_USE_61	Terminals SHOULD offer API fully compliant with the OMA OpenCMAPI Release 1.0 on Status Information & notifications functions.

4.1.2 Wi-Fi On/Off Function Accessibility

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

All terminals have a means of turning off the Wi-Fi 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_USE_62	Terminals SHALL have an accessible means for toggling the Wi-Fi to on or off.

4.2 Device Firmware Updates

Throughout the life cycle of a terminal, firmware updates may be required to improve usability such as new phone applications, features and functional fixes.

In the lifecycle of a particular terminal, there are likely to be updates that can enhance or improve both performance and usability. It is recommended that an update capability for these terminals be in place to further make the terminal more useful to the subscriber.

Req ID	Requirement
TSG22_USE_63	Terminals SHALL have a facility to update its firmware.
TSG22_USE_64	Terminals MAY use standards such as FOTA, SCOMO, OMA DM for the updates.

4.3 Authentication Architecture Overload Data Prevention

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

Hence, some terminals could be parameterized with automatic EAP authentication and perform automatic connection attempts to Wi-Fi. If the network rejects the Wi-Fi access request of the terminal for a repeated number of times due to Wi-Fi 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 Wi-Fi APs will have a detrimental effect on usability and battery life.

Req ID	Requirement
TSG22_USE_65	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_USE_66	Terminals with a UI (User Interface) SHOULD notify to the user the failure of authentication.
TSG22_USE_67	Terminals SHOULD implement fast re-authentication mechanism described in the IETF RFC 4186 - EAP SIM.
TSG22_USE_68	Terminals SHOULD implement fast re-authentication mechanism described in the IETF RFC 4187 - EAP AKA/ IETF RFC 5448 - EAP AKA' .

4.3.1 Pre-Provisioning

Some operators may opt to pre-configure operator-controlled Wi-Fi AP unto terminals.

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

Req ID	Requirement
TSG22_USE_69	Terminals MAY have pre-provisioned information prior to subscriber use, network identifiers e.g. SSIDs and accompanying security keys

4.4 Power Management

4.4.1 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_USE_70	Terminals SHALL have a means of determining low battery level and automatically enabling power save mechanisms.
TSG22_USE_71	Terminals SHOULD make use of WFA power save mechanisms to preserve battery life.
TSG22_USE_72	Terminals SHOULD have a feature for users to toggle to battery saving mode.
TSG22_USE_73	Terminals SHOULD maintain Wi-Fi network connectivity while preserving battery life.

4.4.2 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_USE_74	Terminals SHALL have a traffic inactivity duration setting that will be indicated by the manufacturer trigger power save mechanism.
TSG22_USE_75	Terminals MAY use WFA power save mechanisms to achieve idle power management.

4.5 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-18) when browsing the Internet using cellular data. Wi-Fi is ubiquitous and can be operated by individuals without the need for a license to operate the Wi-Fi AP, thus there is no obligation for these individuals to enforce policies such as adult content filtering.

Req ID	Requirement	Notes
TSG22_USE_76	Terminals SHALL support a mechanism for Parental Control for access to unsuitable web content for children.	
TSG22_USE_77	Terminals SHOULD have their native internet browsers to support parental control.	
TSG22_USE_78	Terminals SHOULD restrict download of third party browsers without parental control feature	
TSG22_USE_79	Terminals MAY support a mechanism to lock/unlock the Wi-Fi access.	

4.6 Advice of Charge

Some geographic or local regulations require Mobile Network Operators to display or notify the user of charges that will be incurred if a service is used.

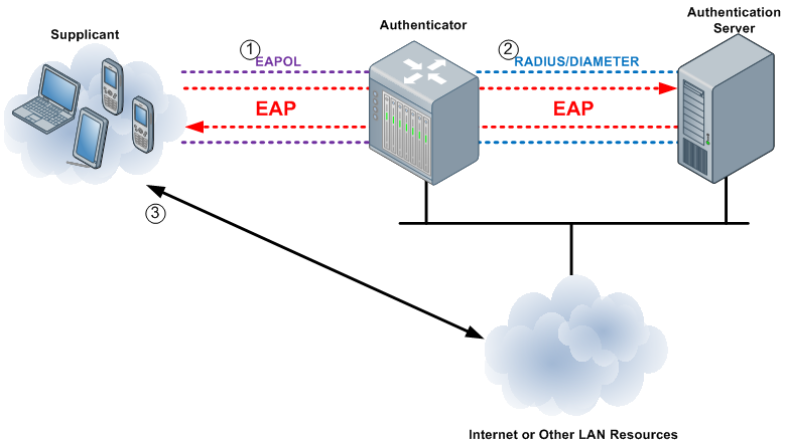
Many jurisdictions require that an advice of charge be presented to users before availing of an optional wireless service. This is the case for Wi-Fi roaming. The advice of charge notice

typically contains a description of service, relevant charges and terms/conditions. Some implementations include simply sending an SMS message and notifying the user of the charge. Others may have an interactive facility that allows the user to confirm the charge before proceeding.

Req ID	Requirement
TSG22_USE_80	Terminals with a UI (User Interface) SHALL provide a mechanism for notifying an advice of charge to users.
TSG22_USE_81	Terminals MAY use a screen display, SMS or sound to notify the user of switching to charged 3G and Wi-Fi tariff plan.
TSG22_USE_82	Terminals MAY support the ability to accept to connect or cancel the attempt to connect to the hotspot.

5 Annex – Network/Connectivity Use Cases

5.1 WPA2, 802.1X (EAPOL), EAP



5.1.1 Description

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

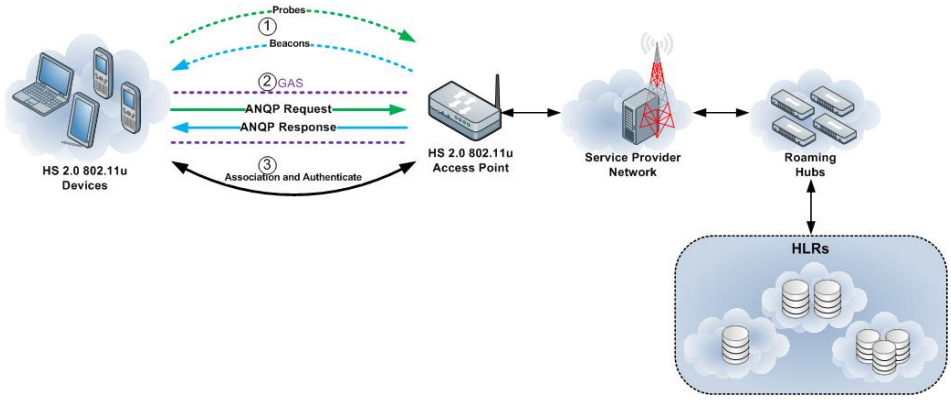
5.1.2 Background

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

5.1.3 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.

5.2 802.11u



5.2.1 Description

Raymond is at a restaurant when he notices that it offers Wi-Fi 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.

5.2.2 Background

This use case attempts to show the convenience that 802.11u provides to the user when connecting to an 802.11u-enabled Wi-Fi 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.

5.2.3 Sequence of Events

1. Users choose to connect to Wi-Fi.
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.

5.3 Home (3G) Switch to Home (Wi-Fi)

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

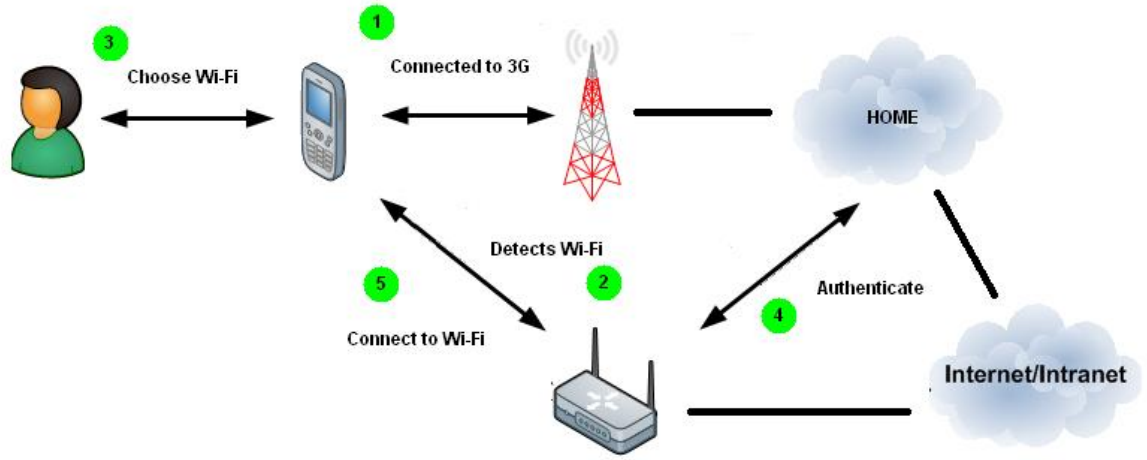
5.3.1 Description

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

5.3.2 Background

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

5.3.3 Sequence of Events



6. Mobile device is connected to the user's home operator network and is currently in 3G.
7. Mobile device detects a Wi-Fi network provided by the user's home operator.
8. User decides to switch to the Wi-Fi network.
9. Mobile device is authenticated and authorized to use the Wi-Fi network by the home operator.
10. Mobile device is now connected to the Wi-Fi network.

5.4 Visited (3G) to Visited (Wi-Fi)

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

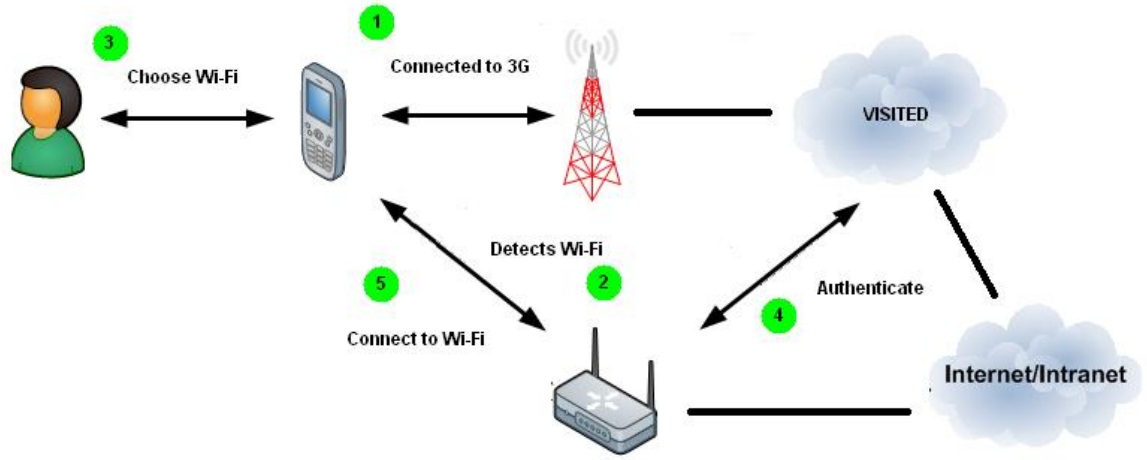
5.4.1 Description

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

5.4.2 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.

5.4.3 Sequence of Events



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

5.5 Visited (3G) to Home (Wi-Fi)

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

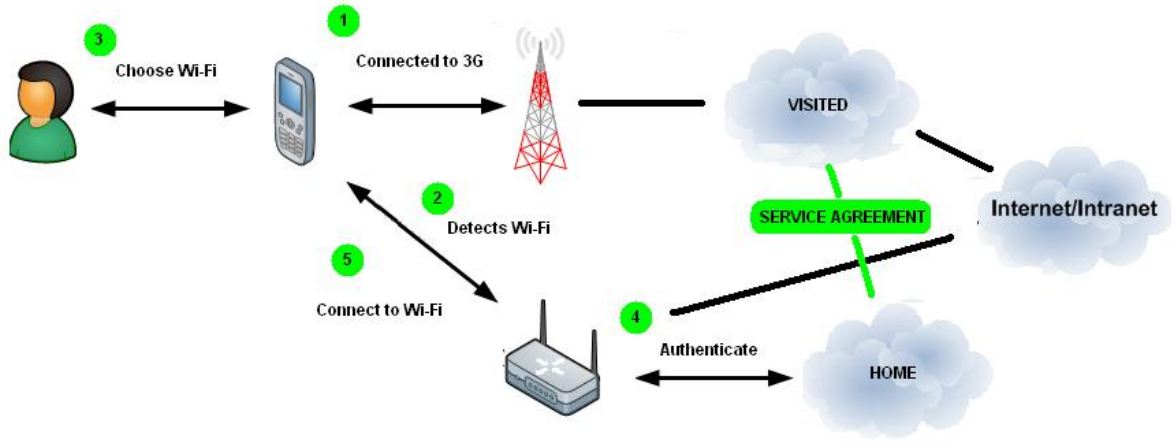
5.5.1 Description

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 Wi-Fi 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 Wi-Fi service to chat with her friends.

5.5.2 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.

5.5.3 Sequence of Events



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

5.6 Home (3G) to Wi-Fi (Provider) with Service Agreement

User decides to switch from 3G, which is provided by the user's home operator, to Wi-Fi

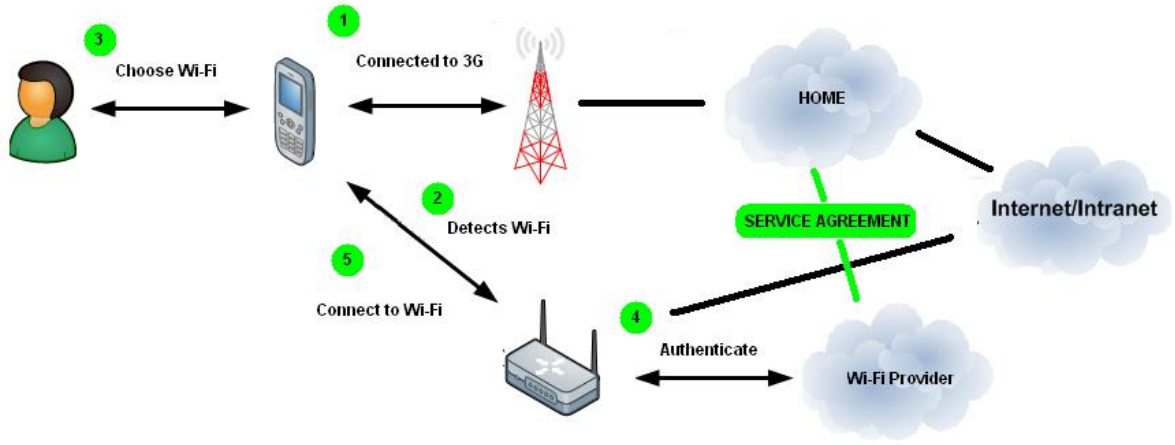
5.6.1 Description

Llorana has a phone subscribed to Smarty Networks and a Wi-Fi 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 Wi-Fi to connect to the internet and sends out her email and continues shopping.

5.6.2 Background

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

5.6.3 Sequence of Events



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

5.7 Home (3G) to Wi-Fi (Provider) with No Service Agreement

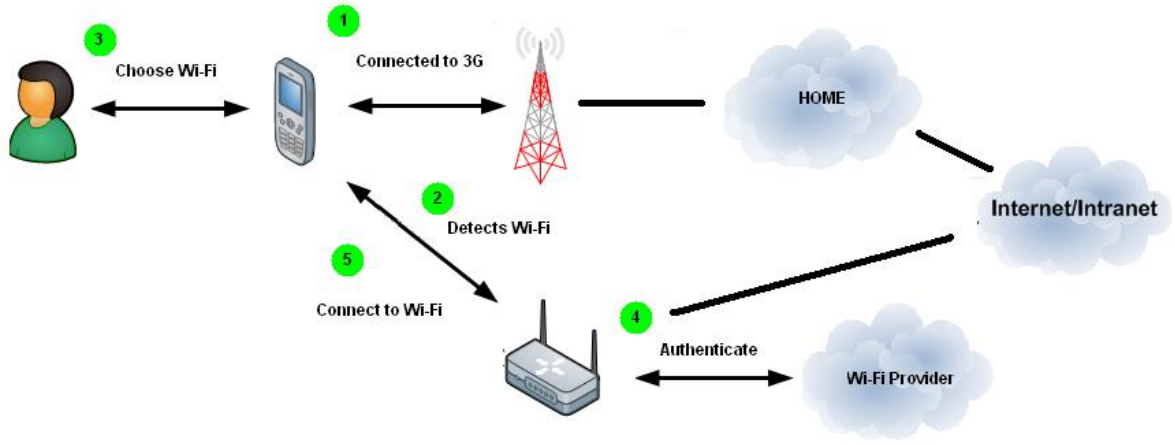
5.7.1 Description

Kristine lives in a small community wherein a number of coffee shops offer Wi-Fi accounts to their loyal customers. Her phone is subscribed to Smarty networks and is not affiliated to any Wi-Fi 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 Wi-Fi account.

5.7.2 Background

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

5.7.3 Sequence of Events



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

5.8 Visited (3G) to Wi-Fi (Provider) with Service Agreement

User decides to switch from 3G, which is provided by the visited operator, to Wi-Fi

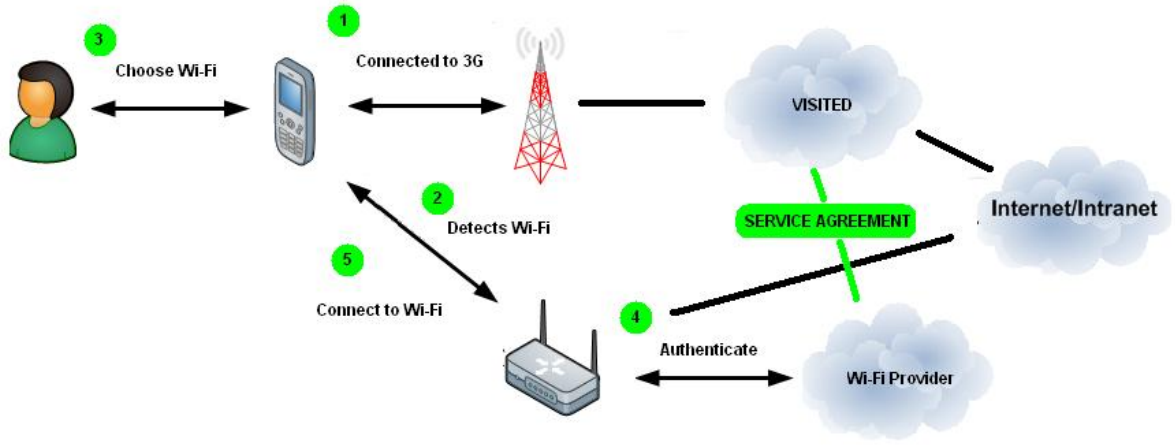
5.8.1 Description

Louella is heavy internet user and prefers to use Wi-Fi to connect whenever she can. She's subscribed to PingPing, a Wi-Fi provider available in a lot of 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 Wi-Fi services, she opts to use Wi-Fi and starts to check her emails.

5.8.2 Background

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

5.8.3 Sequence of Events



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

5.9 Visited (3G) to Wi-Fi (Provider) with No Service Agreement

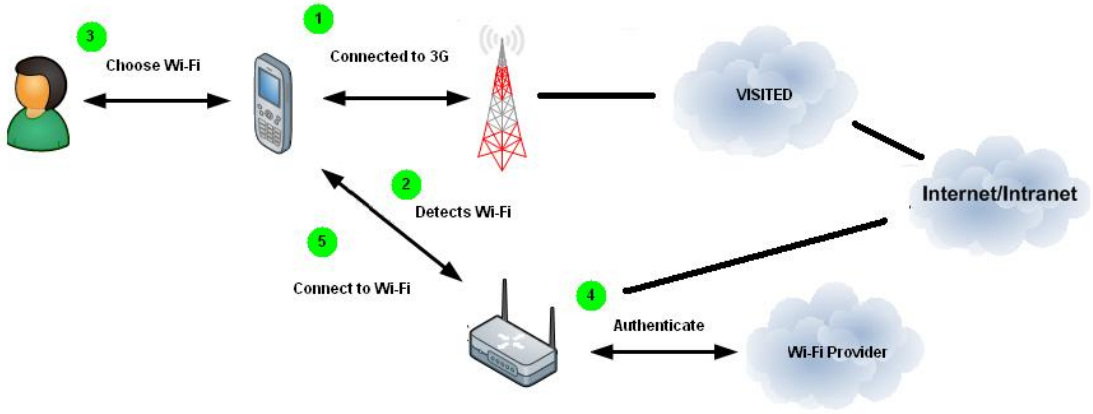
5.9.1 Description

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

5.9.2 Background

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

5.9.3 Sequence of Events



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

5.10 Device concurrently connected with cellular network and WLAN

5.10.1 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 with regards to the offloaded traffic should not be affected, therefore the quality of the WLAN link needs to be taken into account.

5.10.2 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.

5.10.3 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. Wi-Fi network is detected.
4. Mobile device is authenticated and authorized to use the Wi-Fi network.
5. Mobile device is now connected to the Wi-Fi network while keeping the connection with cellular network.
6. (optionally) Mobile device checks that Wi-Fi 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 Wi-Fi and uses the cellular network for all the other traffic.

6 Annex – Usability Use Cases

6.1 Use Case: Connect to a Home Service Provider's hotspot with no intervention

6.1.1 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.

6.1.2 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.

6.1.3 Sequence of Events

1. The mobile device scans and detects a home SP's hotspot in the area.

a) The hotspot's connection policy is assessed by the mobile device's connection manager.

b) The connection manager determines that the mobile device has the needed credentials to connect to the hotspot.

c) Based on the connection policy, the connection manager decides on the specific actions needed in order to connect to the hotspot.

d) 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.

6.2 Use Case: Connect to a HSP hotspot with no intervention

6.2.1 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.

6.2.2 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.

6.2.3 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.

6.3 Use Case: Informed Network Selection based on Network Information when in several Hotspots

6.3.1 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. But 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.

6.3.2 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.

6.3.3 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.

6.4 Use Case: Informed Network Selection based on HSP policies when in several Hotspots

6.4.1 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 Wi-Fi 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. But the mobile device is within the range of two Wi-Fi providers, iBonanza and his Home SP. But 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.

6.4.2 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.

6.4.3 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

6.4.4 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. So 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.

6.4.5 Background

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

6.4.6 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.

6.5 Use Case: Network Hierarchy and Selection

6.5.1 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 Wi-Fi 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 Wi-Fi enabled broadband router which is managed by the residential owner.

6.5.2 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.

6.5.3 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 Wi-Fi APs or thru cellular networks.
3. The residential (private) Wi-Fi hotspot will be chosen as the preferred delivery network.
4. User can now watch his/her favourite TV show

6.6 Use Case: Manual Provisioning and Online sign-up

6.6.1 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 doesn't 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.

6.6.2 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.

6.6.3 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

6.7 Use Case: 3G/Wi-Fi Mobility

6.7.1 Description

Leigh wanted to cruise the city. Knowing the city is blanketed with Wi-Fi 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 Wi-Fi antenna to a 3G lettered icon. Upon entering the next expressway exit, she again hears a beep and blinking icon from 3G to Wi-Fi. She continues her cruising adventure in the next city with her streaming music in the background.

6.7.2 Background

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

6.7.3 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.

6.8 Use Case: WPS

6.8.1 Description

Liza got her new mobile device with Wi-Fi capability. Upon getting home she happily opens up the device and tries to connect to her Wi-Fi home network. Her device prompted for the pre-shared key to access the network. She totally forgot about her pre-shared key and didn't 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 Wi-Fi 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.

6.8.2 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.

6.8.3 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

6.9 Use Case: Wi-Fi Management APIs

6.9.1 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.

6.9.2 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 Wi-Fi capabilities. This alleviates vendors from implementing varying and often conflicting needs of different operators.

6.9.3 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.

6.10 Use Case: Status Information, Function Accessibility, Power Management

6.10.1 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 Wi-Fi for customers. She turns on the Wi-Fi radio in one click on the device home screen and starts to use the Wi-Fi to watch videos. She noticed the Wi-Fi 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 Wi-Fi and enable battery saving.

6.10.2 Background

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

Some smartphones have one-click implementations of turning off the Wi-Fi 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 Wi-Fi radio or checking what is the status of their connection. Having a more cohesive usability behaviour and interface generally benefits the user.

6.10.3 Sequence of Events

1. User turns on Wi-Fi 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 Wi-Fi from the device interfaces.

6.11 Use Case: Connecting to Corporate VPNs

6.11.1 Description

Rea was on vacation and was called by a colleague to quickly reply to critical mail sent to her inbox. She brings out her device and starts connecting to the corporate network. The mail server she is trying to access is behind a corporate firewall accessible only through VPN. She starts the VPN software then puts in the settings, then keys her username and password. She goes to the corporate web page where she clicks on her webmail. She logs in, proceeds to read and answer the emails, then closes off her browser.

6.11.2 Background

Some smartphones today already support capability to connect to VPNs. The intent of this use-case is to illustrate the need for VPN connectivity for secured corporate networks to use internal systems. Though they already exist, a more intuitive means to connect and manage VPN connectivity can add ease to its use.

It is understood that installation of the VPN software is out of scope of this document.

6.11.3 Sequence of Events

1. Device is initiated to connect to a network using VPN.
2. Initial handshake and security parameters are exchanged by the device and network.
3. User keys in VPN settings, or may skip these if cached by the device.
4. User inputs his/her username and password.
5. Network authorizes and establishes the VPN connectivity.
6. User starts using internal corporate systems.
7. User logs off and device terminates the VPN connection.

6.12 Use Case: Child-safe Online Content

6.12.1 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 that she's 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 Wi-Fi. She tries to browse the link given to her but was still unable to do so.

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

6.12.2 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.

6.12.3 Sequence of Events

The following is the sequence for this use case:

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 Wi-Fi 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.

6.13 Use Case: Advice of Charge

6.13.1 Description

Later that day, Karenina's brother sent her a chat message that he needed some airtime load to be able to call up some friends. She then sends a text message to a special operator number with the amount and mobile number of her brother. The system then replies back indicating she will be charged for the transaction. She then replies with "Y" and receives confirmation the transaction has been successful.

6.13.2 Background

The intent of this use-case is to illustrate some scenarios that advise of charges and is currently used by some operators. These additional requirements are necessary depending on the government organization or a regulatory body in the region.

Some regions prescribe or require an advice of charge to subscribers. Notifications may be in the form of pop-up screens or SMS messages to the user to notify of the charge to the subscriber.

6.13.3 Sequence of Events

1. User tries to avail an optional service from an operator.
2. Operator application prompts the user transactions may be charged.
3. User accepts and proceeds on using the service.

6.14 Use Case: Quality of Service Access managed by the network

6.14.1 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 Wi-Fi, 3G, and 4G bearers. Charles wants in particular to watch his video in live streaming.

6.14.2 Background

The throughput on Wi-Fi 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: 2 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

6.14.3 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 Wi-Fi 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	18th December 2012	Removed section 3.13 including the requirements for 802.11v with no underlying certification ready for it; updated ToC. Clarified distinction between EAP-AKA and EAP-AKA'.	Terminal Steering Group	Stephen McCann, RIM

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@gsm.org your comments or suggestions & questions are always welcome.

.