P-HEVOR - System Requirements and Architecture

by NGMN Alliance

Version:	**0.12**
Date:	**February 11, 2013**
Document Type:	**Final Deliverable (approved)**
Confidentiality Class:	**P - Public**
Authorised Recipients: (for CR documents only)	

Project:	**HEVOR**
Editor / Submitter:	**Jan Ellsberger (Ericsson)**
Contributors:	**Jean-Pierre Charles (Project Lead, FT/Orange)** **Jan Ellsberger, Henrik Voigt (Ericsson)** **Laurent Thiebault, Peretz Feder (Alcatel-Lucent)** **Patrick Marsh (NSN)**
Approved by / Date:	**NGMN Board 20th March 2013**

Abstract: Short introduction and purpose of document

The purpose of this document is to define system level requirements for cellular operator integration of Wi-Fi access networks.

Document History

Date	Version	Author	Changes
10/05/2012	V0.1	Ellsberger, Jan – Ericsson	Proposed table of content
02/07/2012	V0.2	Ellsberger, Jan – Ericsson et al	Incorporating contributions from FT/Orange (JPC), ALU (LT, PF), NSN (PM),
28/08/2012	V0.3	Ellsberger, Jan – Ericsson et al	Incorporating additional input from ALU (PF).
24/09/2012	V0.4	Ellsberger, Jan – Ericsson et al	Incorporating additional input from ALU, new text proposed for sections 3, 5 and 6.
27/9	V0.5	Henrik Voigt et al	Updated with comments made during review call
17/10	V0.6	L. Thiébaut	Updated as per AP from CC on Sept 26th
24/10	V0.7	L. Thiébaut – ALU	Updated as per CC on Oct 17th
29/10	V0.71	Peretz Feder – ALU	Update per 10/29 CC
29/10	V0.72	Patrick Marsch – NSN	Updated with additional comments
29/11	V 0.8	Jan Ellsberger – Ericsson	Clean version after 29/10 CC
29/11	V 0.8.1	Jan Ellsberger – Ericsson	Proposed updates for discussion.
13/12 2012	V 0.9.0	Jan Ellsberger – Ericsson	Updates after 3/12 CC, incorporating ALU proposals submitted as input to 3/12 CC + Ericsson proposal for section 5.1.6.
14/12 2012	V 0.9.1	Jan Ellsberger – Ericsson	Incorporating comments/corrections received by e-mail from ALU.
14/12 2012	V 0.10	Jan Ellsberger – Ericsson	Incorporating modifications discussed in 14/12 CC.
8/1 2013	V 0.11	Jan Ellsberger – Ericsson	Final version for approval
11/02/2013	V0.12	Jean-Pierre Charles – orange	Deletion of last bullet of §3.2.3.7

Contents

1 INTRODUCTION AND SCOPE

The purpose of this document is, based on the companion deliverable on Wi-Fi use cases, to derive system level requirements for cellular operator integration of Wi-Fi access networks. The system level requirements are mapped onto on-going standardization activities with the objective to identify any gaps, and conclude with recommendations on standardization and industry activities.

2 SYSTEM REQUIREMENTS

The following system requirements are derived from the scenarios and use cases described in "P_HEVOR Use Cases" [D2],

- For operator integrated managed Wi-Fi:
  - Optimal QoE and network utilization
  - IP session continuity between 3GPP and Wi-Fi access
  - Policy control support and integration with 3GPP PCC, including QoS control in the Wi-Fi network
  - Automatic access selection under operator control (e.g. policy provided via ANDSF or other mechanisms (e.g. RFSP) depending on required dynamicity).

- For operator/shared managed Wi-Fi:
  - Optimal QoE and network utilization
  - IP session continuity between 3GPP and Wi-Fi access, for selected sessions (based on ANDSF)
  - Policy control support and integration with 3GPP PCC ; including QoS control in the Wi-Fi network
  - Support for operator-controlled access selection based on static and/or dynamic policies. Following alternatives are possible: 1) Manual selection, 2) automatic selection based on policies downloaded on the UE (e.g. via ANDSF) 3) Manual selection but constrained by policies downloaded on the UE (e.g. via ANDSF)

- For un-managed Wi-Fi (not further discussed in this document)
  - Nomadicity with possible change of IP address

3 STANDARDIZATION ACTIVITIES

3.1 Relevant Standardization Bodies and Fora

3.1.1 IEEE-SA

With an active portfolio of nearly 1,300 standards and projects under development, IEEE-SA Institute of Electrical and Electronics Engineers – Standards Association) is a developer of industry standards for a wide range of technologies : computer technologies, wired and wireless, power electronics, communications, instrumentation and measurements, healthcare IT, etc. Especially IEEE defines the radio interface for Wi-Fi (802.11)

3.1.2 3GPP

The 3rd Generation Partnership Project (3GPP) unites six telecommunications standards bodies, known as Organizational Partners (ARIB, ATIS, CCSA, ETSI, TTA and TTC) and provides their members with a stable environment to produce the highly successful Reports and Specifications that define 3GPP technologies (GSM, UMTS and now LTE) for PLMN.

3.1.3 Wireless Broadband Alliance (WBA)

The Wireless Broadband Alliance (WBA) was established in 2003 by a group of telecom operators as a global forum for wireless broadband ecosystem. With representatives from international broadband, cellular and integrated operators, the founders viewed Wi-Fi as an integral and strategic complement to other wireless and

broadband networks such as 3GPP/UMTS, WiMAX, DSL, Cable, and more. WBA has developed a diverse range of technical enablers (WISPr 2.0) and commercial frameworks, including the award-winning WRiX (Wireless Roaming Intermediary Exchange).

3.1.4 GSM Association (GSMA)

The GSM Association (GSMA) is an association of mobile operators and related companies devoted to supporting the standardizing, deployment and promotion of the GSM mobile telephone system. The GSM Association was formed in 1995.

3.1.5 Small Cell Forum

The Small Cell Forum is a not-for-profit membership organization which seeks to enable and promote small cell technology worldwide. In February 2012, the Femto Forum was renamed the Small Cell Forum in order to better reflect its work which embraces now residential, enterprise, metro and rural small cells.

3.1.6 Wi-Fi Alliance (WFA)

The Wi-Fi Alliance is a global non-profit industry association of companies devoted to seamless connectivity. With technology development, market building, and regulatory programs, the Wi-Fi Alliance has enabled widespread adoption of Wi-Fi worldwide and has been one of the driving forces behind Hotspot 2.0.

The Wi-Fi CERTIFIED™ program was launched in March 2000. It provides a widely-recognized designation of interoperability and quality and it helps to ensure that Wi-Fi-enabled products deliver the best user experience. Wi-Fi®, Wi-Fi Alliance®, WMM®, Wi-Fi Protected Access® (WPA), the Wi-Fi CERTIFIED logo, the Wi-Fi logo, the Wi-Fi ZONE logo and the Wi-Fi Protected Setup logo are registered trademarks of the Wi-Fi Alliance.

3.1.7 Global Certification Forum (GCF)

The Global Certification Forum (GCF) is an independent certification scheme for mobile phones and wireless devices that are based on 3GPP standards.

3.2 Status of developments regarding Cellular/Wi-Fi Interworking

3.2.1 Overall Requirements

Wi-Fi can be used in a seamless way by a 3gpp UE if solutions are deployed to provide:

- Network Selection: Assist the UE to automatically select suitable Wi-Fi Access Points (using ANDSF rules and Wi-Fi Standards features advertised as part of WFA Hot Spot 2.0 specifications)
- Automatic Authentication Procedures: Support for 3GPP EAP methods to authenticate on the Wi-Fi network using the strong USIM based security.
- Session Mobility: When needed, the UE and network should support seamless mobility between 3GPP and Wi-Fi coverage that preserves the IP address / Prefix allocated to the UE.

3.2.2 IEEE SA

This section outlines projects on-going under IEEE-SA.

IEEE802.11 Wireless Local Area Networks

The IEEE802.11 has just finished its revision project for the IEEE802.11 base standard, which led to the publication of the IEEE802.11-2012 standard. IEEE802.11-2012 includes all previous amendments up to the letter ‘z’, i.e. IEEE802.11n-2009 is incorporated in IEEE802.11-2012.

Currently on-going projects leading to further enhancements of IEEE802.11 for heterogeneous networking are:

P802.11ac: Very High Throughput < 6GHz (Planned completion: 2013)

P802.11ah: Sub 1 GHz license-exempt operation (Planned completion: 2014)

P802.11ai: Fast Initial Link Set-Up (Planned completion: 2013)

IEEE1905 Convergent Digital Home Working Group

P1905.1: Standard for a Convergent Digital Home Network for Heterogeneous Technologies

The standard defines an abstraction layer for multiple home networking technologies. The abstraction layer provides a common data and control Service Access Point to the heterogeneous home networking technologies described in the following specifications: IEEE P1901, IEEE 802.11, IEEE 802.3 and MoCA 1.1. The standard is extendable to work with other home networking technologies.

Planned completion: 2013

IEEE2200 High Quality Mobile Experience Working Group

P2200: Standard Protocol for Stream Management in Media Client Devices

This standard will define reference architectures and interfaces for intelligently routing and replicating content over heterogeneous networks to portable devices with local storage, without disrupting content providers' direct relationship with end users.

Planned completion: 2013

3.2.3 3GPP

3.2.3.1 I-Wi-Fi

The Wi-Fi Interworking (I-Wi-Fi) architecture has been introduced in 3GPP Release 6. This architecture is mainly based on two new services and components:

- USIM based Authentication and Authorization to access a Wi-Fi access: a AAA server authenticates a Wi-Fi UE based on USIM credentials and sends authorization data to the Access network that will serve this UE.
  - Over Wi-Fi, the authentication mechanism is similar to the existing USIM-based mechanism over 3GPP radio.
  - The AAA server is linked to the HLR/HSS through a new interface allowing to fetch security credentials as well as authorization data
- Wi-Fi access to PLMN IP services: a Packet Data Gateway (PDG) terminates a 3gpp based VPN between the 3gpp UE and a PLMN, and provides access to PLMN based IP services (service equivalent to that of a GGSN but without mobility)
- The 3gpp based VPN provides security over any un-secured Wi-Fi access[1] but requires a specific IKE implementation in the UE and requires the network to support one IPSec tunnel per UE

[1] This architecture provides no mobility between 3gpp access and Wi-Fi.

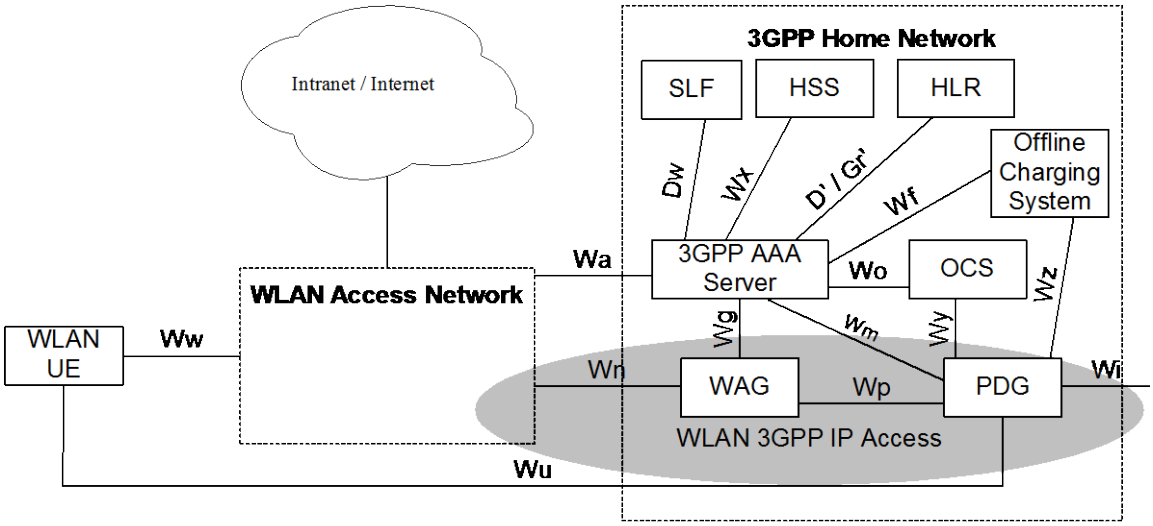

Figure 1 : I-Wi-Fi architecture

For Wi-Fi UE, the authentication mechanism is similar to the existing SIM-based mechanism for non-Wi-Fi 3GPP UEs. The AAA server is linked to the HLR/HSS through a new interface called Wx.

3.2.3.2 EPC Architecture

The EPC architecture has been designed to not only provide support both legacy (2G/3G) and LTE access, but also to provide support for access to mobility with non-3GPP access (e.g. Wi-Fi). Support of non-3GPP access is described in 3GPP TS 23.402 [FFS].

Two kinds of access network, un-trusted and trusted[2] are defined by 3GPP TS 33.402 [FFS]:

- "When all of the security feature groups are considered sufficiently secure by the home operator, the non-3GPP access is identified as a trusted non-3GPP access for that operator."
  - Procedures allowing to consider Wi-Fi as a Trusted Access are only defined as part of 3GPP Rel11 specifications, refer to §4.2.3.6
- "When one or more of the security feature groups is considered not sufficiently secure by the home operator, the non-3GPP access is identified as an un-trusted non-3GPP access for that operator." In this case, the UE has to establish an IPsec tunnel to the ePDG by conducting IKEv2 with EAP-AKA' for UE authentication.

[2] 3GPP specifications do not dictate whether a non 3GPP access technology (Wi-Fi, WIMAX,...) is to be considered as trusted or non trusted as whether a non 3GPP access is to be trusted is determined by the Home operator of the user based on operational conditions.

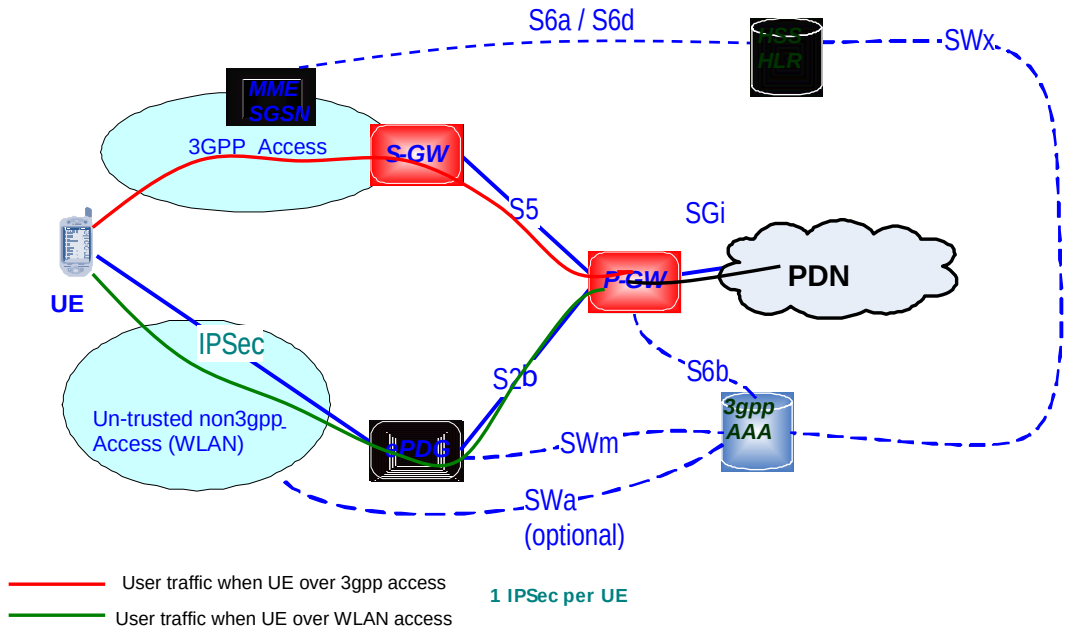

Figure 2: 3GPP/Non-3GPP interworking architecture (3gpp Rel8/9 EPC)
NOTE: Only the cased of Network Based mobility with an Un-trusted non 3gpp access shown

3GPP TS 23.402 allows two IP mobility management mechanisms for non-3GPP access:

- NBM: Network based mobility (S2a, S2b interfaces): S2a / S2b rely on protocols such as GTP or PMIPv6 terminated in network entities managing mobility in the access network.
- HBM: Client/Host based mobility (S2c interface): S2c relies on DSMIPv6 mobility signaling terminated in the UE. It doesn't rely on any specific characteristic of the access network/technology.

The mobility between 3gpp and non-3gpp accesses is always UE-initiated. As the UE moves between Wi-Fi and 3gpp coverage, it may indicate that it is a "Handover" related request. The Handover indication ensures that the P-GW will be kept as local mobility anchor and that the IP address of the session is preserved, thereby enabling mobility without interrupting the existing session.

The Authentication, Authorization and Accounting (AAA) server performs UE authentication based on USIM credentials and accesses the Home Subscriber Server (HSS) through SWx interface to get subscriber's information and security credentials. The authentication relies on EAP-AKA[3] and the authorization data may contain the P-GW serving the UE over 3GPP coverage.

Finally, S6b interface is used to indicate to the HSS via the AAA server the P-GW selected (allowing re-using the same P-GW when the UE moves to a 3gpp access).

The relative priorities between Radio Access Technology (Wi-Fi/3GPP) may be controlled by ANDSF based rules (refer to §4.2.3.5).

[3] EAP-AKA' method is defined by IETF RFC 5448

3.2.3.3 MAPCON & IFOM

When the subscriber happens to be under Wi-Fi coverage, it is beneficial for the operator to offload some traffic to the Wi-Fi access. At the same time it may be beneficial to still keep some traffic (e.g. VoIP flow) over the cellular access. 3GPP Rel 10 defines following enhancements to the 3GPP core packet network for UE able to simultaneously use 3GPP and Wi-Fi radio for IP traffic:

- **MAPCON**, provides a selective transfer of PDN connections between accesses: the UE may transfer only a subset of the active PDN connections from the source to the target access. This allows at 3GPP to Wi-Fi mobility to e.g. keep the PDN connection for VoIP/IMS over 3GPP and to move only the PDN connection for HSI/Internet/VPN over Wi-Fi. MAPCON does not require the UE to support client-based MIP (DSMIPv6 aka S2c). Conversely, it implies that the UE manages more than one PDN connection i.e. more than one IP address.

Which APN may/should/shall use which Radio Access Technology may be controlled by ANDSF based rules (refer to §4.2.3.5).

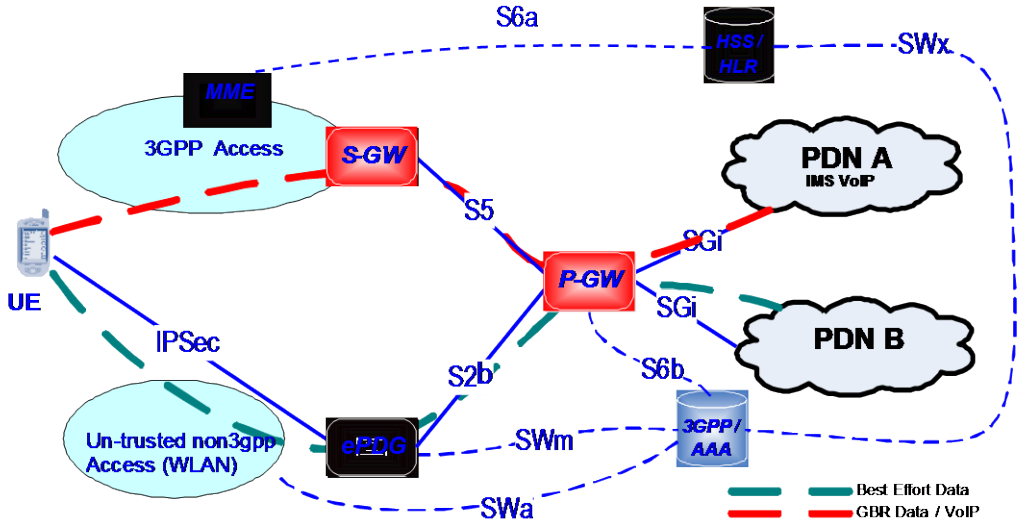

Figure 3: MAPCON architecture

- **IFOM**[4] provides the capability for 3GPP terminals to access a PDN connection via a Wi-Fi access, while maintaining connectivity to the same PDN connection (IP address) via the 3GPP radio. IFOM permits individual flows to the same PDN connection to be routed over different access based on network policy; for example, best-effort traffic may be routed over Wi-Fi while QoS-sensitive traffic such as voice telephony may be routed only over the 3GPP radio. Current definition of IFOM requires the UE to support a DSMIPv6 stack which may be a hurdle for its deployment.

[4] Specified in 3gpp 23.261 []

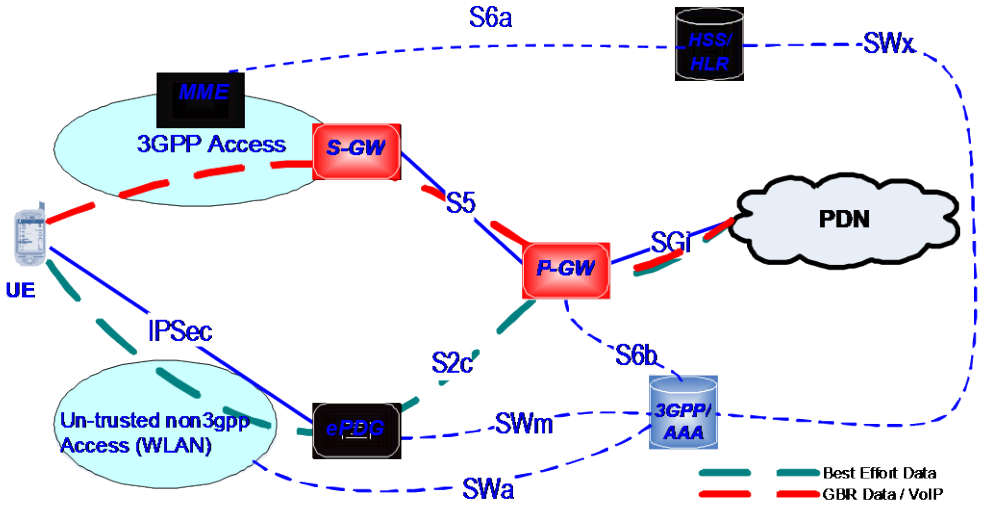

Figure 4: IFOM architecture

Which IP flow may/should/shall use which Radio Access Technology may be controlled by ANDSF based rules (refer to §4.2.3.5).

3.2.3.4 Non-seamless Wi-Fi Offload

Non-seamless Wi-Fi offload can offload the mobile core network of certain traffic such as Internet traffic. The break-out is usually done at the Wi-Fi access. The UE, based on user settings, external triggers and ANDSF policies, can route specific IP flows via the Wi-Fi access without traversing the EPS. For performing the non-seamless Wi-Fi offload, the UE needs to acquire a local IP address on Wi-Fi access, and it is not required to connect to an ePDG.

Which IP flow may/should/shall use NON Seamless Wi-Fi offload may be controlled by ANDSF based rules (refer to §4.2.3.5).

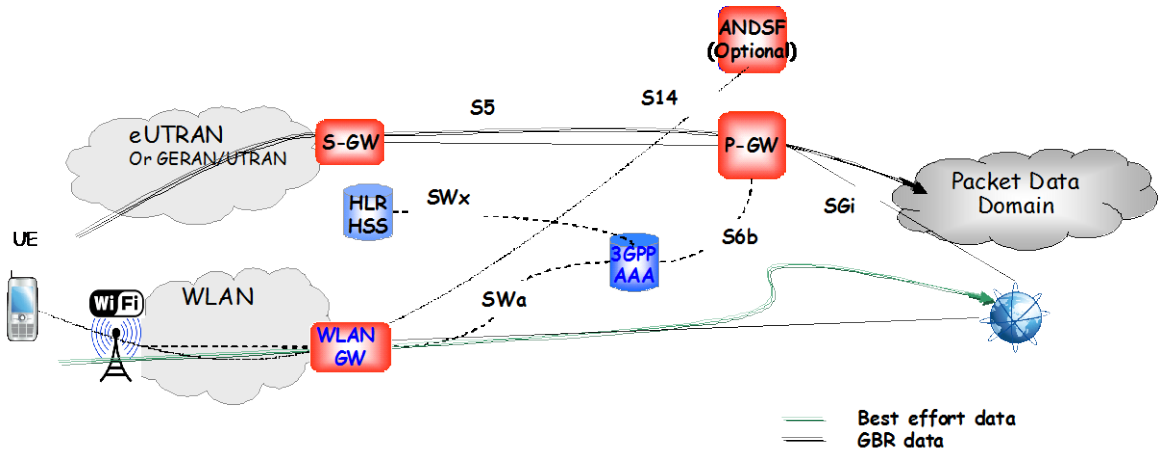

Figure 5: Non-seamless Wi-Fi offload

3.2.3.5 ANDSF

The Access Network Discovery and Selection Function (ANDSF) provides the UE with (non 3gpp) network discovery and selection assistance data as per operators' policy. It is defined in 3GPP TS 23.402. The ANDSF information is represented by ANDSF Management Object described in 3GPP TS 24.312 [FFS], an XML document compatible with OMA-DM standards. This XML document may specify following types of information:

- Mobility policies: prioritized rules that control which network (3GPP, Wi-Fi/SSID, WiMax …) should be used by an UE. Each rule defines a location and a time when a particular access network can be used.
- Discovery information allows the mobile device to map from its current location to a list of alternative access networks that may also be available. For example a list of Wi-Fi access networks within the current 3GPP cell or LTE traffic area.
- (3gpp Rel10): ISRP that control the MAPCON, the IFOM and/or the NON Seamless Wi-Fi offload features.

3.2.3.6 Access to EPC over Trusted Wi-Fi

Pre 3GPP Rel11 specifications include 2 main deployment scenarios to access to the EPC from Wi-Fi:

- "Non Trusted Non 3GPP Access to EPC": to maintain trust, the UE has to establish a dedicated VPN access to the EPC. This VPN is specific to 3GPP networks. For each UE, at least one such VPN connection is established over Wi-Fi towards the ePDG.
- "Access to EPC with Host Based Mobility": in this scenario, the UE establishes a DSMIPv6 connectivity to the EPC mobility anchor (i.e. the P-GW) transparently over Wi-Fi. On top of DSMIPv6 support in the UE, this again requires the support of at least an IPsec tunnel between the UE and the network.

Fulfilling such requirements is not an easy task for the UE and up to now very few terminals supports one of these features. This means that traffic sent by UE over Wi-Fi escapes from the mobile operator and that operator cannot really sell a service that spans over both 3GPP and Wi-Fi radios.

It has further to be noted that requiring UE to set up a VPN to access to the EPC

- Is costly for the operator as it implies the support of an IPsec tunnel per UE, thus requires the deployment of costly nodes that terminate a large number of IPsec tunnels
- May imply the support of nested VPN (a corporate VPN within the 3GPP VPN) when the UE uses the access to EPC to set up a VPN to the corporate network of the user which may not be supported by terminal operating systems.

As part of 3gpp Rel11, 3gpp has defined procedures allowing usage of Wi-Fi as a trusted non 3gpp access to EPC, allowing thus to connect to the EPC without the burden of establishing a dedicated 3GPP VPN or a DSMIPv6 link with the network.

The solution is based on the observation that in many cases the Wi-Fi AN is either directly owned by the mobile operator or controllable via a partnership agreement and so at least one SSID on the AN may be configured to meet the 3GPP requirements for "trusted" non-3GPP.

The solution requires the Trusted Wi-Fi to terminate:

- Security per IEEE 802.11 2007 profile (previously called 802.11i). This entails support of the strong EAP(AKA) based authentication and of strong AES based ciphering over Wi-Fi radio.
- A AAA interface ("STa") e with a 3gpp AAA server to support UE authentication as well as retrieval of user Authorization data.
- A S2a interface with the P-GW where each user session is mapped to a GTP or PMIP session to a P-GW (similar mapping as enforced in a SGW or an ePDG).

These interfaces and features are very similar to the interfaces and features of an ePDG with the difference that the secured interface with the UE does not rely on an IPSec tunnel per UE but on a Wi-Fi secured interface per UE.

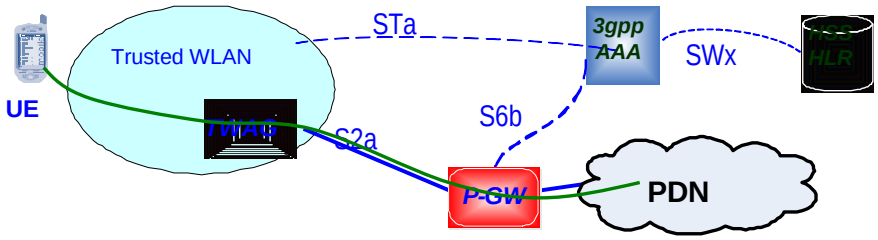

Figure n: Architecture with Trusted Wi-Fi access to EPC

The 3gpp work for Rel11 targets only "non-modified" UE (i.e. is aimed at working with legacy UE) which means support of following function is not defined by that version of the specification:

- IP address preservation when moving between 3GPP and Wi-Fi.
- Telling the network which APN (Access Point Name) is targeted (the APN to be used over Trusted Wi-Fi is defined as part of Authorization data retrieved from the 3gpp AAA server).
- Multiplexing over Wi-Fi traffic targeting different APN or Multiplexing over Wi-Fi traffic targeting the EPC and traffic corresponding to non-seamless offload.

3.2.3.7 Foreseen 3GPP Rel-12 Improvements

Following features are studied (and some of them may be defined) as part of 3gpp Rel12

- Remove some or all the limitations of the Rel11 Trusted Wi-Fi solution
- Ensure the proper inter-working between 3gpp network selection, Wi-Fi selection per ANDSF rules and PLMN selection over Wi-Fi
- Possibly leverage information advertised by Hot Spot 2.0 for Wi-Fi selection by a 3gpp UE
- Possibly have ANDSF rules that distinguish between various 3gpp Access Types (2G, 3G and LTE)
-

3.2.4 Small Cell Forum

The Small Cell Forum group has recently edited a white paper on "Integrated Femto-Wi-Fi (IFW) networks" (index number: 033 – February 2012). This document provides comprehensive view of the use cases, scenarios and challenges that integrated femto-Wi-Fi (IFW) devices and networks are, or may be facing in residential, enterprise and metro deployment. It also intends to address some technical background around IFW architectures, IFW mobility, and related technical details as well as standard development and requirements.

3.2.5 Wi-Fi Alliance and IEEE 802.11u

3.2.5.1 HotSpot 2.0

The Wi-Fi Alliance has created a new standards activity, Hotspot2.0 and released a technical specification for Wi-Fi Alliance (WFA) that defines a set of protocols that facilitate WFA Hotspot 2.0 operation. Requirements for HS 2.0 are provided by the WFA Marketing Requirement Document (MRD) developed by the WFA Marketing Working Group. The requirements list is still under development and as of this writing, continues to expand. HS2.0 solution for next generation hotspots is expected to specify at least three releases where the development of the first

release was completed in 1Q 2012. Presently HS 2.0 Release 2 is under development and expected to complete at the end of 2012. Among the agreed Release 1.0 requirements, HS2.0 improves the ability of Wi-Fi devices to discover and securely connect to public Wi-Fi hotspots, thereby enabling easier roaming between public Wi-Fi networks. Release 2 of HS2.0 will provide online signup protocol and policy provisioning.

The WFA launched a certification program for access points and devices that comply with HS 2.0 releases. Products that completed and successfully passed the HS 2.0 tests are labelled Wi-Fi Certified Passpoint Release x products (where x=1,2,3). The Passpoint certification program will offer users a consistent streamlined Wi-Fi hotspot connection process and support the use of one set of account credentials for multiple hotspots. It will further allow service providers to ease data offload and enable roaming agreements making Wi-Fi a true extension of service provider networks.

In addition, WFA will publish in 2Q 2012 Passpoint Release 1 Deployment Guide. The purpose of the deployment guide is to provide additional guidelines and recommended best practice for deployment features which are part of the Passpoint Release 1 certification. The deployment guideline provides Release 1 reference architecture, security recommendations, configuration and provisioning recommendation for hotspot access network equipment including ANQP server (see below) and mobile devices.

The Hotspot2.0 work builds on the recently ratified IEEE 802.11u specification, which provides query mechanisms to/from ANQP Server. The ANQP server is an advertisement server defined in IEEE 802.11u and located as a functional entity in the Passpoint Hotspot Operator's network. The query mechanism enables Wi-Fi devices to discover information about the available roaming partners, link and connection characteristic, home realms and type of credentials which may be used with the access point.

The HotSPot 2.0 Release 1 ANQP defined elements include:

- Network authentication Type Information (list of supported authentication methods)
- Roaming Consortium List
- NAI Realm List (list of SSPs whose networks or services are accessible via the HS)
- 3GPP Cellular Network Information (for HSs having roaming agreements with cellular SPs)
- Domain Name List (one or more domain names of the entity operating the HS)
- HS Query List (list of HS2.0 identifiers for which the device is providing ANQP query)
- HS Capability list (information and capability configured in the AP)
- Operator Friendly Name (zero or more operators of the 802.11 AN)
- WAN Metrics (link characteristics and loading conditions)
- Connection Capability (connection status of the commonly used protocols and ports)
- NAI Home Realm Query (realms of which the device has security credentials)
- Operator Class Indication (group of channels in the frequency band the Wi-Fi AN sis using)

Typically, HS2.0 mobile device will discover and select a hotspot operated by its Home SP or a partner. The obtained Domain Name list will be matched to the FQDN associated with the provisioned device credentials. A mobile device provisioned by a cellular provider, can use a domain name that is generated from the obtained PLMN ID to identify its home SP.

Hot Spot 2.0 incorporates the long ratified IEEE 802.11i based WPA2 Enterprise security specification which enables secure authentication and encryption for Wi-Fi data using a variety of user credentials including (U)SIM, digital certificates and username/passwords.

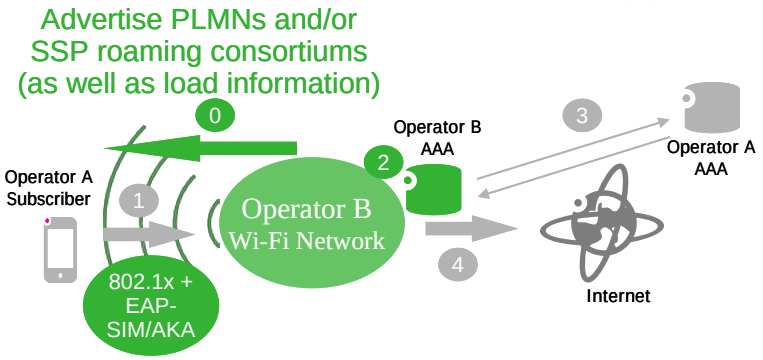

Figure 6: Hot Spot 2.0 Access Principles.

3.2.5.2 IEEE 802.11u

IEEE 802.11u, which provides the HS 2.0 building blocks, is an extension to the IEEE 802.11 standard to improve the ability of devices to discover, authenticate, and use nearby Wi-Fi access points. IEEE 802.11u introduced the concept of Subscription Service Provider (SSP), which is the entity responsible for managing the user's subscription and associated credentials. Multiple SSPs are typically accessible through a single access point, reflecting the various roaming relationships. The SSP concept is a key to enabling easier Wi-Fi roaming as it breaks the relationship between the SSID and the access credentials. Instead, devices dynamically query which SSPs are accessible via the AP, irrespective of the SSID(s) that the AP is broadcasting. This allows Wi-Fi devices to automatically discover roaming agreements on access points it has never previously connected to.

IEEE 802.11u defined changes to the Beacon and Probe messages as well as a new Public Action Frame based Generic Advertisement Service (GAS) that allows unauthenticated devices to query an access point capabilities and supported SSPs before associating. Changes to the beacon and probe messages allow access points to broadcast their support for 802.11u for example, as well as for some broad roaming information such as Roaming Consortium OUI. A roaming consortium is a group of subscription service providers (SSPs) having inter-SSP roaming agreements. GAS enables devices to perform more detailed queries to the WFA Passpoint network often relying on ANQP elements that can be obtained from the ANQP server.

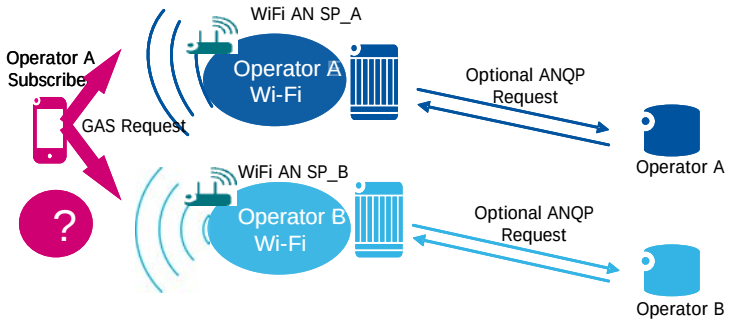

Figure 7: GAS Requested information provided through an optional ANQP server.

IEEE 802.11u also introduced Homogeneous Extended Service Set ID (HESSID). The HESSID identifier is used to identify a set of access points (BSS) that belong to the same network and which consequently exhibit common networking behaviour. It is the identifier of the network behind the Layer 2 wireless route and it should be used in

conjunction with SSID, which is the existing Wi-Fi radio access identifier. Both HESSID and SSID are therefore used together to discover a specific Wi-Fi and its network attachment. Coupled together, they provide a unique identifier for a Wi-Fi access network. If the HESSID parameter is not available in the HS2.0 hotspot, then the SSID is used only, as with current implementations. The HESSID is typically the value of the BSSID of one of the access points in that set. The HESSID is optionally present in the IEEE 802.11u beacon messages and so can be discovered prior to association.

IEEE 802.11 u Generic Advertisement Services (GAS) defines pre and post association queries and responses that can be formatted using a number of protocols; however, Passpoint networks will be using just the Network Query Protocol (ANQP). ANQP defines a number of standard Information Elements, which allow devices to query specific information such as location, cellular network roaming, emergency services support, authentication realms and so on. ANQP is also a two-way exchange enabling the Wi-Fi device to provide its values for these information elements to the access point or to an ANQP server during the exchange. As the 802.11 beacon/probe messages may be limited in size, ANQP allows the mobile device to query a longer list of roaming consortium identifiers. Thanks to the 3GPP Cellular Network Information Element, ANQP can also provide the list of PLMNs that can be accessed via the Passpoint Access Point.

In addition to improving the ability of devices to discover compatible Wi-Fi networks, IEEE 802.11u also provides extensions to the basic IEEE 802.11e QoS mechanisms to improve the ability of the Wi-Fi network to manage traffic for multiple SSPs. A Wi-Fi network, as part of the roaming agreement, can be provided with a QoS Mapping from the SSP which determines how downlink IP traffic classes should be mapped to the over-the-air IEEE 802.11 QoS traffic classes.

Also, a new QoS Action Frame message (QoS Map Configure) allows the AP to send this SSP specific QoS mapping definition to the device, thereby enabling the device to apply the QoS mapping to uplink IP traffic.

3.2.6 Wireless Broadband Alliance

The WBA has developed a set of specifications to facilitate commercial roaming between operators: WRIX (Wireless Roaming Intermediary eXchange). It includes WRIX-i (Interconnect), WRIX-d (Data Clearing) and WRIX-f (Financial Settlement). Each of these specifications can be deployed by Visited Network Providers (VNPs) and Home Service Providers (HSPs) either in-house or through an intermediary WRIX service provider. The latest release of WRIX version 1.04 includes support for EAP authentication providing the transport and indicating which radius attributes to use. This specification recommends Network operators support the following EAP methods: EAP-SIM, EAP-AKA, EAP-TLS, and EAP-TTLS. Other EAP methods may be supported transparently by the VNP but are not part of this specification.

WISPr 2.0 (March 2010): this specification contains release 2.0 of the Annex D “Smart Client to Access Gateway Protocol” defined in WISPr 1.0 best practices document which has been available in the public domain. WISPr 2.0 scope is limited to the specification of client software to public Wi-Fi network interface. The WISPr 2.0 is designed for “non” IEEE 802.1x networks as it requires IP communication with the Access Gateway prior to the authentication of the user. WISPr offers authentication services based on layer 3 networking. It is designed as a front-end to authentication protocols such as Radius, Diameter and the WBA WRIX specification

WiMAX to Wi-Fi interworking Function (December 2010): this specification is an addendum to the WRIX-i specification and defines the Interworking function to facilitate roaming between the Wi-Fi and WiMAX networks

WRIX-L (July 2009) defines the format and data the operators shall exchange for feeds of partner service locations. This specification includes both the file format and file exchange method. It clearly describes the Mandatory verses Optional fields in the WBA Location database so that there is uniformity of information across all the WBA Members.

In 2012, Wireless Broadband Alliance is conducting a trial on Next Generation Hotspot (NGH). The objective of this trial is to help the operators and vendors (device manufacturers, infrastructure providers & Hub providers) to join force and demonstrate the ability of Next Generation Hotspot capabilities primarily in operator networks.

The main objective of this trial according to WBA is the following:

- Run an end-to-end Wi-Fi international roaming trial using key NGH elements such as equipment supporting IEEE 802.11u, IEEE 802.1x Wi-Fi networks & EAP authentication methods
- Validate seamless interoperability across home and visited network operators using the draft specification under the new Wi-Fi Alliance CERTIFIED hotspot program;
- Open to invited operators, infrastructure providers, device vendors and roaming providers
- Provide a "real world" like test of the NGH specifications in as close to a production environment as feasible using many different types of Wi-Fi providers and third party connectivity providers to complete inter-carrier, secure, auto authentication
- Identify key items needed to upgrade home networks to support NGH capabilities while still supporting backward compatibility with legacy authentication methods.
- Identify implementation instructions on NGH roaming lifecycle from operator's perspective AND key requirements from a device/terminal aspect based upon learning's from the trial.

3.2.7 GSMA–WBA joint Wi-Fi Roaming taskforce

The GSMA and the WBA are collaborating to simplify connectivity to Wi-Fi hotspots from mobile devices such as smartphones or tablets. This joint initiative (Wi-Fi Roaming initiative) is developing technical and commercial frameworks for roaming. The work in this joint initiative is now progressing on definition of guidelines for security, billing, data offload, device implementation and network selection to create a consistent solution for WBA and GSMA members. A first white paper was issued during phase 1 by this joint task force : Wi-Fi Roaming White paper version 1.0 (December 2nd, 2011). This document is confidential. The following topics are analysed in this document and recommendations are provided for each topic:

- AAA and security aspects
- Roaming and billing aspects
- Terminal aspects
- Automated network discovery and selection

For phase 2, the joint Wi-Fi Roaming taskforce has identified the following topics :

- Handoffs / IP Address Preservation
- Support for QoS in Wi-Fi networks
- Service Control for non-internet type services
- Policy support in Wi-Fi network

4 MAPPING OF SYSTEM REQUIREMENTS TO STANDARDIZATION ACTIVITIES

This section describes the standardization status of different system requirements and identifies gaps as well as need for option pruning/profiling. System requirements described in Section 3 can be divided into the following categories.

- Charging
- Policy control and QoS
- Mobility
- Network discovery and selection
- Security and authentication
- Services

Note: Indication that some work is on-going, as part of 3gpp Rel12, may need to be revisited as the scope of 3GPP Rel12 has not been finalized yet (3GPP Rel12 architecture work deadline is December 2012).

4.1.1 Charging

- Available standards:
    - For cases where traffic is routed via EPC, e.g. using S2a, charging can be performed in the 3GPP domain per 3GPP specifications.

- 3GPP and BBF are cooperating on charging aspects for 3GPP-BBF interworking/convergence.
    - 3GPP specifications for 3GPP-BBF interworking also describe accounting aspects for traffic offloaded in Wi-Fi/fixed domain. The specifications for this have however not been fully completed. Further 3GPP work is on-going as part of 3GPP Rel12 P4C-F.
- Charging/accounting in Wi-Fi/fixed domain is partly proprietary, although descriptions of best-current-practice for RADIUS accounting have been developed by WFA (WISPr1.0).
- Work has been done by WBA and GSMA on specifications to facilitate commercial roaming between operators, including e.g. settlement aspects

- Overlap
    - None
- Gaps
    - In case of Trusted WI-FI access to EPC 3GPP Rel11 specifications do not support the capability to provide the PGW (and the charging entities) with the Identity of a TWAN operator that would be different from the local PLMN.

4.1.2 Policy control and QoS

- Available standards:
    - Policy control for traffic routed via EPC is provided using 3GPP PCC.
    - Policy control in Wi-Fi/fixed domain is to a large degree proprietary.
    - 3GPP and BBF cooperating on policy control aspects for 3GPP-BBF interworking/convergence
    - Wi-Fi standards for QoS include 802.11e as well as certification programs by Wi-Fi Alliance
- Overlap:
    - Thus far, separate and different policy control standards are defined by 3GPP, TISPAN, BBF etc.. Joint efforts of 3GPP and BBF are on-going (as part of P4C 3GPP Rel-12) to align Policy control between Wireline and Wireless.
- Gaps:
    - To support FL-RTC services in network integrated and shared Wi-Fi scenarios, there may be a need to better specify how Wi-Fi QoS mechanisms can be integrated with and utilized in integration with 3GPP PCC.
    - 3GPP and BBF have cooperated on Policy Interworking solutions between mobile 3GPP and BBF/fixed domains and this work was almost completed in Rel-11. However, in the case of Trusted Wi-Fi access to EPC, the mechanism of providing location information (e.g., geo-location info) from the Trusted Wi-Fi access to the PCC and charging entities is nevertheless still missing and being considered as part of 3GPP Rel-12 P4C-TC/P4C-TI future work.

4.1.3 Mobility

- Available standards:
    - For unmanaged Wi-Fi scenarios, overlay solutions (S2b and S2c) have been defined by 3GPP. For managed Wi-Fi scenarios, in network integrated and shared deployments, Wi-Fi integration using S2a can be used. These options include protocol variants (GTP and PMIP for S2a/S2b and DSMIP for S2c).
    - IEEE 802.21 includes handover signalling between heterogeneous networks and L2/L3 protocols to handle communication between the Point of Attachment (i.e. AP) and the Information Server.

- Overlap:
    - 3GPP defines multiple solutions (S2a, S2b, S2c) that are partially overlapping
- Gaps:
    - Pruning and recommendations of the options may be beneficial

- For network integrated and operator/shared Wi-Fi, the S2a-based solution needs further work in 3GPP and possible other bodies to support mobility between 3GPP access and Wi-Fi (work started in 3GPP rel-12)

4.1.4 Network discovery and selection

- Available standards:
  - For operator/shared Wi-Fi, ANDSF-based solution is defined by 3GPP ..
  - For loose coupling network integrated solution., , network discovery and selection policies are provided via the ANDSF. i.
  - IEEE 802.21 includes support for discovery and access selection mechanisms.
  - WFA is currently working on access selection based on HS2.0 policies.
- Overlap:
  - Overlap potentially exists between 3GPP and HS2.0 network/PLMN selection policies.

- Gaps:
  - For operator/shared scenarios, on-going work in 3GPP Rel12 (Wi-Fi network selection) addresses ANDSF enhancements, e.g. to benefit from capabilities provided by HS 2.0.
  - For network integrated scenarios, since ANDSF in its current form is not suitable for very dynamic policy updates or direct network control of access selection, an evolution thereof and/or other solutions allowing more dynamic RAT (3GPP/Wi-Fi) network selection should be considered.
  - 3GPP and WFA are encouraged to define how different network discovery and selection mechanisms can be used in a collaborative manner to complement each other.

4.1.5 Security and authentication

- Available standards:
  - 3GPP based access authentication using (U)SIM credentials defined since rel-6 (I-Wi-Fi) and rel-8 (EPC).
  - Wi-Fi Alliance HS2.0 certification, which is part of the Passpoint / HS2.0 development, ensures that UEs and APs claiming compatibility to Passpoint / HS2.0 include support for EAP based authentication and authorization using (U)SIM credentials (i.e. SIM, AKA, AKA').
- Overlap:
  - None identified.
- Gaps:
  - None identified

4.1.6 Services

- Available standards:
  - GSMA have developed specifications for IMS Voice and Video call over HSPA and LTE bearers (IR.92, IR.58, IR.94).
- Overlap:
  - None.
- Gaps:
  - For support of IMS Voice and Video call in network integrated Wi-Fi scenarios, further work in GSMA is needed.

5 CONCLUSIONS AND RECOMMENDATIONS

Based on the gaps and overlap identified in Section 5, the following conclusions and recommendations can be made:

- It is recommended that GSMA and WBA define the identity of a TWAN operator so that the identity may be provided to the charging entities in case the TWAN operator is different from the local PLMN. (See section 5.1.1).
- To support FL-RTC services in network integrated and shared Wi-Fi scenarios, it is recommended that 3GPP specifies how Wi-Fi QoS mechanisms can be integrated with and utilized in integration with PCC. (See section 5.1.2).
- A mechanism for providing location information (e.g. geo-location information) from the Trusted Wi-Fi access to PCC and charging mechanism is missing. It is recommended that 3GPP consider this aspect as part of future work. (See section 5.1.2).
- For network integrated and operator/shared Wi-Fi, it is recommended that 3GPP enhance the S2a-based solution to support mobility between 3GPP access and Wi-Fi (work started in 3GPP Rel-12). (See section 5.1.3).
- For network integrated scenarios, since ANDSF in its current form is not suitable for very dynamic policy updates or direct network control of access selection, an evolution thereof and/or other solutions allowing more dynamic RAT (3GPP/Wi-Fi) network selection should be considered (See section 5.1.4).
- 3GPP and WFA are encouraged to define how different network discovery and selection mechanisms can be used in a collaborative manner to complement each other. (See section 5.1.4).
- It is recommended that GSMA consider how to support IMS Voice and Video call in network integrated Wi-Fi scenarios. (See section 5.1.6)

6 APPENDIX

7 REFERENCES

[1] Small Cell Forum: “Integrated Femto-Wi-Fi (IFW) Networks “White paper (February 28 th, 2012)

[2] GSMA/WBA: Wi-Fi Roaming Whitepaper Version 1.0 (December 2nd, 2011)

[3] 3GPP TS 23.402: "Architecture enhancements for non-3GPP accesses".

[4] 3GPP TS 33.402: "3GPP System Architecture Evolution: Security aspects of non-3GPP accesses".

[5] 3GPP TS 24.312: "Access Network Discovery and Selection Function (ANDSF) Management Object (MO)".

[6] 3GPP TS 23.261: "IP Flow Mobility and seamless Wi-Fi offload; Stage 2".