Wi-Fi Roaming Guidelines
Version 10.0
08 May 2015

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 Scope

The main purpose of this document is to describe the Wi-Fi Access to the Evolved 3GPP Packet Switched domain also known as the Evolved Packet Core (EPC) as defined in the 3GPP specifications TS 23.402 and TS 24.302. The document is based on 3GPP Release 11 and later.

The document concentrates on the roaming scenarios but also includes some non-roaming scenarios to give the full picture, including mobility between E-UTRAN and pre-E-UTRAN 3GPP radio access technologies, policy control and charging, and authentication.

The main focus of the current version of the document are S2b and S2a interfaces using GTP. Out of scope are the S2c interface and usage of PMIP (for both S2b and S2a).

> **NOTE:**The case of Non-seamless offload (i.e. data traffic directly to a data network without passing through EPC) is FFS.

The previous version of PRD IR.61 (version 6.0) is moved to the Annex A, thus if the reader is not interested in EPC integrated Wi-Fi roaming (s)he can still find the common guidelines for the pre-Release 12 Wi-Fi roaming including:

- Access interfaces including connection procedures (also according to WiFi Alliance WFA HotSpot 2.0 specification) and authentication
- Inter-operator interfaces for RADIUS authentication and accounting procedures (recommendations for charging principles, billing and settlement are handled in detail by BARG and TADIG)
- 3GPP Release-7 Interworking WLAN related Domain name System (DNS) naming conventions, DNS deployment considerations and guidance for Public Land Mobile Network (PLMN) selection
- 3GPP Release-7 Interworking WLAN related Network Access Identifies naming conventions

Please refer to the introductory note of Annex A for the status of I-WLAN in 3GPP.

2 Abbrevations and Terminology

Abbreviation	Term	Description
	Access Independence	The WLAN UE is able to establish WLAN 3GPP IP Access connectivity and access 3GPP PS services without prior authentication to WLAN 3GPP Direct Access.
	Accounting	The process of collecting resource usage measurements and apportioning charges for joint service between interworking and/or co-operating service/network providers.

Abbreviation	Term	Description
	Billing	A function whereby Call Detail Records generated by the charging function are transformed into bills requiring payment.
	Customer	A business entity or an individual with a direct contractual relation to receive the Service from the Home Wi-Fi Service Provider.
	Home Wi-Fi	The network operated by the Home Wi-Fi Service Provider-.
	RADIUS Roaming Proxy (WLAN Roaming Proxy)	RADIUS Roaming Proxy (or WLAN Roaming Proxy) shall mean a component transporting RADIUS messages from visited Wi-Fi Service Provider to Home Wi-Fi Service Provider (and vice versa). This component typically also carries out some security functions. The interface between RADIUS Roaming Proxies is an inter-operator interface described in this document.
	Roaming Agreement	Agreement between two parts to enable end users of each to utilize the other parts network using their Home account service provider authentication parameters.
	Roaming Partner	The WO who has entered into a Roaming Agreement with another WO.
	Roaming Service	Roaming Service in this document means provision of Internet service over WLANs for customers of another WO, also known as the Roaming Partner. The Roaming Service enables customers from Roaming Partners to access at least their subscribed services through each other's network by using the same authentication credentials as in its Home WLAN
	Settlement	
	User	The individual receiving the Service.
	Visited Wi-Fi	The network operated by the Visited Wi-Fi Service Provider -
	Non-seamless WLAN Access/Offload **NOTE**: This is to use the same terminology as 3GPP and also to avoid any confusion with "WiFi Direct" feature now supported by some UEs.	The WLAN UE has an access to an IP network directly from a WLAN AN without passing data to a PMN (e.g. EPC) via a tunnel. It is a non-EPC based solution.
	WLAN 3GPP IP Access	The WLAN UE is allowed to access 3GPP PS based services provided via WLAN. The data traffic gets always routed PLMN.

Abbreviation	Term	Description
3GPP AAA-Proxy		3GPP defined RADIUS and Diameter AAA proxy for the 3GPP Rel-6
3GPP AAA-Server		3GPP defined RADIUS and Diameter AAA server for the 3GPP Rel-6
802.1X PAE	IEEE 802.1X Port Access Entity	The logical port controlling the flow of user data on an 802.1X enabled Access Point till authentication is complete.
AC	Access Controller	
Alternative NAI	Alternative Network Access Identifier	A NAI that shall have the form of: '<any_non_null_string>@unreachable.3gppnetwork.org'
ANDSF	Access Network & Discovery & Selection Function	3GPP framework comprising of a network entity (ANDSF Server) and a UE entity (ANDSF Client) that supports operator's policies for network slection and traffic steering between 3GPP and non-3GPP accesses (e.g. WLAN).
AP	Access Point	Interface between the radio network part and the wired network part of a WLAN network, offering wireless connectivity to MTs
BARG	Billing, Accounting, and Roaming Group	Working Group within GSMA.
Decorated NAI	Decorated Network Access Identifier	A NAI that shall have the form 'Homerealm!username@visitedrealm'
Diameter		Authentication, Authorization and Accounting (AAA) protocol
EAP	Extensible Authentication Protocol	A protocol to transfer authentication information between a MT and a Home WO AAA-server.
EAP-AKA	Extensible Authentication Protocol using a USIM profile	Extensible Authentication Protocol with Universal Mobile Telecommunications System (UMTS) Authentication and Key Agreement (AKA) mechanism method as standardized in RFC 5448
EAP-AKA'	Extensible Authentication Protocol using a USIM profile	Improved Extensible Authentication Protocol Method for 3rd Generation Authentication and Key Agreement as standardized in RFC 5448
EAP-SIM	Extensible Authentication Protocol using a SIM profile	Authentication method used with EAP to support authentication using a SIM, as standardized in RFC 4186
EAP-TLS	Extensible Authentication Protocol using a certificate	Authentication method used with EAP to support authentication through Transport Layer Security, in which secure digital certificates are used to mutually identify a user and a server's identity, as standardized in RFC 5216

Abbreviation	Term	Description
EAP-TTLS	Extensible Authentication Protocol using Username/Password	Authentication method used with EAP to support authentication through Tunnelled Transport Layer Security, in which secure digital certificates are used to identify a server's identity (and optionally, a device's or user's identity), establish a tunnel, and then allow for user identification over the encrypted tunnel, as standardized in RFC 5281 tools. **NOTE:** that there is often an inner EAP method used with EAP-TTLS, such as MSCHAPv2 (see RFC 2759).
EPC	Evolved Packet Core	EPC is an end-to-end packet core architecture for 4G Long-Term Evolution (LTE) that provides a converged voice and data networking framework to connect users to an LTE network
ePDG	Evolved Packet Data Gateway	IPsec GW that connects UE to Untrusted Non-3GPP network
EPS	Evolved Packet System	
Fast Re-authentication NAI	Fast Re-authentication Network Access Identifier	A NAI that is optionally used only during the EAP-SIM/AKA/AKA' fast re-authentication procedure. The NAI shall have the form of: '<any_string>@realm' or just '<string>'
FQDN	Fully Qualified Domain Name	An unambiguous domain name that specifies the node's position in the DNS tree hierarchy absolutely
Home Wi-Fi SP	Home Wi-Fi Service Provider	The Party contracting to provide the Service to its own Customers and authenticates and charges the customer.
HS2.0	HotSpot 2.0	WFA standardized protocol for the automated network discovery in Wi-Fi networks
IARP	Inter-APN Routing Policy	Operator rules determining which traffic should be routed across which PDN connection and which traffic should be non-seamlessly offloaded to WLAN
IKEv2	Internet Key Exchange version 2	Version 2 of the Internet Key Exchange protocol, which is used to negotiate a Security Association at the outset of an IPsec session.
IPSec	IP Security	A suite of protocols for securing IP communications by authenticating and/or encrypting each IP packet in a data stream.
IREG	International Roaming Experts Group	Working Group within GSMA.
MAC	Message Authentication Codes	These are unique cryptographic values computed and attached to each protocol message to provide message authenticity.
MAP	Mobile Application Part	Mobile related SS7 application protocol that is used in the GSM Core Network to talk to the AuC/HLR.
MNO	Mobile Network Operator	

Abbreviation	Term	Description
MT	Mobile Terminal	End system equipment providing the interface towards human beings through a set of applications NOTE: The MT includes, among other things, the functions and protocols necessary to provide and handle the communication to the WLAN network, as well as against other networks, services, and applications.
MTP	Message Transfer Part	Layer 1,2,3 of the SS7 stack
PCRF	Policy Charging and Rules Function	LTE network functionality that supports service data flow detection, policy enforcement and flow-based charging
PDG	Packet Data Gateway	A 3GPP flavoured IKEv2 IPsec gateway
PDN Gateway	Packet Data Node GW	Gateway acts as the interface between the LTE network and other packet data networks
PGW	PDN Gateway	Gateway acts as the interface between the LTE network and other packet data networks
PLMN	Public Land Mobile Network	
PSPL	Preferred Service Providers List	A prioritised list of service providers preferred by the UE's (3GPP) home operator for WLAN roaming.
Root NAI	Root Network Access Identifier	A NAI, that shall have the form ‘username@realm’.
SA	Security Association	An establishment of shared security information between two network entities to support secure communication.
SCCP	Signalling Control Connection Part	Control part of SS7 protocol that manages Signalling Transfer Points (STPs)
S-GW	Serving Gateway	Routes data packets through the access network.
SS7	Signalling System 7	Circuit Switched Network Signalling Protocol for connection management.
TADIG	Transferred Account Data Interchange Group	Working Group within GSMA.
TCAP	Transfer Capabilities Application Part	Mobile related SS7 protocol that is used in the GSM Core Network to talk to the AuC/HLR.
TFT	Traffic Flow Template	
TWAG	Trusted WLAN Access Gateway	Gateway that interfaces P-GW using S2a.
TWAN	Trusted WLAN Access Network	Trusted WLAN network that does not require the use of IPsec with the UE. The detailed functional split within a TWAN is out of scope of 3GPP. Whether a Non-3GPP access is trusted or not to EPC is left for the (AAA server of the) Home operator to decide.
TWAP	Trusted WLAN AAA Proxy	Relays AAA information between TWAN and 3GPP AAA Server (or Proxy in case of roaming) using the STa (Swd) interface.

Abbreviation	Term	Description
Visited Wi-Fi Service Operator	Visited Wi-Fi Service Provider	The Party providing the Roaming Service to the Customer-of the other Party.
WAG	WLAN Access Gateway	A 3GPP flavoured Access Controller
W-APN	WLAN APN	WLAN equivalent for GPRS Access Point Name (APN)
WFA	Wi-Fi Alliance	
Wi-Fi SP	Wi-Fi Service Provider	Owner and/or Provider of Wi-Fi network infrastructure. This entity could be a Mobile Network Operator (MNO) or a Wireless Internet Service Provider (WISP).
WISP	Wireless LAN Internet Service Provider	
WLAN	Wireless Local Area Network	Usually referred to the IEEE 802.11 product family.
WLANSP	WLAN Selection Policies	Operator rules that determine which WLAN AP to select
WLAN UE	WLAN User Equipment	A terminal with WLAN capability
WLCP	WLAN Control Plane (protocol)	Control (only) protocol between UE and TWAG to (dynamically) setup / release a PDN connection when under trusted WLAN access.
WPA	Wi-Fi Protected Access	This is a Wi-Fi Alliance promoted WLAN device security feature set. It includes IEEE 802.1X support, Support for portions of the IEEE 802.11i draft specification namely TKIP and optional AES cipher suite support.
WPA2		Wi-Fi Protected Access II

3 References

Document	Name
RFC 2865	Remote Authentication Dial In User Service (RADIUS)
RFC 2866	RADIUS Accounting
RFC 2869	RADIUS Extensions
RFC 2607	Proxy Chaining and Policy Implementation in Roaming
RFC 5247	PPP Extensible Authentication Protocol (EAP)
RFC 4186	EAP SIM Authentication
RFC 3579	Radius support for Extensible Authentication Protocol
RFC 3580	IEEE 802.1X RADIUS Usage Guidelines
RFC 1851	The ESP Triple DES Transform
RFC 2401	Security Architecture for the Internet Protocol
RFC 4372	The Chargeable User Identity
RFC 4284	Identity Selection Hints for the Extensible Authentication Protocol (EAP)
RFC 4282	The Network Access Identifier
RFC 4306	Internet Key Exchange (IKEv2) Protocol
RFC 5448	EAP-AKA and EAP-AKA' Authentication
RFC 5216	The EAP-TLS Authentication Protocol
RFC 5281	The EAP-TTLS Authentication Protocol
RFC 5580	Carrying Location Objects in RADIUS and Diameter
PRD AA.80	Agreement for IP Packet eXchange (IPX) Services
PRD IR.21	Roaming Database, Structure and Updating Procedures
PRD IR.33	GPRS Roaming Guidelines
PRD IR.34	Inter-PLMN Backbone Guidelines
PRD IR.40	Guidelines for IPv4 Addressing and AS Numbering for GPRS Network Infrastructure and Mobile Termin
PRD IR.67	DNS Guidelines for Operators
PRD IR.88	LTE and EPC Roaming Guidelines
3GPP TS 23.003	Numbering, addressing and identification
3GPP TS 23.402	Architecture enhancements for non-3GPP accesses
3GPP TS 24.244	Wireless LAN Control Plane protocol for trusted WLAN access to EPC
3GPP TS 24.302	Access to the 3GPP Evolved Packet Core (EPC) via non-3GPP access networks
3GPP TS 24.312	Access Network Discovery and Selection Function (ANDSF) Management Object

Document	Name
3GPP TS 24.234	WLAN User Equipment (WLAN UE) to network protocols (See introductory **NOTE** in Annex A)
3GPP TS 29.234	3GPP System to Wireless Local Area Network (WLAN) Interworking; Stage 3; Release-7 (See introductory **NOTE** in Annex A)
3GPP TS 33.234	Wireless Local Area Network (WLAN) interworking security; Release-7 (See introductory **NOTE** in Annex A)
3GPP TS 33.402	Security aspects of non-3GPP accesses

4 EPC Overview (Informative)

4.1 EPC Access Overview

3GPP Rel-8 introduced the Enhanced Packet Core (EPC) as part of EPS and the integration of non-3GPP accesses into EPC. It also supports local breakout for the services when UE is roaming.

General guidelines for the EPC roaming environment using 3GPP accesses are described in IR.88.

4.1.1 EPC-integrated Wi-Fi Overview

Integration of Wi-Fi Access into EPC enables Mobile Services to be available through Wi-Fi. Release-11 and later makes it possible to use mobile services, like IMS-based voice and video, MMS and SMS over IP over the Wi-Fi Access.

Wi-Fi Access is divided into two scenarios, one for Trusted Wi-Fi Access and one for Untrusted Wi-Fi Access. In case of Trusted Wi-Fi Access, the Wi-Fi connects directly to the PDN Gateway via S2a interface, using GTP.

In Untrusted Wi-Fi Access an additional IPsec tunnel is established between UE and ePDG using SWn interface. After successful IPsec tunnel setup, ePDG forwards the user traffic to PDN GW via S2b interface using GTP. In a roaming scenario, the HSS/3GPP AAA Server in HPLMN makes the decision of whether a Wi-Fi Access is used as Trusted or Untrusted Wi-Fi Access. The HSS/3GPP AAA Server may take the VPLMN's policy and capability returned from the 3GPP AAA Proxy and roaming agreement into account.

Figure 1 illustrates the overall roaming architecture for EPC when using the interfaces S5, S2a and S2b as specified in 3GPP TS 23.402. SWd is required as a roaming interface. For EPC/LTE roaming interfaces, please refer to IR.88.

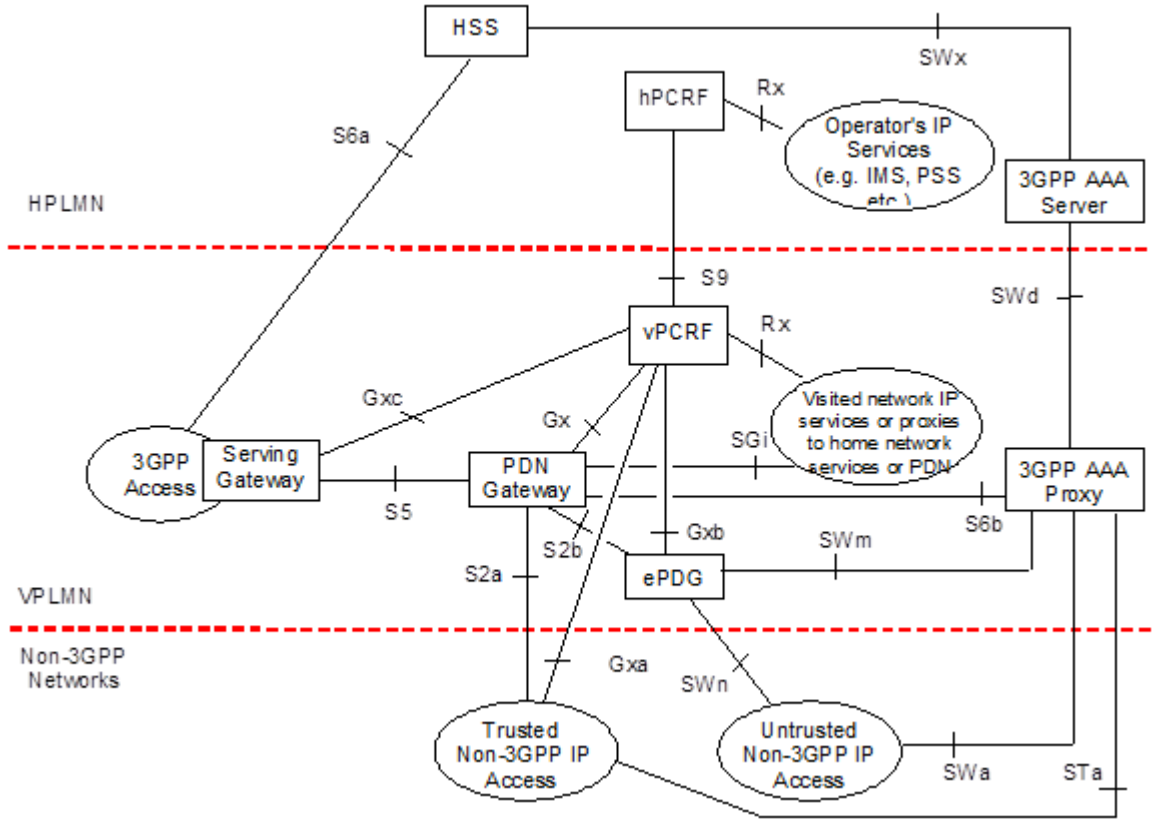

Figure 1: Roaming Architecture for EPC using S5, S2a, S2b – Local Breakout (from 3GPP TS 23.402)

4.1.2 EPC Specific Nodes

The following list briefly describes key EPC components.

- PDN Gateway EPC supports GPRS Tunnelling Protocol for the control plane and the user plane to provide PDN connectivity to UEs using trusted or untrusted Wi-Fi Access.
- ePDG is placed at the border between the Untrusted Wi-Fi Access and the PLMN. It is used to create an IPsec tunnel to the UE and is connected to the PDN Gateway via S2b interface when using Untrusted Wi-Fi Access..
- For S2a, the functional structure of the trusted WLAN access network is summarised in Figure 2. In this case there is no need for an IPSec tunnel between the UE and Trusted WLAN Access Gateway (TWAG): It leverages the appropriate security provided by IEEE 802.11-2012 (802.11i, AES) over the air interface (SWw) between UE and the WLAN Access Network. The TWAP (Trusted WLAN AAA Proxy) relays AAA information between TWAN and 3GPP AAA Server (and via a 3GPP Proxy AAA when roaming). The internal structure and interfaces of the Trusted Non-3GPP Access Network (e.g. fixed BB Access for WLAN support) are out of scope of 3GPP.

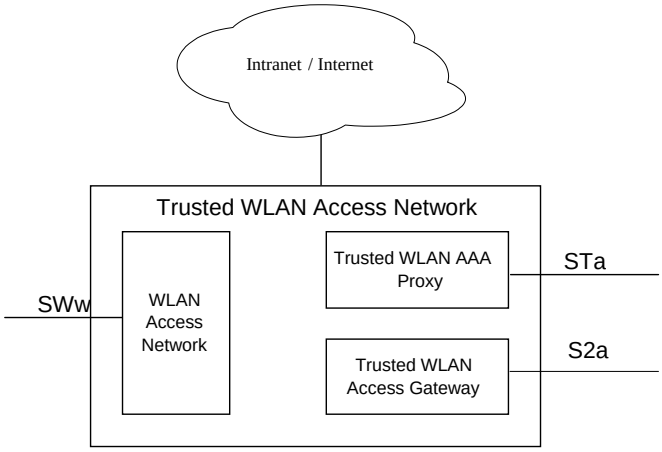

Figure 2: Trusted WLAN Access Network functions (from 3GPP TS 23.402)

PCRF is a Policy Charging and Rules Function. Among its responsibilities are the need to provide QoS information and charging policies information to the PDN Gateway and to manage and control sessions.

5 Access Interface

5.1 Interactions between AAA & HSS

The interaction between 3GPP AAA server and HSS in the HPLMN via SWx reference point for Wi-Fi Access is described in 3GPP TS 23.402 chapter 7. It defines the Location Management procedures, Subscriber Profile Management procedures as well as Authentication Procedures.

Location Management procedures are common to all Wi-Fi Accesses, whether Trusted or Untrusted, and are independent of the mobility protocol used.

The Subscriber Profile Management is invoked by the HSS when the subscriber profile has been modified and needs to be sent to the 3GPP AAA Server. This may happen due to a modification of the user profile data in the HSS.

The 3GPP AAA Server may also request the user profile data from the HSS. This procedure is invoked when the subscription profile of a subscriber is lost or needs to be updated.

The authentication procedures between HSS and 3GPP AAA Server are described in 3GPP TS 33.402 chapter 8.

NOTE: fast re-authentication is FFS

The authentication procedures define the process in which the 3GPP AAA Server interacts with the HSS to acquire necessary data (i.e. Authentication Vectors for EAP-AKA, RFC 4187 or EAP-AKA', RFC 5448) from the HSS to successfully authenticate the user to access the Wi-Fi system.

For supporting multiple PDN connections, all PDN connections shall be setup either as Trusted or as Untrusted, i.e. it shall not be possible to use the procedure to access one PDN using the Wi-Fi Access Network via a Trusted Wi-Fi Access, while using the same procedure to access another PDN using the same Wi-Fi Access as Untrusted Wi-Fi Access

5.2 Wi-Fi Access Network Selection

5.2.1 Wi-Fi Access Selection

NOTE: For support and status of I-WLAN refer to Annex A introductory note.

5.2.2 ANDSF Support

The Access Network Discovery and Selection Function (ANDSF) may be used to support access Wi-Fi selection and traffic streering over WLAN and 3GPP accesses.

The ANDSF is a framework consisting of a UE client and a network (EPC) server defined by 3GPP. It is specified in 3GPP TS 23.402, 3GPP TS 24.302 and 3GPP TS 24.312. With 3GPP Release 12, ANDSF provides a complete and consistent set of rules for both WLAN selection and Traffic Steering.

The simplified architecture of this framework is illustrated below. The interface between the UE and ANDSF server (S14) is based on OMA-DM (Device Management) and runs on an IP based network and reachable via 3GPP or WLAN access. ANDSF is applicable for both trusted and untrusted accesses.

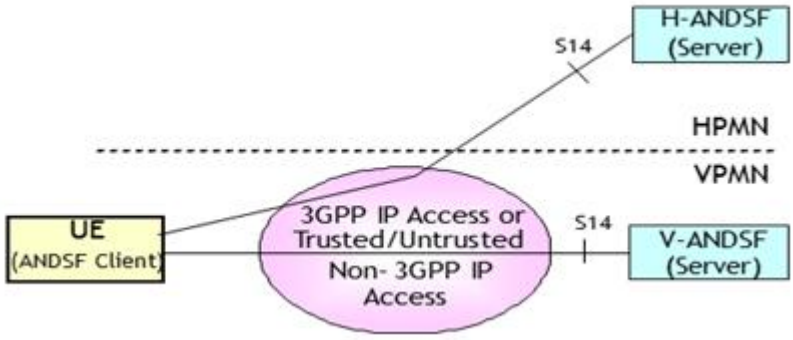

Figure 3: ANDSF Architecture

ANDSF (Release 12) supports the following:

- WLAN access selection (and PMN selection) consisting of:
  - WLAN Selection Policies (WLANSP) which are operator rules that determine which WLAN AP to select.
  - The Preferred Service Providers List (PSPL) which contains a prioritised list of service providers preferred by the UE's (3GPP) home operator for WLAN roaming. The PSPL is provided by the HPLMN through H-ANDSF (or can be statically provisioned in the UE).
- Traffic steering: this has been enhanced by the introduction of:
  - Inter-APN Routing Policy (IARP) which are operator rules determining which traffic should be routed across which PDN connection and which traffic should be non-seamlessly offloaded to WLAN (NSWO).
  - 3GPP RATs (E-UTRAN, UTRAN and GERAN) in Inter-System Routing Policies (ISRP) allowing better rule granularity than the Release 11 "Wi-Fi" and "3GPP" choice

With 3GPP Release 12, ANDSF provides a complete and consistent set of rules for both WLAN selection and Traffic Steering and this for both S2a and S2b.

NOTE: An alternatives to ANDSF (e.g. static provisioning or “RAN rules” based) is FFS.

NOTE: The 3GPP Release 12 work on 3GPP / WLAN Radio inter-working (consideration of e.g. access load, signall strength / quality) is also relevant for network selection / traffic steering decisions and can be described when the related work is sufficiently advanced and stable. In this work, the ANDSF is optional in the sense that two solutions will be specified: one with ANDSF and one without (“RAN rules”).

5.3 EPC-integrated Wi-Fi Access Authentication and Security

EPC-integrated Wi-Fi Access authentication defines the process that is used for Access Control (i.e. to permit or deny a subscriber to attach to and use the resources of an EPC-integrated Wi-Fi Access). Access authentication signalling is executed between the UE and the 3GPP AAA server/HSS. The authentication signalling may pass through AAA proxies and the UE must support both EAP-AKA and EAP-AKA’.

3GPP based access authentication is executed across a SWa/STa reference point as depicted in the EPC architecture diagram. The following principles shall apply in this case:

- The Wi-Fi access only ensures relaying of authentication signalling (in EAP) and does not need to interpret this signalling.
- The 3GPP based access authentication signalling shall be based on IETF protocols, (e.g., Extensible Authentication Protocol (EAP) as specified in RFC 3748).

SWa interface must be used to connect the Untrusted Wi-Fi Access with the 3GPP AAA Server/Proxy and transport access authentication, authorization and charging-related information in a secure manner (see Figure 1).

STa interface connects the Trusted Wi-Fi Access with the 3GPP AAA Server/Proxy and transports access authentication, authorization, mobility parameters and charging-related information in a secure manner (see Figure 1).

The details of the access authentication procedure are defined in 3GPP TS 33.402 chapter 6.1, 6.2, 6.3 and chapter 8 and 3GPP TS 24.302 chapters 6.4 and 6.5.

5.4 Identities

In order to access the 3GPP Evolved Packet Core from Wi-Fi Accesses, and get Authentication, Authorization and Accounting services from the Evolved Packet Core, the RFC 4282 based user NAI (user identification) defined in 3GPP TS 23.003 shall be used.

5.5 IP Address Allocation

The following descriptions are about allocation of IP address for the data plane.

5.5.1 IP Address Allocation in Untrusted Wi-Fi Access

When an Untrusted Wi-Fi Access is used the following IP addresses are allocated to the UE

- An IP address, which is used by the UE within the Untrusted Wi-Fi Access Network to get IP connectivity towards the ePDG

- One or more IP address(es), which is used by the UE towards the external PDNs via the allocated PDN GW(s).

5.5.2 IP Address Allocation in Trusted Wi-Fi Access

When using Single-connection mode and Multi-connection mode, the UE sees the PDN Connection as a point-to-point link similar to how it is in 3GPP access. Shared link parameters such as netmask and default router IP address are not used.

In Transparent Single-connection Mode (3GPP Release 11 and above), TWAG shall act as DHCPv4/v6 server for the UE and handles the RS/RA signalling for Stateless Address AutoConfiguration.

In Single-connection mode and Multi-connection mode (both 3GPP Release 12):

- To support IPv4 connectivity, the IPv4 address shall be allocated and sent to the UE during PDN connection establishment.

To support IPv6 connectivity, the PGW handles the RS/RA messages and to support IPv6 parameter configuration the UE may use stateless DHCPv6. The PGW acts as DHCPv6 server.

5.6 PDN Connectivity Service

5.6.1 Untrusted Access

5.6.1.1 Connectivity Services

For Wi-Fi Access to the EPC the PDN connectivity service is provided by IKEv2 and IPsec connectivity between the UE and the ePDG concatenated with S2b bearer(s) between the ePDG and the PGW. During this connection procedure the UE and the ePDG must support mutual authentication for the IPsec tunnel establishment between the UE and the ePDG (SWu reference point). The Tunnel authentication is using a SWm reference point to the AAA Proxy / Server. The use of S2b bearers is depicted in Figure 4.

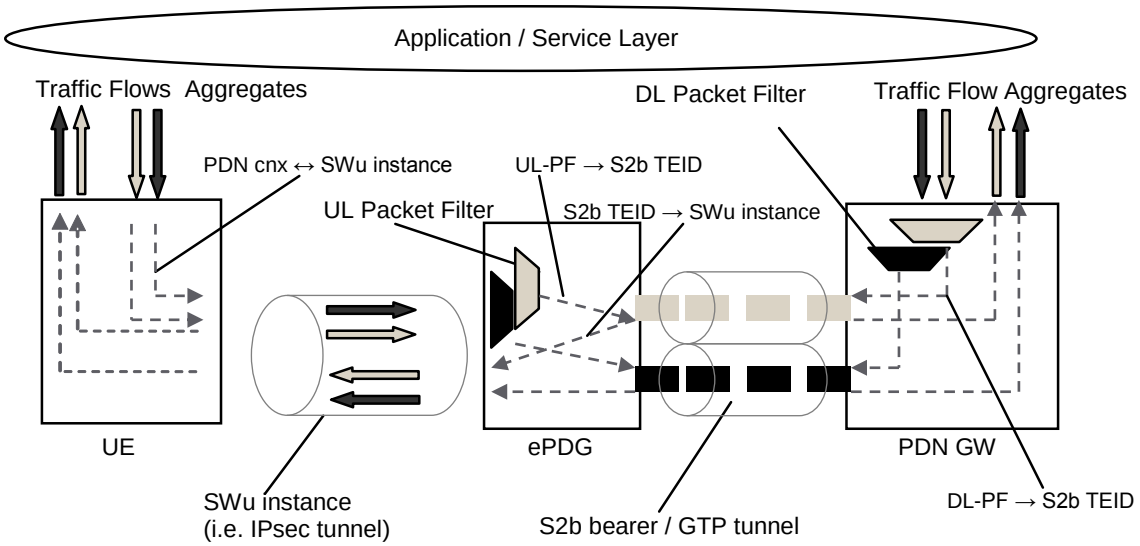

Figure 4: Two Unicast S2b bearers (GTP based S2b)

The UE must establish a separate SWu instance (i.e. a separate IPsec tunnel) for each PDN connection.

One default S2b bearer must be established on the S2b interface when the UE connects to a PDN, and that remains established throughout the lifetime of the PDN connection to provide the UE with always-on IP connectivity to that PDN. Additional dedicated S2b bearers may be established for the same PDN connection depending on operator policy. The PGW establishes dedicated S2b bearers for the same PDN connection based on PCC decisions as specified in 3GPP TS 23.203.

The ePDG must release the SWu instance when the default S2b bearer of the associated PDN connection is released.

The S2b bearer is realized by the following elements:

- A GTP tunnel on S2b transports the packets of an S2b bearer between the ePDG and a PDN GW;
- The ePDG stores the mapping between uplink packet filters it receives from the PGW (e.g. in the Create Bearer Request message) and the corresponding S2b bearer;
  The PDN GW stores the mapping between downlink packet filters and an S2b bearer.

In support for the UE connectivity with the PDN:

- A SWu instance (i.e. a IPsec tunnel) transports the packets of all S2b bearer(s) for the same PDN Connection between the UE and the ePDG.

The ePDG shall route uplink packets to the different bearers based on the uplink packet filters in the TFTs assigned to the bearers in the PDN connection, in the same way as a UE does for uplink traffic under 3GPP access. If no match is found, the uplink data packet shall be sent via the bearer that does not have any uplink packet filter assigned. If all bearers (including the

default bearer for that PDN) have been assigned an uplink packet filter, the ePDG shall discard the uplink data packet.

The PDN GW shall route downlink packets to the different bearers based on the downlink packet filters in in the TFTs assigned to the S2b bearers in the PDN connection, in the same way as the PDN GW does on GTP-based S5/S8 bearers (see 3GPP TS 23.401 clause 4.7.2.2).

5.6.2 Trusted Access

The PDN connectivity service (Figure Y, from TS 23.402) is provided by the point-to-point connectivity between the UE and the TWAG concatenated with S2a bearer(s) between the TWAG and the PDN GW.

The bearer model of GTP based S2a interface is similar to that of GTP based S5/S8 interface and GTP based S2b interface. The TWAN handles the uplink packets based on the uplink packet filters in the TFTs received from the PDN GW for the S2a bearers of the PDN connection as depicted in Figure 5, in the same way as an ePDG does for GTP based S2b interface.

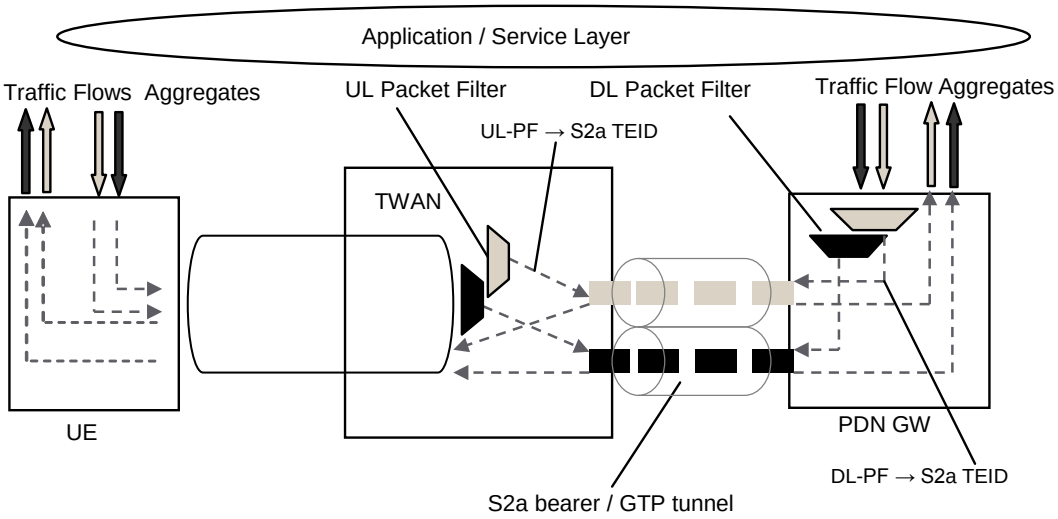

Figure 5 : Two Unicast S2a bearers (GTP based S2a)

The trusted access can be used in the following modes:

- Non-Seamless offload mode (as from Release 11): this mode does not make use of a P-GW (EAP-AKA' however supported) and the traffic is routed directly to an external data network via the TWAG. It can also be considered as a specific case of a Single-connection mode.
- Transparent connection mode (as from Release 11): single connection to P-GW using S2a but without mobility support between 3GPP and WLAN. Selective offload (e.g. moving one PDN out of two from one access to another) is not possible. This nomadic PDN connectivity enables to have a consistent 3GPP service (re-use of P-GW functionalities) while using a WLAN.
- Single-connection mode (as from Release 12): support of a single connection at a time (non-seamless or with a single PDN connectivity). The use of the Single-Connection

mode and the associated parameters of the connection can be negotiated during authentication over TWAN. Seamless mobility between accesses in this mode is possible.

- Multi-connection mode (as from Release 12): support of multiple connections simultaneously. One connection may be used for Non-Seamless offload and one or more simultaneous connections may be used for PDN connectivity. The use of the Multi-Connection mode can be negotiated during authentication over TWAN and a requested PDN connection can be setup with the WLCP (WLAN Control Plane protocol, as per 3GPP TS 24.244). This mode therefore enables the support of MAPCON (Multi-Access PDN Connectivity) where selective offload is possible (e.g. two PDN connections (e.g. IMS, Internet) over 3GPP and only one (e.g. Internet) needs to be moved to WLAN based on operator policy / rules). Seamless mobility in this mode between accesses is possible.

The above modes are managed in a consistent manner using ANDSF Release 12 and must all be supported by the network. UE-Network negotiation for the chosen mode is done during EAP-AKA' procedure. For the case of Non-seamless offload see section 6.4.

Seamless mobility (IP address preservation) is possible for trusted access using S2a as from Release 12 and this is possible with both Single-connection and Multi-connection modes. Mobility of a PDN connection between 3GPP and WLAN is not possible with Release 11 as no modifications to the UE was allowed for that release. This restriction has been removed for Release 12.

NOTE: It has been recommended by the GSMA / WBA Roaming Task Force to IREG (PACKET#66, July 2013) to support seamless mobility (IP address preservation). Delivery of voice and real time services over Wi-Fi will be the key drivers. Furthermore, besides the recommendation of using GTP as protocol to reach P-GW from a WLAN gateway, usage of Trusted WLAN Access was also mentioned as a priority.

NOTE: QoS support for real-time MMTel services as voice and video telephony is required to maintain an appropriate user experience over WLAN, in particular for seamless mobility support. QoS for these services is provided by the network (that can map QoS requirements received over GTP-C onto a proper DSCP to be used over the access leg). The UE is assumed to either derive the uplink QoS from the QoS of the downlink stream or to have the appropriate uplink QoS set by the application.

NOTE: TWAG discovery by the UE is not required as the UE just contacts the AP (beacon) and then the AP selects a TWAG. How the AP selects the TWAG is out of scope of 3GPP. When Multi-Connection Mode applies, the UE needs to contact directly the TWAG over IP (using WLCP).

6 Functional Description & Procedures of EPC-Integrated Wi-Fi

6.1 Overview

The EPC supports the use of Wi-Fi Access Networks. The PDN GW is an anchoring point of services (for all accesses), 3GPP services are available through Wi-Fi and there is a local breakout available. Also mobility between 3GPP Access Networks and Wi-Fi is possible.

6.2 Mobility Management

Depending on operator policy the EPC network must support network-based mobility management mechanism based on GTP over S2b and (with 3GPP Release 12) over S2a reference points as specified in 3GPP TS 23.402. Connection modes supporting mobility using S2a are described in section 5.6.2.

The mobility management procedures are specified to handle mobility between 3GPP and Wi-Fi Accesses. This applies to UEs either supporting simultaneous radio transmission capability or not supporting it. EPC-based mobility between GERAN/UTRAN Access and Wi-Fi Access requires S4-based SGSNs.

NOTE: The handover indication as specified in 3GPP TS 23.402 chapter 8.6 is only supported in GTPv2.

For multiple PDN-GWs connecting to the same PDN, all the PDN GWs shall support the same mobility protocols.

6.3 Local Breakout

The EPC supports local breakout of traffic whether a roaming subscriber is accessing the EPC via a 3GPP or Wi-Fi Network according to the design principles described in TS 23.402 7.2.4, 7.4.3 and 7.4.4.

6.4 Non-seamless Wi-Fi Offload

Policies for non-seamless Wi-Fi offload must be either pre-defined by the home operator and reside on the UE or be provided via ANDSF according to Release 12 3GPP TS 23.402, that

- determine which traffic should be routed across different PDN connections and which traffic should be non-seamlessly offloaded to Wi-Fi.

6.5 Multi Access PDN Connectivity

The network must support Multi Access PDN Connectivity (MAPCON) as specified in 3GPP TS 23.402 and 3GPP TS 24.302.

7 Roaming Interface

7.1 NNI Overview

EPC integrated Wi-Fi roaming reuses the general IP based NNI structure currently used by other systems and services, such as VoLTE roaming and IMS interconnection.

As the EPC integrated Wi-Fi roaming uses the Local Breakout model in order to be aligned with the general model selected for the VoLTE roaming, the interfaces carrying signalling over NNI are the main consideration for this document.

General requirements for IP addressing and routing are contained within IR.33, IR.34 and IR.40. General DNS guidelines are described in IR.67.

7.2 IPX Specifics

Generally speaking, the IPX (IP eXchange) as defined by IR.34 is the preferred inter-Service Provider IP network for GSMA. Thus it should also be used EPC integrated Wi-Fi roaming purposes.

For further details on IPX, please see GSMA PRDs IR.34 and AA.80.

7.3 SWd

SWd runs between the 3GPP AAA Proxy and 3GPP AAA Server. The main purpose of this interface is to transport AAA signalling between home and visited networks. The actual SWd protocol is specified in TS 29.273.

The SWd interface uses Diameter protocol as defined in RFC 3588. IR.88 describes how Diameter is used in the EPC roaming environment, giving guidance for example on routing and identity related topics. Generally speaking the functionality of SWa, STa, SWm and S6b also applies to SWd. There is no specific Diameter application defined for SWd but it proxies the applications of the interfaces listed above.

As shown in the Figure 6 below, the 3GPP AAA Proxy in the Visited SP acts as a Diameter proxy agent and forwards Diameter commands between the roaming Diameter client and the Diameter server located in the Home SP. As described in IR.88, Diameter traffic over NNI is strongly preferred to use DEA (Diameter Edge Agent) nodes at the border of the Service Provider core network to support scalability, resilience and maintainability.

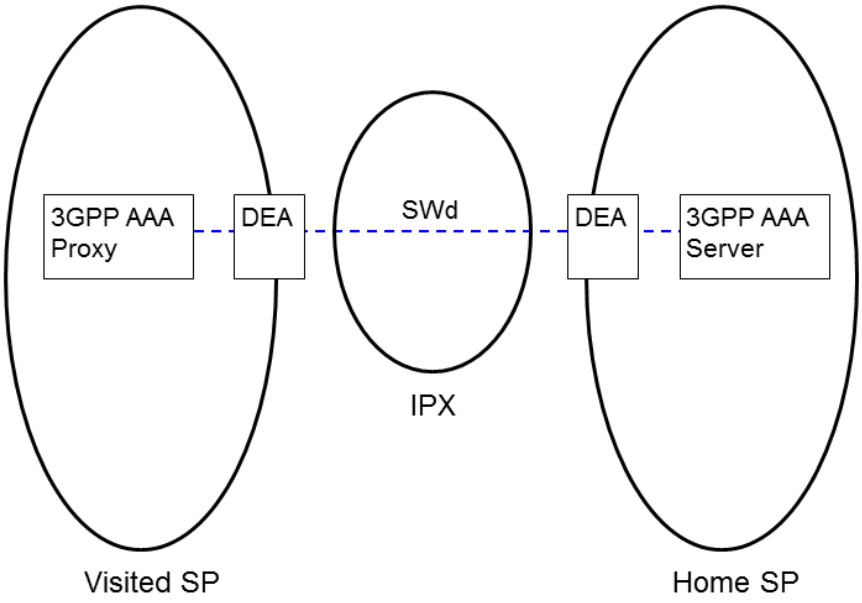

Figure 6 : SWd Interface Overview

SWd is used for the following purposes:

- Carrying data for authentication signalling between 3GPP AAA Proxy and 3GPP AAA Server;
- Carrying data for authorization signalling between 3GPP AAA Proxy and 3GPP AAA Server;

- Carrying charging signalling per user;
- Carrying keying data for the purpose of radio interface integrity protection and encryption;
- Carrying authentication data for the purpose of tunnel establishment, tunnel data authentication and encryption, for the case in which the ePDG is in the VPLMN;
- Carrying mapping of a user identifier and a tunnel identifier sent from the ePDG to the 3GPP AAA Proxy through the 3GPP AAA Server;
- Used for purging a user from the access network for immediate service termination;
- Enabling the identification of the operator networks amongst which the roaming occurs;
- If QoS mechanisms are applied: carrying data for AN QoS capabilities/policies (e.g. the supported 3GPP QoS profiles) within authentication request from 3GPP AAA Proxy to 3GPP AAA Server.
- Carrying the IP Mobility Capabilities between 3GPP AAA Proxy and 3GPP AAA Server.

7.4 Other Functions

Access Control:

Without an explicit agreement from the HPLMN, the VPLMN must block the access of inbound roamers into their Wi-Fi Access network. This is compulsory to ensure roamers will not experience any service disruption because the necessary technical requirements have not been implemented and tested with the HPLMN.

Annex A Pre-Release 12 Wi-Fi Roaming Guidelines (a.k.a. The Previous Version of IR.61)

A.1 Basic Information

NOTE: 3GPP SA agreed in June 2014 that the WLAN IWK feature supersedes I-WLAN feature from Release 12 onwards and that functional modifications of I-WLAN shall be stopped from Release 12 onwards. Some specifications (e.g. TS 29.234) have been discontinued from Release 12 onwards, and others are partially maintained to allow re-use of generic procedures or because some external standards bodies still reference them in their own specifications. However, the I-WLAN work (based on 3GPP Release 6/7) from the "legacy IR.61" is annexed here and not deleted (at least for now) as it may be deployed and used by some operators. The 3GPP I-WLAN specifications referenced in this annex (TS 24.234, TS 29.234 and TS 33.234) are all concerned (along with a some others) by the 3GPP decisions above.

A.1.1 Scope

The main purpose of this document is to specify a common technical solution for Roaming Service between Wi-Fi Service Providers (SP) from an inter-operator perspective.. As a new item it includes WFA relevant aspects of Hotspot 2.0 (HS2.0) implementation to provide automatic network discovery to access roaming Wi-Fi networks. HS2.0 specifies usage of the EAP-methods, too.

It shall cover the following aspects:

- Access interfaces including connection procedures (also according to HS2.0 specification) and authentication
- Inter-operator interfaces for RADIUS authentication and accounting procedures (recommendations for charging principles, billing and settlement are handled in detail by BARG and TADIG)
- 3GPP Release-7 Interworking WLAN related Domain name System (DNS) naming conventions, DNS deployment considerations and guidance for Public Land Mobile Network (PLMN) selection
- 3GPP Release-7 Interworking WLAN related Network Access Identifies naming conventions

The scope of this document is to describe an interoperable way to implement RADIUS based Wi-Fi roaming. Also, within the scope of this document is to describe an interoperable and upwards compatible way to implement 3GPP rel-7 WLAN 3GPP Internet Protocol (IP) Access and 3GPP WLAN Direct Access based roaming that can be deployed before 3GPP Release 7 specifications conforming implementations. 3GPP has implemented inter-operator interface based on AAA protocol (Diameter or Remote Authentication Dial In User Service (RADIUS), however, this document only considers the RADIUS case). This means that also UMTS Subscriber Identity Module ((U)SIM based authentication can be implemented without using

Mobile Application Part (MAP) between operators. GSM Association acknowledges the value of using (U)SIM in Wi-Fi environment.

It is understood that, the current solutions for authentication are Web based login using Username and Password and also the login using Extensible Authentication Protocol (EAP)-SIM or Extensible Authentication Protocol Method for UMTS Authentication and Key Agreement (EAP-AKA or EAP-AKA') over 802.1X. . These solutions use RADIUS as the backend protocol. This document discusses roaming using Web based Username/Password (some implementations may use One Time Passwords for example via help of SMS) or EAP-SIM, EAP-AKA and EAP-AKA' over 802.1X procedures in detail but also touching other EAP methods. This document also includes recommendations how the relevant aspects of HS2.0 specification should be implemented in this environment.

The importance of (U)SIM-based authentication in a Wi-Fi environment is being addressed by the GSM Association through its strong support for EAP-SIM, EAP-AKA and EAP-AKA' inter-operator roaming. Preference has also been given to EAP-SIM EAP-AKA and EAP-AKA' by 3GP*P*, which is defining an inter-working architecture for 3GPP and WLANs.

A.2 Roaming Network Architecture

The Wi-Fi reference roaming architecture described here defines open interfaces for Access and Inter-Service Provider roaming. This architecture when implemented enables users to globally access Wi-Fi as long as roaming agreements are in place between the Service Providers (MNOs providing Wi-Fi or any other Wi-Fi SP).

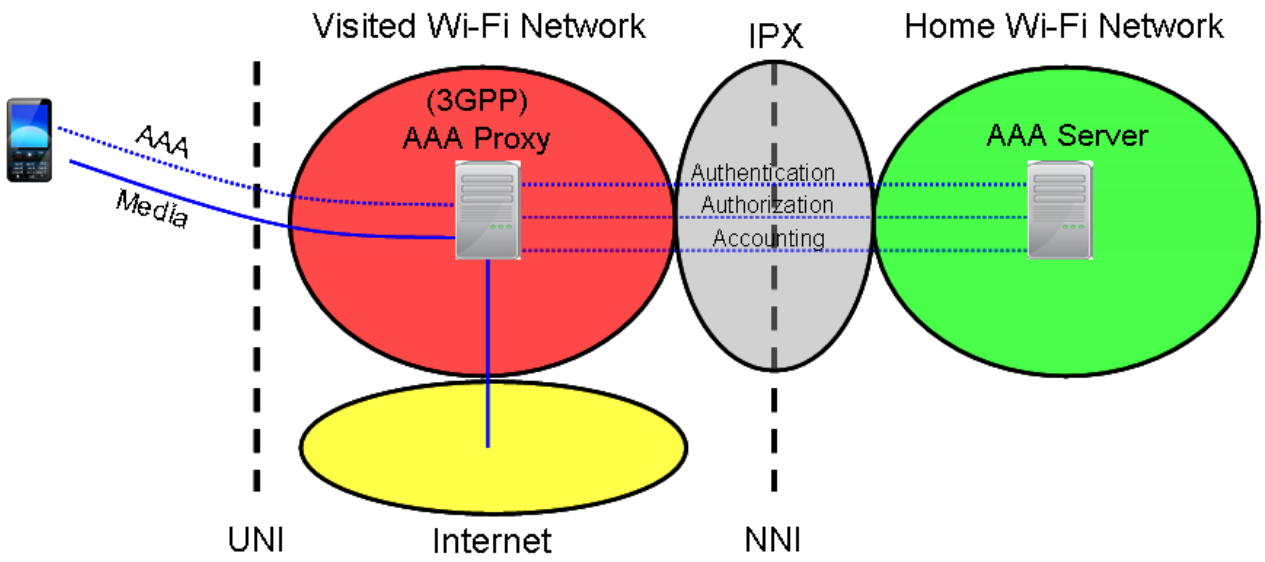

Figure 7: WLAN Roaming Reference Architecture.

Two sets of interfaces are required to support the roaming, one between the MT (Mobile Terminal) and the Visited Wi-Fi Network (Ww and Wa interfaces) and another set between Visited Wi-Fi Service Network and Home Wi-Fi Service Network (Wd interface), defined by

3GPP TS 33.234. These interfaces are based on standard protocols defined by 3GPP, IEEE, IETF and WFA.

The first set of interfaces, as a minimum, is required to provide authentication of the user. User authentication mechanism is a Web based login, using Username/Password over a Secure Sockets Layer (SSL) link with a Web Server hosted by the Visited Wi-Fi SP Network or alternatively EAP-SIM, EAP-AKA or EAP-AKA' that allows the use of a SIM or USIM for authentication using the IEEE 802.1X EAP framework. Also, it is recommended that other EAP based mechanisms such as EAP-Transport Layer Security (TLS) and EAP- Tunnelled Transport Layer Security (TTLS) are supported in the Access networks, so that they can support those EAP-TLS/TTLS roaming users.

The second set of interfaces is between the Visited Wi-Fi SP Network and the Home Wi-Fi SP Network. This set of interfaces shall perform at least two functions: Authentication and Accounting. In addition, Authorization may also be supported for Username/Password Roaming or SIM/USIM based Roaming using EAP-SIM, EAP-AKA, EAP-AKA' including other EAP framework methods the protocols are following:

- Authentication protocols and frameworks: EAP-SIM, EAP-AKA, EAP-AKA', EAP-TLS and EAP-TTLS, EAP, HS2.0, IEEE 802.1X, RADIUS
- Accounting protocols: RADIUS
- Authorization protocols: RADIUS

RADIUS accounting messages shall always be transferred between Home Wi-Fi SP and Visited Wi-Fi SP especially for fraud monitoring and other requirements. Further details are within IETF RFC 2866.

An inter-Service Provider Network is needed when Wi-Fi Roaming between Service Providers is used. This is due to the fact that the RADIUS Roaming Proxy (3GPP AAA Proxy) in the Visited network needs to be able to connect to RADIUS Server in the Home network, since the RADIUS Server located in the Home network is always responsible for example actually authenticating the user, regardless of whether they are roaming or not. This inter-Service Provider interface (NNI) is always based on IP.

IP Exchange (IPX) is the preferred solution for the IP based inter-Service Provider network (between RADIUS Servers) roaming between Service Providers which are MNOs, as it is for other inter-Service Provider IP traffic purposes, for example LTE roaming and MMS interworking. For traffic between Wi-Fi SPs, or between Wi-Fi SP and MNO Wi-Fi SP, alternative solutions such as IPSec could be used. Issues such as quality of service, security, and control of interworking networks, overall reliability and issuing of new network features are easier handled inside IPX than when using public internet to relay RADIUS based roaming traffic between Service Providers. It should be noted that this does not in any way prevent Service Providers from using public Internet as an inter-Service Provider network, if needed. Security issues related to RADIUS based roaming need to be addressed (for example RFC 2607).

A.2.1 3GPP-WLAN Interworking Overview

The 3GPP-WLAN Interworking and roaming architecture briefly described here defines open interfaces for the Inter-Service Provider roaming. This architecture, when implemented, enables users to globally access 3GPP-WLANs as long as roaming agreements are in place between the Service Providers (Mobile Network Operator (MNO) provided Wi-Fi or any other Wi-Fi Service Provider).

A.2.1.1 Roaming Network Architecture

Figure 5 illustrates the 3GPP-WLAN roaming reference model as defined in 3GPP TS 33.234. The figure contains both WLAN 3GPP Direct Access and WLAN 3GPP IP Access scenarios. WLAN 3GPP IP Access specific components are inside the grey area. The Home network is responsible for access control. Charging records can be generated in the Visited and/or the Home 3GPP networks. The 3GPP Authentication, Authorization and Accounting (AAA) proxy relays access control signalling and accounting information to the Home 3GPP AAA Server using the Wd reference point. The 3GPP network interfaces to Wi-Fi Access Networks via the Wa reference point.

This document concentrates to the following reference points:

- Wd – this inter-operator reference point is between the 3GPP AAA Proxy and 3GPP AAA Server, possibly via intermediate networks. The interface is RADIUS or Diameter based. The prime purpose of this reference point is to transport authentication, authorization and related information in a secure manner. EAP-SIM EAP-AKA and EAP-AKA' as well other EAP framework method authentications shall be transported over the Wd reference point from Visited Wi-Fi SP Network to the Home Wi-Fi SP network.
- Wa – This reference point is between the WLAN AN and 3GPP AAA Proxy. This interface is almost the same as Wd interface.
- Ww – This reference point is between the WLAN UE and WLAN AN. It contains e.g. 802.1X protocol and functionalities according to HS2.0.

In addition to the interfaces listed above this document also discusses related functionality such as network nodes wherever required.

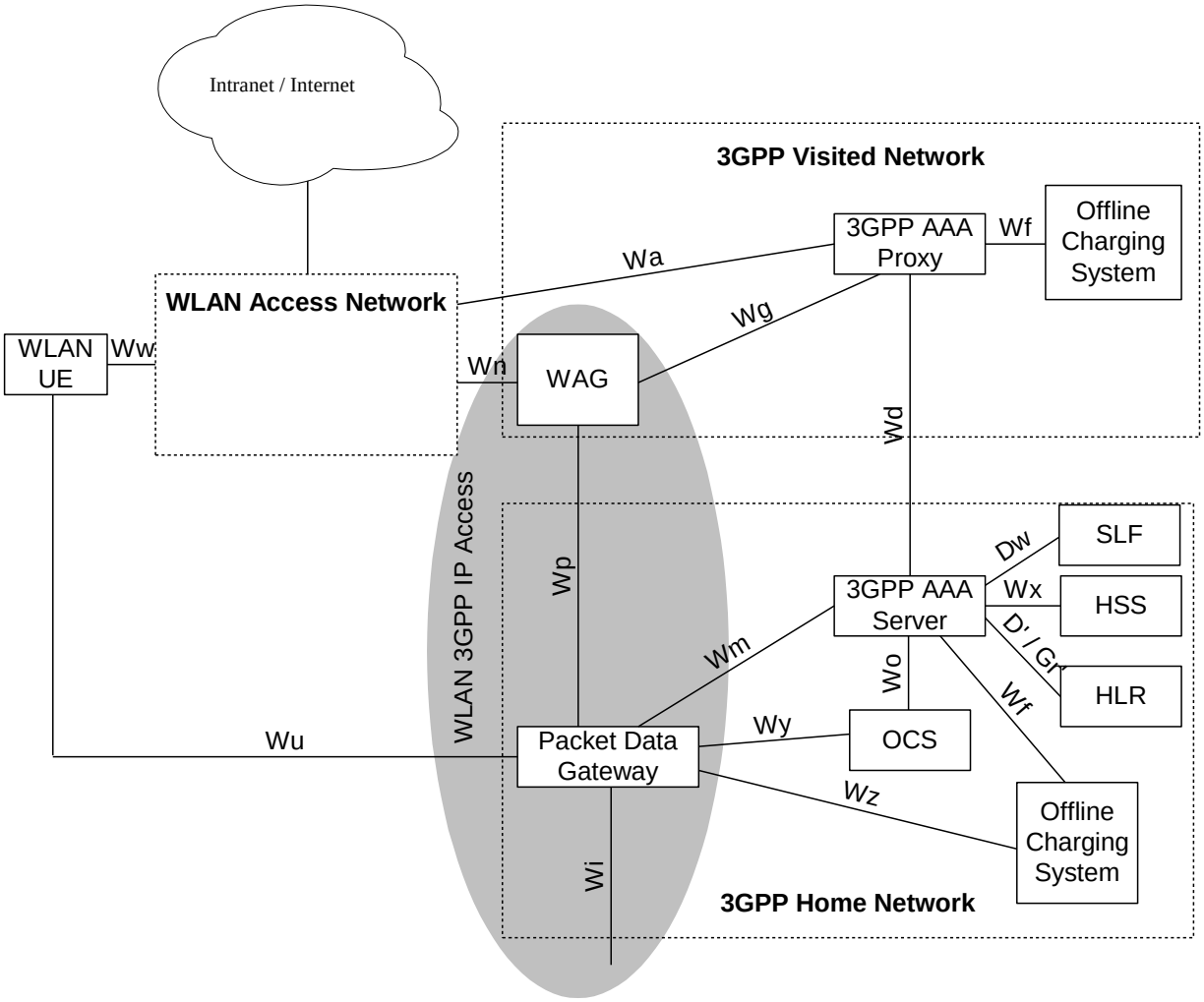

Figure 8: 3GPP-WLAN Roaming Reference Model - WLAN 3GPP Direct Access and WLAN 3GPP IP Access, 3GPP TS 33.234 rel-7

A.3 Access Interface

This section describes how the roaming user connects to the Wi-Fi and the related procedures and the messaging flow. The Authentication and the Authorization process on the Access interface involves the following steps

1. 802.11 Association (Open Authentication)
2. 802.1X Authentication process with EAP-SIM, EAP-AKA or EAP-AKA'
3. 802.1X Authentication process according to HS2.0 specification including EAP-methods.

A.3.1 MT Association to the Wi-Fi

For association to the Wi-Fi, the minimum requirement is knowledge of the Visited Wi-Fi Network Service Set Identifier (SSID). There are four basic methods for this association to occur:

1. Manual configuration of the MT with the right SSID
2. Media sensing, browsing and selecting the right SSID

3. Automatic network discovery based on HS2.0 specification
4. Automatic network discovery based on 3GPP Service Provider Advertisement and Selection

A.3.2 Web Based login

A.3.2.1 Sign-on Procedure

The user performs a login to the Wi-Fi Service using the login page provided by the Web browser. The user must provide the Username, which is of the form of a Network Access Identifier (NAI) as defined in RFC 4282. This NAI shall be of the form: Username@Realm.

Where the Username identifies a unique user in the domain described by the Realm. The Realm should be a fully qualified domain name, which signifies the Home Wi-Fi SP. After the Username@realm entry, a password is entered for authentication process. The login page shall not display the password entered.

The Visited Wi-Fi SP can also provide a dropdown box for choosing the Home operator. In this case, the user enters the Username part of the NAI and chooses the Home operator brand name from a list in a dropdown box on the login page (brand name will be given to a roaming partner in IR.21). The Visited Network then concatenates the correct Realm to the Username (thus creating a complete NAI).

A.3.2.2 Secure Login

The Web based login shall use SSL for secure transmission of the user credentials.

A.3.2.3 Protocol Implementation

The Web based login described above is implemented by the Access controller (AC). When the user first tries to browse the Internet, performing a Hypertext Transfer Protocol (HTTP) Get, using the Wi-Fi, the browser is redirected to the login page. The user enters the Username/Password and this is sent using a Hypertext Transfer Protocol Secure (HTTPS) Put to the AC. The AC has a RADIUS client on the backend which transports the Username/Password in the Access request to the Home Wi-Fi SP Radius Server. The rest of the key messages are shown in Figure 6. In some cases Wi-Fi SPs are using WFA specified WISPr mechanism to ease username/password roaming.

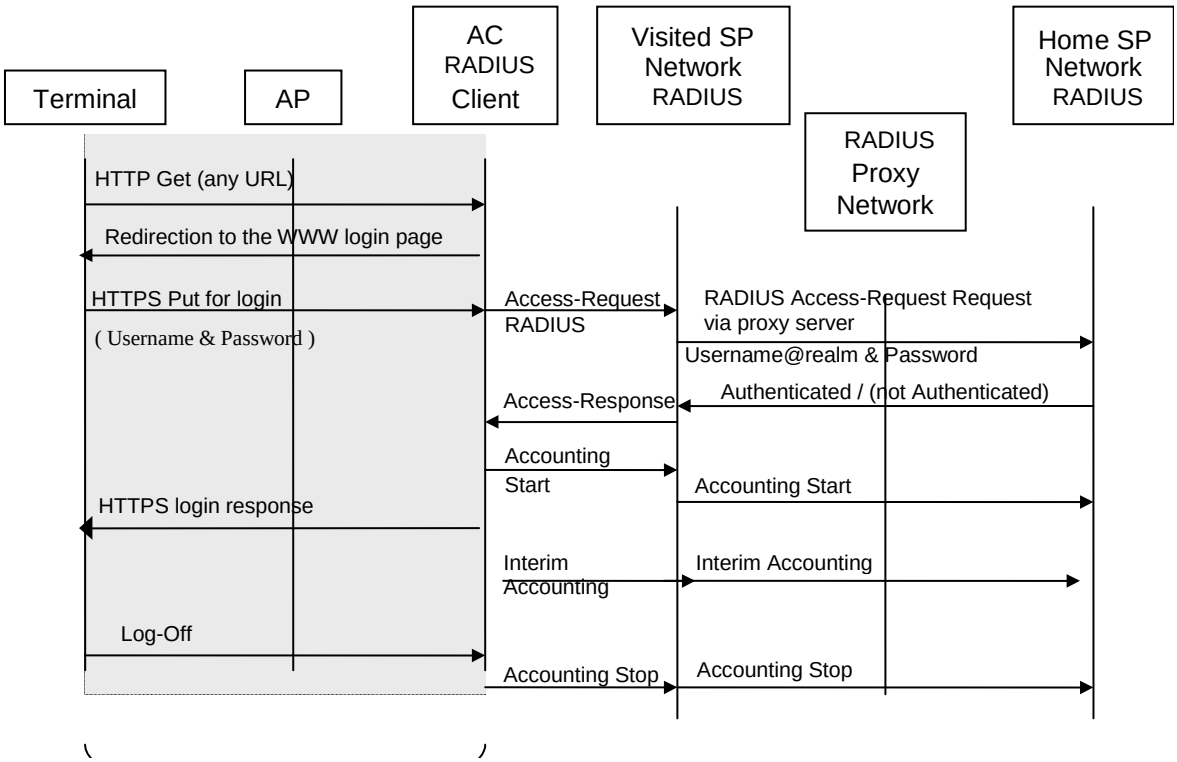

Figure 9: Web Based Login Message Flow Overview

NOTE: All RADIUS accounting messages are acknowledged even though this is not presented in Figure 6.

There is no mandatory behaviour for the HTTPS login response. Depending on business considerations the Visited Wi-Fi SP Network may decide to push as a HTTPS response to the logon procedure one or multiple pages. Those pages could be any of the following:

- Simple login result page
- Portal page from either the Visited network, Home operator, or hotspot location
- Any other page

A.3.2.4 Log-Out

There should be a method for explicit disconnect by the user on a page displayed by the Visited Wi-Fi SP after a successful authentication. This can be for example, a clearly labelled log-out button on a session window provided by the visited Wi-Fi SP.

There is a requirement for Immediate Service Termination functionality by the Home Wi-Fi SP, for example in case of fraud. As there are no standardized ways to implement this functionality (RFC3579 is informational). The recommended mechanism to control user sessions is using Session-timeout parameter to limit their maximum length. The Home Wi-Fi SP should decide the used Session-timeout value.

A.3.3 802.1X AND EAP-SIM, EAP-AKA OR EAP-AKA' Login

A.3.3.1 SIM/USIM Based Login

There are various user scenarios for SIM/USIM based logins. Authentication can be used in the handheld devices, in 3G laptops (also certain Universal Serial Bus (USB) modems support this feature) and in tablets equipped with 3G. The amount of similar devices is rapidly increasing; consumers expect to connect everywhere and require the same access to the Wi-Fi networks similar to the cellular networks meaning that that is transparent as much as possible. That is increasing the Wi-Fi usage and simultaneously offloading traffic from cellular networks to the Wi-Fi networks.

A.3.3.2 802.1X Authentication

When the users with the Mobile Terminals roam into the Wi-Fi Hotspot they expect to get authenticated by the GSM Home Network using SIM/USIM credentials they possess. The Wi-Fi service based on 802.11 uses 802.1X as the flexible authentication and security framework for supporting multiple authentication credential types including SIM/USIM. EAPOL defined within 802.1X provides this flexibility by allowing EAP based authentication methods to be used transparently over the radio link. The Wi-Fi AP that supports RADIUS also allows EAP messages to be carried transparently to the Home SP Network.

A.3.3.3 EAP-SIM, EAP-AKA and EAP-AKA' Authentication

This section describes (U)SIM based Wi-Fi authentication using the EAP-SIM protocol IETF RFC4186 or the EAP-AKA and EAP-AKA' protocol, IETF RFC 5448. The use of EAP-SIM provides the following features:

- Allows re-use of the existing GSM authentication infrastructure for Wi-Fi authentication
- Mutual authentication of the Mobile Terminal and the Network
- Dynamic session key establishment for use in link layer (WPA or WPA2) encryption
- Basic IMSI privacy protection
- An optimized re-authentication procedure

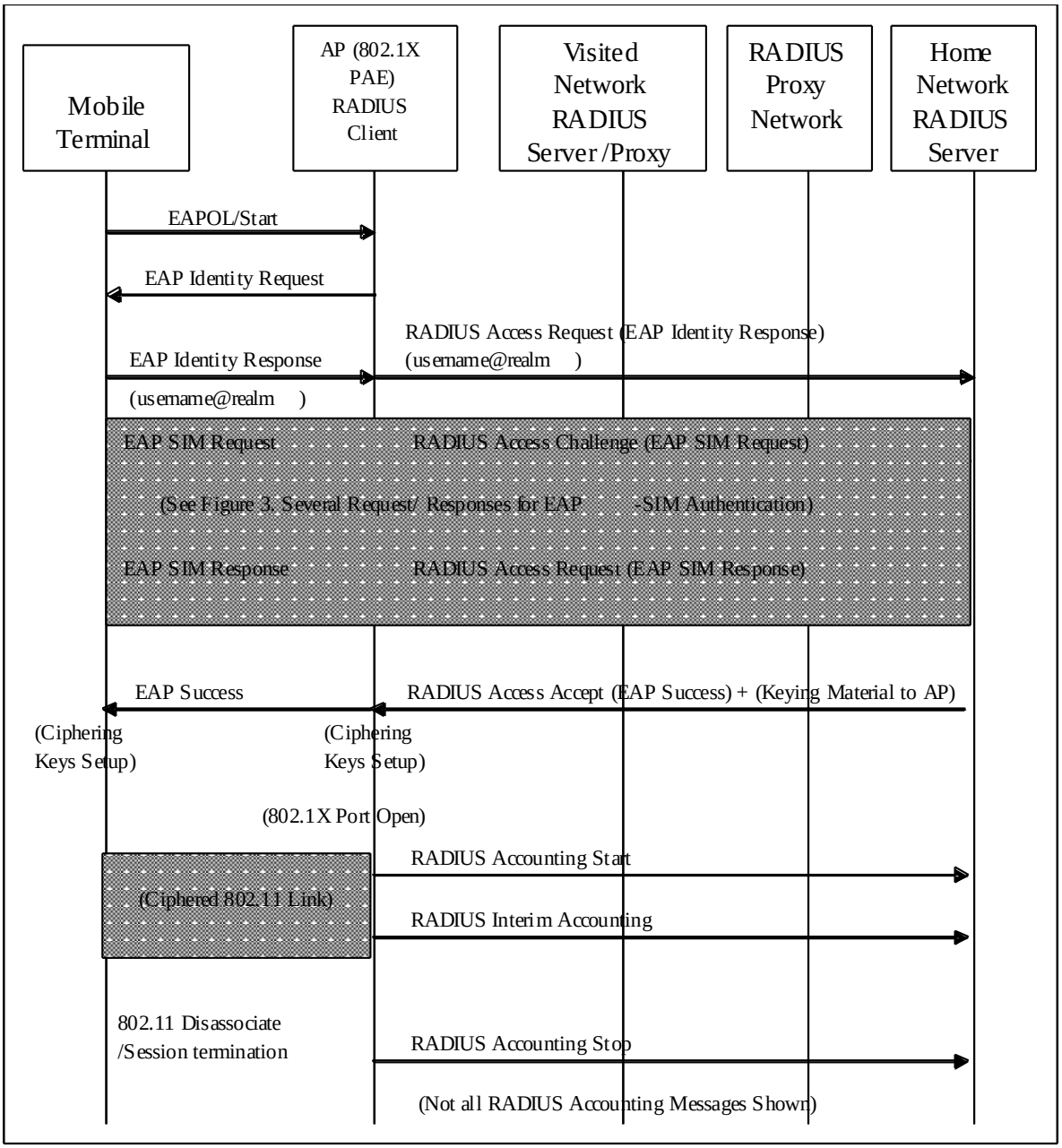

Figure 10: SIM Based Login Message Flow Overview

Figure 7 captures the high-level message flows between the various entities in the visited Wi-Fi Network and the Home Wi-Fi Network RADIUS Server. The IEEE 802.1X Protocol runs between the Mobile Terminal and the Access Point for the purposes of authentication. The Port Access Entity (PAE) implemented on the Access Point is responsible for blocking all user traffic except EAP packets until authentication completes. The AP also has a RADIUS client function which is responsible for initiating the RADIUS protocol which finally terminates on the Home Wi-Fi Network RADIUS Server. This RADIUS client is implemented based on the “IEEE 802.1X RADIUS usage guidelines”, RFC3580, and is responsible for interpreting and appropriately forwarding the EAP packets between the AP and the Home SP Wi-Fi Network. The Visited SP Wi-Fi Network RADIUS Server/Proxy does not modify the EAP message passing through it. However the Visited SP Wi-Fi Network RADIUS Server/Proxy is

responsible for routing the EAP packets to/from the appropriate Home SP Wi-Fi Network RADIUS Server.

Once the Mobile Terminal associates with the Access Point, the EAPOL-Start message is optionally sent by the MT to trigger the 802.1X authentication process based on EAP. The EAP Identity Request is the sent to the MT which responds with EAP Identity Response which carries the NAI (username@realm). The Username can be IMSI or a temporary pseudonym and the 'realm' will be a fully qualified domain name that identifies the home Wi-Fi SP Network. The usage and format of NAIs for 3GPP-WLAN Interworking have been defined in the 3GPP TS23.003. Within IR.61 scope the definitions standardized in the 3GPP TS23.003 should be followed.

The home Wi-Fi SP Network RADIUS Server recognizing the Username will attempt to start the EAP-SIM exchanges using the RADIUS Access Challenges/Requests. Following the successful authentication using EAP-SIM the RADIUS Access Accept message sent from the server will result in an EAP Success message to the Client by the AP. This RADIUS message also carries EAP-SIM derived keying material for the session, which needs to the provided to the AP. The MT also derives keying material as part of EAP-SIM authentication. Ciphering keys are set-up using this keying material on the MT and the AP as part of completing the 802.1X key setting procedures. Please refer to the IEEE 802.1X and 802.11i specifications for details on the key setting procedure. The 802.1X PAE now opens the WLAN for user data traffic that is ciphered using the keys setup earlier.

The Accounting Start message needs to be sent by the AP to the Home Wi-Fi SP Network RADIUS Server for indicating the start of the accounting session. When the Mobile Terminal Disassociates, or terminates the login session, the AP needs to send the Accounting Stop message to indicate the session termination to the Home Wi-Fi SP Network RADIUS Server. Interim Accounting messages are also sent during the session for fraud monitoring and other purposes. These Accounting Messages are defined in RFC 2869.

The EAP-AKA and EAP-AKA', IETF RFC 5448, network access authentication principle is identical to the EAP-SIM. Access network nodes (including WLAN Access Points) and intermediate networking nodes do not need to be upgraded for the EAP-AKA or EAP-AKA' if the EAP-SIM is already supported. However, support for the AKA or AKA' is required from both terminal and backend AAA-server.

A.3.3.4 NAIs for EAP-SIM/AKA/AKA' Authentication

EAP-SIM, EAP-AKA and EAP-AKA' use a set of different identities during the authentication. These identities, full identity, pseudonym identity and re-authentication identity are expressed in form of Network Access Identities (NAI). The following sub-clauses describe all these identities as they are defined in the 3GPP TS23.003. The username part of the NAI contains the identity of the subscriber and the realm part is used for AAA routing. The GSMA PRD IR.67 contains more information concerning the realms used within 3GPP-WLAN Interworking.

A.3.3.4.1 Root NAI

The NAI used within the Release-7 3GPP-WLAN Interworking during full authentication is the Root NAI. The format of the root NAIs are shown below:

- "0<IMSI>@wlan.mnc<MNC>.mcc<MCC>.3gppnetwork.org", for EAP-AKA authentication and
- "1<IMSI>@wlan.mnc<MNC>.mcc<MCC>.3gppnetwork.org", for EAP-SIM authentication
- "6<IMSI>@wlan.mnc<MNC>.mcc<MCC>.3gppnetwork.org", for EAP-AKA' authentication

For example, for EAP-SIM authentication: If the IMSI is 234150999999999 (MCC

=234, MNC=15), the root NAI then takes the form 1234150999999999@wlan.mnc015.mcc234.3gppnetwork.org.

A.3.3.4.2 Fast Re-authentication NAI Root NAI

Fast re-authentication is an optional but important optimization to EAP-SIM/AKA/AKA' and defined in the respective IETF RFCs 4186,5448 and 3GPP TS23.003. The Fast re-authentication provides authentication that does not require new vectors from the HLR/HSS, which makes it a relevant optimization considering the possible reduction on the HLR/HSS load.

A WLAN UE should honour and utilize the fast re-authentication identity returned by the Home AAA-server. If the 3GPP AAA server does not return a complete NAI including both username and realm parts, the Fast Re-authentication NAI shall consist of the Username part of the fast re-authentication identity as returned from the 3GPP AAA server and the same realm as used in the permanent user identity. If the 3GPP AAA server returns a complete NAI as the re-authentication identity, then this NAI shall be used.

A.3.3.4.3 Pseudonym Length

3GPP TS33.234 defines the algorithm for the pseudonym generation and encoding to be used with EAP-SIM/AKA/AKA'. These are additional clarifications to the respective EAP-SIM, EAP-AKA' and EAP-AKA, RFCs. IETF RFCs allow identity and pseudonym lengths up to 253 octets whereas the 3GPP defines the maximum 63 octets (including the possible realm part of the identity). Because of the backwards compatibility reasons with some RADIUS implementations 63 octets maximum length should be used. Furthermore, some WLAN UEs may restrict the length of the NAI to less than 253 octets, thus 63 octets from this point of view is also a safe value.

A.3.3.5 Support of Other EAP Methods

HS2.0 specifies the usage of the other EAP-methods. Each Wi-Fi SP Network should be capable to transmit EAP-TLS and EAP-TTLS requests to the customer's Home SP Network (note: this does not mean that each SP should support EAP-TLS/TTLS authentication for their own customers, but just to support forwarding these requests to the correct Wi-Fi SP according to roaming agreements). The functionality of Hotspot 2.0 also makes it possible to deploy roaming to Wi-Fi networks on a large scale.

Accounting messages for EAP-TLS and EAP-TTLS are the same as on EAP-SIM/AKA/AKA'.

A.3.4 HS2.0 Based Network Discovery

The HotSpot 2.0 specification provides automatic network discovery for Wi-Fi networks, a functionality that is presented and familiar from the mobile networks and it is based on 802.11u specification. This functionality automates correct SSID discovery and simplifies authentication thus increasing the Wi-Fi usage and data offloading. It also uses EAP methods for the authentication and uses WPA2-Enterprise for the encryption of the data.

A.3.4.1 Network selection

The functionality is based on the AP advertising/broadcasting roaming partners NAI Realm list that the AP/Service Provider has a roaming agreement. The functionality is like in the mobile networks.

Even though HS2.0 supports all kinds of NAI Realms, it is recommended that MNOs use 3GPP defined Home Network Realm for WLAN usage (FQDN: wlan.mnc<MNC>.mcc<MCC>.3gppnetwork.org) as per TS 23.003 Section 14.2, since generation of this Home Network Realm can be automatically created from the (U)SIM card in the mobile device.

A.3.4.2 EAP support

The HS2.0 specification includes support for EAP-SIM, EAP-AKA and EAP-AKA' as well EAP-TTLS and EAP-TLS. The specification mandates a Hotspot 2.0 SP (MNO) having SIM/USIM infrastructure to support SIM/USIM credentials and their associated EAP methods and shall support at least one of the following: username/password or certificate credentials and their associated EAP method.

NOTE: HS2.0 mandates all HS2.0 operators to provide EAP-TLS or EAP-TTLS for their own customers. MNOs cannot commit to this since this is business related decision and the choice is up to MNO what to support/provide for their own customers.

A.3.5 Service Provider Advertisement and Selection

Figure 8 provides a logical overview what kind of use scenarios 3GPP-WLAN SP/network advertisement and selection is supposed to support. Basically the WLAN UE may authenticate back to home SP Network either directly or via some visited SP Network.

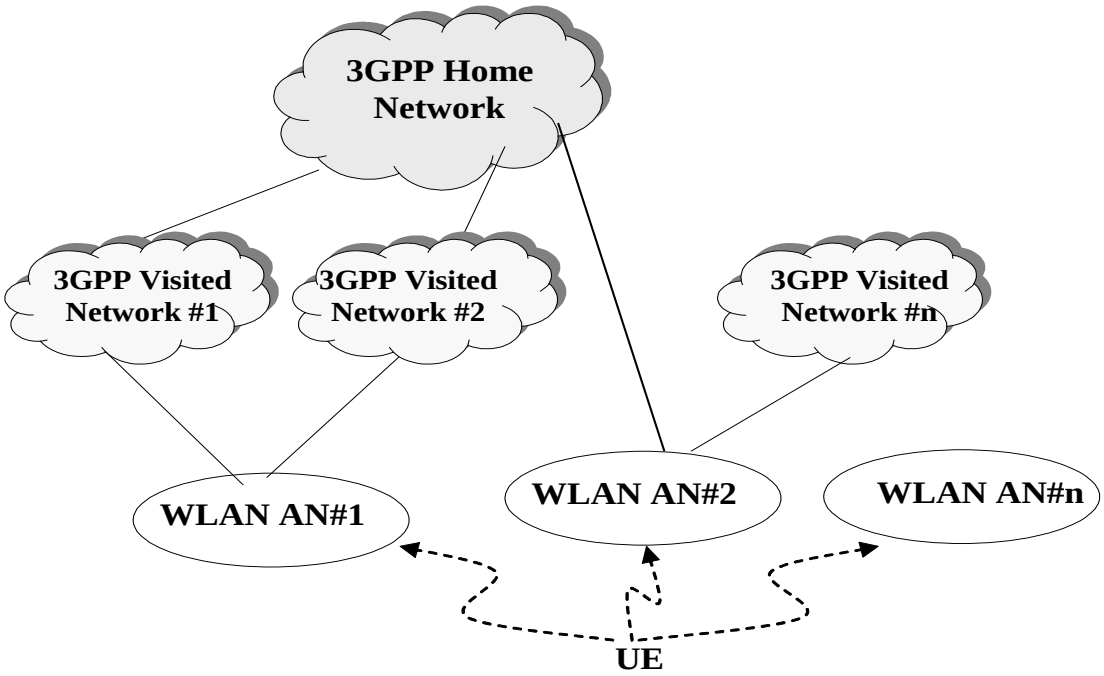

Figure 11: PLMN and Network Advertising and Selection Scenario

3GPP-WLAN Interworking Network selection consists of two procedures: the Interworking WLAN Access Network selection procedure, and the PLMN selection procedure. These procedures are applicable to initial network selection at WLAN UE switch on and following recovery from lack of WLAN radio coverage. In order to ensure that the result of network selection is the association with an Interworking WLAN that has direct connection to HPLMN, both procedures are linked to each other. Two 3GPP-WLAN Interworking network selection modes are defined: automatic and manual. Other network selection modes may be supported but they are implementation dependent.

During the WLAN access network selection procedure the WLAN UE uses at least passive scanning to find all available SSIDs. WLAN UE may also support and use active scanning. The result of passive and active scanning is a list Available SSIDs, which is then used to assist the subsequent PLMN selection procedure.

The Network discovery and selection procedure is executed between WLAN UE and the local AAA for the purpose of sending the WLAN UE the Supported PLMNs list for Wi-Fi access. The WLAN UE should support the Network discovery procedure as specified in the IETF RFC4284. The automatic network discovery procedure is greedy and the WLAN UE always tries to authenticate directly to HPLMN. Whenever a direct connection to HPLMN is found the WLAN UE exits the network selection procedure. If no direct connection is found the WLAN UE should use the highest priority VPLMN that provides connectivity to the HPLMN. In practise terminal and infrastructure vendors have been very slow in adopting 3GPP defined network discovery and selection functionality. Everything is still practically based on lists of SSIDs.

Should the WLAN UE want to find all PLMNs supported by all reachable WLAN ANs, then the WLAN UE must use the manual network selection procedure. During the manual network selection procedure the WLAN UE uses an AlternativeNAI instead of the Root NAI. The WLAN

UE initiates the EAP network discovery with every Wi-Fi network it can hear and attach to. The AlternativeNAI triggers the network discovery procedure and is used for the manual selection procedure. The AlternativeNAI MUST have the Realm part **"unreachable.3gppnetwork.org"** (as mandated by GSMA).

User and the operator should have a possibility to prioritize the order the WLAN UE selects WLAN networks and eventually selects the used PLMN. This is achieved through the use of:

- User defined list of preferred SSIDs and PLMNs (if Visited PLMNs are supported)
- Operator defined list of preferred SSIDs and PLMNs (if Visited PLMNs are supported)

The priority order is 1) user defined list, 2) operator defined list and 3) WLAN UE defined order (based on the implementation).

A.3.6 WLAN 3GPP IP Access End-To-End Tunnelling

The end-to-end tunnel in WLAN 3GPP IP Access is currently Internet Protocol Security (IPSec) and Internet Key Exchange (IKEv2) described in IETF RFC4306, based Virtual Private Network (VPN)-tunnel. The tunnel end-points are the UE and the Packet Data Gateway (PDG) in Home Wi-Fi Service Provider (also Visited Wi-Fi Service Provider case has been specified), and its purpose is to provide the user with a secure data access to the 3GPP-WLAN core network for accessing 3GPP PS based services (for example IMS). The tunnel establishment is initiated by the WLAN UE, specifically speaking a VPN client running in the WLAN UE, to the VPN gateway running in the PDG. A PDG is located using Wireless Access Point Names (W-APN) in a same way APNs are used in the mobile networks. The WLAN UE is authenticated during the IKEv2 negotiation using EAP-SIM/AKA/AKA'. After the IKEv2 IPSec tunnel establishment the user plane IP traffic from the WLAN UE gets securely routed through the PDG towards the external network pointed by the W-APN.

The WLAN UE constructs a FQDN using the W-APN Network Identifier and (V)PLMN ID as the Operator Identifier and performs a DNS query to resolve it. The DNS response will contain one or more IP addresses of equivalent PDGs that support the requested W-APN in the (V)PLMN according to standard DNS procedures. If the (V)PLMN does not support the W-APN, then the DNS query returns a negative response. The detailed DNS related information is documented in GSMA PRD IR.67.

3GPP has specified that there can be operator defined number of IPSec Sas per IKE SA. This information is configured into each PDG. The subscriber may have several simultaneous active tunnels set up (that is multiple IKE SAs). The maximum number of IKE SAs can be specified by the operator in the subscriber profile data.

A.4 Inter-Service Provider Interface (NNI)

Subscribers roaming in Wi-Fi Networks are authenticated and authorized using the Inter-Service Provider interface between the Visited Wi-Fi SP Network and the Home Wi-Fi SP Network. Another Inter-operator interface is responsible for the Data clearing or specifically the charging and settlement functionality. The Authentication, and Authorization Inter-operator interface is based on RADIUS as shown in the Figure 9. RADIUS is used to transfer the Authentication and Authorization information between the Visited Wi-Fi Network and the Home

Wi-Fi SP Core Network where the AAA Server resides. These transfers are made based on Roaming Agreements signed between the Wi-Fi SPs

The AAA information in the roaming case may be routed from the Visited Wi-Fi SP Network to Home Wi-Fi SP Network directly or using a single RADIUS proxy or a network of such proxies that work in tandem. Such a RADIUS proxy network is often used in complex Wi-Fi Network deployments across several geographies for optimal AAA routing purposes. It is possible for the same business entity to support the WLAN Roaming Proxy function using RADIUS proxies and the Data clearing functions.

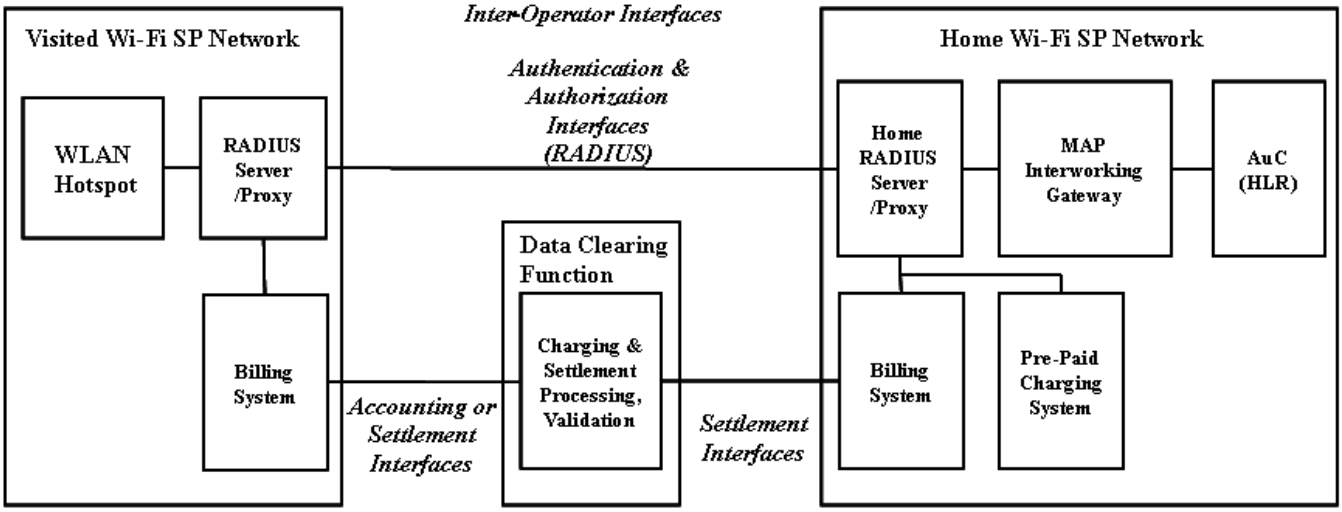

Figure 12: Inter-Operator Interfaces for AAA, Charging and Settlement

A.4.1 Radius Roaming Network

RADIUS Roaming Network is used for passing authentication, authorization and accounting data, AAA.

- AAA server requirements:
- AAA servers shall be capable of RADIUS Proxy.
- AAA servers shall be capable of identifying realms in a Username string and taking proxy action based on the realm.

Figure 10 gives an overview of how RADIUS Roaming Traffic is routed to different Roaming Partners based on Realms using IPX. Local user database in Figure 10 is an informative entity used only when inter-operator roaming is not used, that is user local access Wi-Fi service. It is therefore not directly related to actual inter-operator roaming.

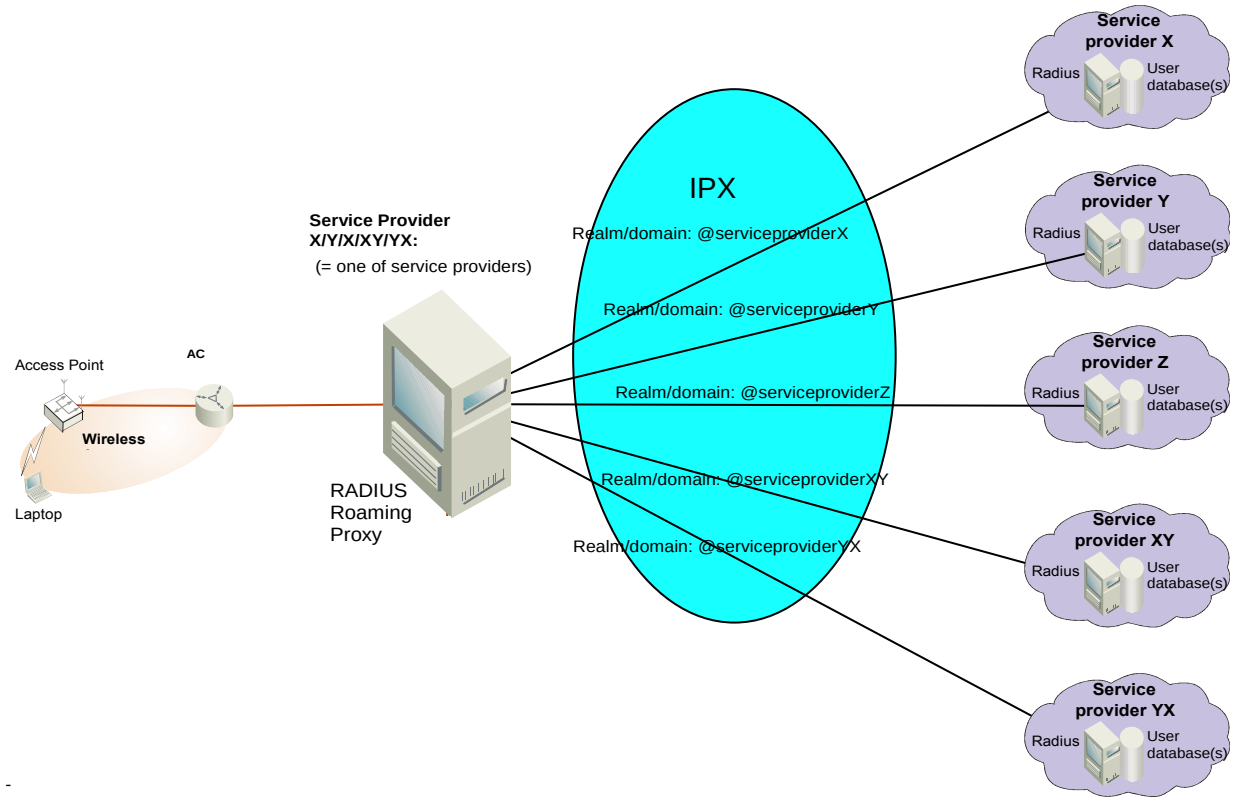

Figure 13: Logical overview from a provider's perspective how connection is made to the Roaming Partner networks. Service Provider X can represent any of the Roaming Partners.

Figure 10 also demonstrates how Roaming Partners actually connect to each other via Inter-Service Provider Network, e.g. IPX. During the Roaming login, user inserts their Username (with realm) & password and authentication request is proxied to Service Provider Y. User is then authenticated using the Service Provider Y's user database. Necessary RADIUS messages are transferred between RADIUS Roaming Proxies using the IP based inter-Service Provider network, e.g. IPX.

An IPX network is used for transporting RADIUS authentication and accounting messages for Wi-Fi roaming services.

A.4.1.1 Authentication and Authorisation

RADIUS Server controlling the Visited SP Wi-Fi will recognize the Realm and proxy the RADIUS Access-Request towards the identified Home Wi-Fi RADIUS Server based on Realm. Username and password are RADIUS parameters.

Local validation is ignored and Access-request is routed to the Home SP Wi-Fi SP authentication server.

The Home Wi-Fi Service receives the Access-request and authenticates the user, e.g. using PAP either EAP-SIM/AKA authentication.

Following authentication, during Home SP Wi-Fi RADIUS Server authenticates the user and sends an Access-Response to the Visited Wi-Fi SP RADIUS server. It should be noted, that

Home Wi-Fi SP carries out subscriber specific barring or prevention of Wi-Fi access. If the Home Wi-Fi SP sends a successful RADIUS Authentication Accept to Visited Wi-Fi SP, then the Visited Wi-Fi SP can assume that this subscriber is allowed to use the Wi-Fi service.

If the authentication was successful, the Visited Wi-Fi SP RADIUS Server enables session.

The Home Wi-Fi SP sends a subscriber identity to a Visited SP using Radius Chargeable User Identity attribute defined in IETF RFC 4372. It may include IMSI, Username or any other identity that is used for the billing purposes and is agreed with Roaming Partners.

A.4.1.2 Accounting and Log-out

When a new session starts, the following actions are performed:

1. Visited Wi-Fi SP RADIUS Server starts session statistics recording and sends RADIUS Accounting Start message to the Home Wi-Fi SP.
2. During connection the Visited Wi-Fi SP RADIUS Client checks if the connection is disconnected e.g. by radio connectivity loss or user inactivity timer expiry. If this occurs, RADIUS Accounting Stop message must be sent to the Home Wi-Fi Service.
3. Interim accounting messages shall be supported according to the requested time interval set by the Home Wi-Fi SP (e.g. to support prepaid and prevent fraud). It is recommended in RFC2869 that the interim time interval should not be smaller than 600 seconds. Time interval can be a part of IR.21 (or part of Wi-Fi Roaming Agreement).
4. A Log-out session window is provided by the Visited Wi-Fi SP.
5. When the user log-offs, the connection is terminated and the Visited Wi-Fi Service Provider´s RADIUS Client completes session statistics recording and sends RADIUS Accounting Stop message to the Home Wi-Fi SP.

A.4.1.3 RADIUS Attributes for Web Based Login

Basic RADIUS authentication and authorization is defined in RFC 2865. RADIUS accounting is defined in RFC 2866, while RADIUS extensions are defined in RFC 2869. The following list defines the minimum preferred RADIUS attribute set for the RADIUS servers and roaming proxies used in GSMA Wi-Fi roaming concept:

Required Attribute	#	Type	Auth Request	Auth Response	Acct'ing start	Acct'ing stop	Acct'ing interim	Comment
User-name	1	String	x		x	x	x	- Users NAI (includes Username and realm) - This is given by the user over SSL. - Authentication reply can be used to override the Username given by user
User-password	2	String	x					This is given by the user over SSL
NAS-IP-Address	4	Ipaddr	x		x	x	x	IP address of the Access Controller (the address of RADIUS client). This address is not necessarily a public IPv4 address (see Note (1)). This address has typically an operator internal significance. Within one WLAN session the NAS IP address shall remain constant.
Class	25	String		X	x	x	x	Class attribute is used to link authentication and accounting sessions in RADIUS server. This Attribute is sent by the Home RADIUS server to the client in an Access Response and MUST be sent unmodified by the RADIUS client in Visited Network as part of all the Accounting-Start packets. May be also used for e.g. fraud detection.
Session-timeout	27	Integer		X				Forced logout once timeout period reached (seconds). Can be used e.g. for pre-paid subscribers, to limit the potential financial loss from fraud cases, and to enable terminating on going accounting sessions in error cases (See note 2).
Acct-status-type	40	Integer			x	x	x	1=start, 2=stop, 3=Interim update
Acct-Input-	42	Integer				x	x	Volume of the downstream traffic of the user.

Required Attribute	#	Type	Auth Request	Auth Response	Acct'ing start	Acct'ing stop	Acct'ing interim	Comment
Octets								
Acct-Output-Octets	43	Integer				x	x	Volume of the upstream traffic of the user.
Acct-Session-ID	44	String			X	x	x	A session ID given by a NAS for a unique accounting correlation ID (between accounting start, interim and stop). Accounting and authentication messages related to a certain WLAN session will use the same session ID.
Acct-session-time	46	Integer				x	X	WLAN session duration in seconds
Acct-Input-packets	47	Integer				x	X	Number of packets (downstream)
Acct-output-packets	48	Integer				x	X	Number of packets (upstream)
Acct-terminate-cause	49	Integer				x		1=explicit logoff, 4=idle timeout, 5 =session timeout, 6=admin reset, 9=NAS error, 10=NAS request, 11 =NAS reboot
Acct-Input-Gigawords	52	Integer				X	X	Indicates how many times the Acct-Input-Octets counter has wrapped around its 4 byte length (i.e. Acct-Input-Gigawords > 0 when volume of the downstream traffic of the user exceeds 4 GB). Attribute present if needed
Acct-Output-Gigawords	53	Integer				X	X	Indicates how many times the Acct-Output-Octets counter has wrapped around its 4 byte length (i.e. Acct-Output-Gigawords > 0 when volume of the upstream traffic of the user exceeds 4 GB). Attribute present if needed
Event time stamp	55	Integer			X	x	x	Number of seconds elapsed since January 1 1970. UTC time.
NAS-port-type	61	Integer	x		x	x	x	15=Ethernet, 19=802.11

Required Attribute	#	Type	Auth Request	Auth Response	Acct'ing start	Acct'ing stop	Acct'ing interim	Comment
Acct-Interim-Interval	85	Integer		X				Interval (seconds) to send accounting updates given by Home operator. Needed e.g. if pre-paid is implemented between operators.
Operator-Name	126	String	x		x	x	x	This attribute defines the operator identity with which the roaming user's Home Operator has the roaming agreement. The operator identity can be e.g. used for Inter Operator Tariffing purposes. IETF RFC 5580 See Appendix A for more information about this vendor specific attribute.
Location-Information	127	String	x		x	x	x	This attribute defines the location of the operator the roaming user's Home operator has a roaming agreement with. Mandatory information in this attribute includes: ISO 3166 country code. The location information can be e.g. used for the end user roaming billing taxation, and roaming awareness purposes. See Appendix A for more information about this vendor specific attribute.
Location-Data	128	String	X		X	X	X	This attribute defines the name for the location of the operator the roaming user's Home Operator has a roaming agreement with. Locations are names as "Airport", "Hotel", "Mall" and so on. Refer the IETF DRAFT `draft-ietf-simple-rpid-02.txt` for the exact presentation of this attribute. See Appendix A for more information about this vendor specific attribute.
Vendor Specific Attribute Visited-Operator-ID	26, 15297 ,196	String	X		X	X	X	This attribute defines the Visited Operator identity with which the roaming user's Home operator has the roaming agreement. This attribute is used to identify the intermediating operator if there is no direct roaming relationship between the Visited Network Operator and the Home Network Operator. The Operator-Visited identity can be e.g. used for Inter Operator

Required Attribute	#	Type	Auth Request	Auth Response	Acct'ing start	Acct'ing stop	Acct'ing interim	Comment
								Tariffing purposes. See Appendix A for more information about this vendor specific attribute.

A.5 NOTES:

If a NAS-IP-Address is a private address; correlation of RADIUS-Accounting messages is not possible. Therefore this address should be a public one. However, an operator most likely has several access controllers and also several NAS-IP-Addresses. Thus achieving roaming awareness (i.e. from which Visited Wi-Fi SP the RADIUS Accounting message came via just this attribute is not practical. A Wi-Fi Service Operator would have to keep up to date lists of all the NAS-IP-Addresses of all its Roaming Partners. Furthermore, this attribute does not explicitly define the location of the Wi-Fi User, as there can be several hotspots under one Access Controller. A way to transport location information and to achieve better roaming awareness is for further study.

By using session timeout limiting the maximum length of a user session and thus limit the maximum loss that can occur after a user account is terminated because of fraud.

Also if for some reason no Acct-stop message is received from the Visited Wi-Fi SP in the Home Wi-Fi SP, there are two different possibilities to control it:

It is possible to terminate the accounting session if it is longer than the session timeout interval, therefore no accounting sessions are left open indefinitely. Leaving accounting sessions open may prevent users from logging in again if the Home WO does not allow more than one session per subscription. The session-timeout also limits the maximum loss for the customers if the Wi-Fi connection is left open and idle timeout mechanisms are not working ideally (e.g. when Users mobile terminal/client software is keeping the Wi-Fi connection alive).

Interim accounting timers are recommended and offer a more flexible way to control the session if some messages get lost. Recommended interval for sending Interim accounting messages is 20 minutes. However, if they are not supported by one of both Wi-Fi Roaming Partners, the solution is then applicable for managing the session when RADIUS messages get lost. Even if Acct-Interim messages are used, the Visited Wi-Fi SP should accept the Session-Timeout attribute sent by the Home Wi-Fi SP and use it to limit the maximum session length.

A.5.1.1 RADIUS Attributes for EAP-SIM, EAP-AKA' and EAP-AKA Usage

Basic RADIUS authentication & authorization is defined in RFC 2865. RADIUS accounting is defined in RFC 2866, while RADIUS extensions are defined in RFC 2869. EAP-SIM, EAP-AKA and EAP-AKA' using 802.1X are defined in RFC 3579, RFC 3580 and RFC4372. 3GPP 29.234 defines how the attributes are used in the GSMA Wi-Fi roaming.

A.5.1.2 Configuration

Configuration parameters:

RADIUS IP (public IPv4 address)
Within the first phase it is expected that static mappings are used to find RADIUS Roaming Proxies, thus DNS is not utilized.

Shared Secret encryption is limited to the password. For this reason the Shared Secret must be delivered to each Roaming Partner. If an IPX is used as inter-operator network, then Shared Secret could offer enough security, since the IPX is a private network.

However, if an inter-operator network is based on public Internet, inter-connection MUST be protected by an IPSec VPN tunnel, in addition to the RADIUS Shared Secret encryption, since VPN offers a higher level of security.

RADIUS Message Encryption
It is beneficial to secure RADIUS messages between Home Wi-Fi SP and Visited Wi-Fi SP. If IPX is used as an inter-operator network, then Shared Secret could offer enough security since IPX is a private network. However, if public Internet is used as an inter-operator network, then it IPSec ESP VPN with 3DES encryption is recommended to secure RADIUS messages. Options are not limited to that, for example DES could be used instead of 3DES, if 3DES is not allowed due to regulations.

Actual parameters of VPN should be bilaterally agreed on, however, both parties need to have identical configurations. Because of this, it is recommended that the parameters given in Table 5.1.6 be used to facilitate setting up IPSec connections and IKE if dynamic keying is to be used.

NOTE: This VPN is deployed only between RADIUS Roaming Proxies of Visited Wi-Fi SP and Home Wi-Fi SP, thus RADIUS Message Encryption is not related to any kind of VPN used between MT and e.g. corporate network.

Ports(UDP)
Recommended standard is port 1812 and 1813.

Summary of IKE Settings	
Diffie-Hellman Group	2
Protocol	Encapsulating Security Payload
Mode	Main
Authentication	Pre-shared secrets
Identities	IPv4
Encryption Algorithm	3DES (or DES if using 3DES illegal for V/H WO)
Authentication Algorithm	SHA1
Lifetime	28800 seconds, 0 kbytes

The preferred way to establish security associations	On per-host basis for compatibility and performance reasons. Port level filtering can be done in private interfaces with e.g. outbound lists.

Summary of IPsec Settings	
Protocol	Encapsulating Security Payload in Tunnel Mode
Encryption Algorithm	3DES (or DES if using 3DES illegal for V/H WO)
Authentication Algorithm	SHA1
Lifetime	28800 seconds, 0 kbytes
Perfect Forward Security	No

Figure 14: Recommended IPSec Parameters

A.5.1.3 Realms

The user needs to provide the Username, which is of the form of a Network Access Identifier NAI as defined in RFC 4282. This NAI shall be of the form: Username@Realm.

The Username in NAI identifies a unique user in the domain described by the Realm. The Realm shall be a fully qualified domain name signifying the Home Wi-Fi SP.

A.5.1.4 Roaming Implementation

This informative section lists issues that are needed in order to implement Wi-Fi Roaming using RADIUS:

In case of Web-based login, Wi-Fi services shall be open and WEP encryption not to be used.
Inform each Roaming Partner about:

- Shared Secret
- RADIUS Roaming Proxy/DNS
- Ports (UDP)
- Realms

The firewalls shall be open for each connection between two IP-addresses and ports.

NOTE: That only public IPv4 addresses should be used in roaming proxies.

RADIUS Servers have to be configured so that remote RADIUS Servers are clients for the local RADIUS Server. Shared secrets for each connection have to be defined.

RADIUS Roaming Proxy features should be configured so that certain Realm is mapped to the certain IP-address/port.

Usernames and passwords for the testing have to be delivered for each Roaming Partner.

Define Test Instructions: Perform tests according to Test Instructions.

A.5.2 Radius Attributes for EAP-AKA AND EAP-AKA' Application

The required RADIUS attributes for EAP-AKA and EAP-AKA' authentication are exactly the same as for the EAP-SIM.

A.6 Co-Existence and Migration

A.6.1 Web Based Authentication and 802.1x Authentication

Web based login using username/password authentication is considered as an existing solution for the Wi-Fi authentication when the target solution today is an EAP based authentication solutions. It is important still that it is possible for existing solutions to work as long as justified from a business perspective beside the target solution. Going even further HS2.0 brings a new target, reusing EAP methods with new automated network discovery functionality.

To support EAP-SIM/AKA/AKA'/TLS/TTLS based roaming, it is expected that the Visited Wi-Fi Service Provider supports 802.1X and WPA (Wi-Fi Protected Access) or WPA2. WPA is a standards-based specification that provides an interoperable security solution for accessing Wi-Fi services. WPA2 is also a standards-based specification that provides enhanced security than WPA presenting Advanced Encryption Standard (AES) encryption.

To support relevant aspects of HS2.0 from roaming point of view does not bring anything new to the existing roaming interface. The new features are between Mobile Terminal and a Wi-Fi access point. The main HS2.0 features required to the Mobile device are support for automatic network selection based on 802.11u and support for WPA2-Enterprise data encryption. HS2.0 also includes the fall-back functionality, in case that device is equipped with HS2.0 capabilities but the networks are not. In that case user must use other methods to find correct SSID.

A.6.1.1 Web Based Authentication Using Home Wi-Fi SP Login Page

The web based username/password authentication shall be supported in the Visited SP Network as described in Chapter 4. However, there can be roaming cases where enabling additionally the use of Home Wi-Fi SP login page in Visited Wi-Fi SP Network can be necessary. Some operators may require the functionality for their login method to work (for example some implementations that send One Time Passwords via SMS). Additionally in this solution, the login and help/other informational pages can be displayed in a language chosen by Home Wi-Fi SP.

While displaying the Home Wi-Fi SP login page in the Visited Wi-Fi SP Network should not be mandated, it can be bilaterally agreed on within the Roaming Agreements. Described below is a recommendation how to implement a redirection to a Home Wi-Fi SP login page in a way that ensures maximal interoperability and minimal effect on the roaming infrastructure. The described mechanism can be implemented without changing the Visited

Wi-Fi SP Network RADIUS elements. This is because the mechanism works on the http(s) level, the RADIUS message flow does not change.

The proposed roaming functionality requires some modifications both to Home and Visited Wi-Fi SP Network's web login page hosting elements. It also introduces WWW-proxy server to Visited Wi-Fi SP Network that forwards the parameters used in Visited login page's http(s) post operation to the access controller. The Home Wi-Fi SP Network needs to implement a WWW server that hosts their login page(s) and can use the parameters from the Visited Wi-Fi SP Network.

A.6.1.2 Sign-on Procedure

After being redirected to the Visited Wi-Fi SP login page, the user selects his Home Wi-Fi SP (for example from a drop-down list). The user is then directed to the Home Wi-Fi SP login page. The user performs a login to the Wi-Fi using that page. The user needs to provide the Username, Password, and the realm as described in chapter 4.

A.6.1.3 Secure Login

The Web based login shall use SSL for secure transmission of the user credentials.

A.6.1.4 Protocol Implementation

The Web based login described above is implemented by the Access Controller (AC), Visited Wi-Fi SP WWW-proxy, and Home Wi-Fi SP WWW-server.

When the user first tries to browse the Internet, performing an HTTP Get, the browser is redirected to the Visited Wi-Fi SP login page. The Home operator choice is forwarded to the Visited Wi-Fi SP WWW-proxy-server in a HTTP(S) Get. The Visited WWW-proxy forwards it as an HTTP(S) Post to Home SP WWW-server. The Visited Wi-Fi SP adds hidden attributes to the HTTP(S) Post that inform the Home network about the correct address to which the final html-form should be submitted. The Home WWW-Server is capable of changing its login page's variable names using the hidden attributes. Because the variables must be the same in both Visited and Home Wi-Fi SP Networks, a recommended format is presented in Table 6.1.4.

Variable Name	Variable's function	Example
Username	Stores the variable name for the username-attribute. The username-attribute also contains the realm.	$username = "user@realm"
Password	Stores the variable name for the password-attribute	$password = "pwd"
loginPostURL	Stores the address to which the HTML-Form is submitted	$loginPostURL = "192.168.1.1/cgi-bin/login"

Table 1: Recommended Format for Parameters

Using the variables above, the Home Wi-Fi SP Network modifies its login page's parameters to use the Visited Wi-Fi SP Network's login page's parameters. The user enters a Username/Password-pair to the Home Wi-Fi SP login page and this is sent using the

received attributes via an HTTP Post to the Visited Wi-Fi Service Provider´s AC. The resulting RADIUS message flow is as described in chapter 4.

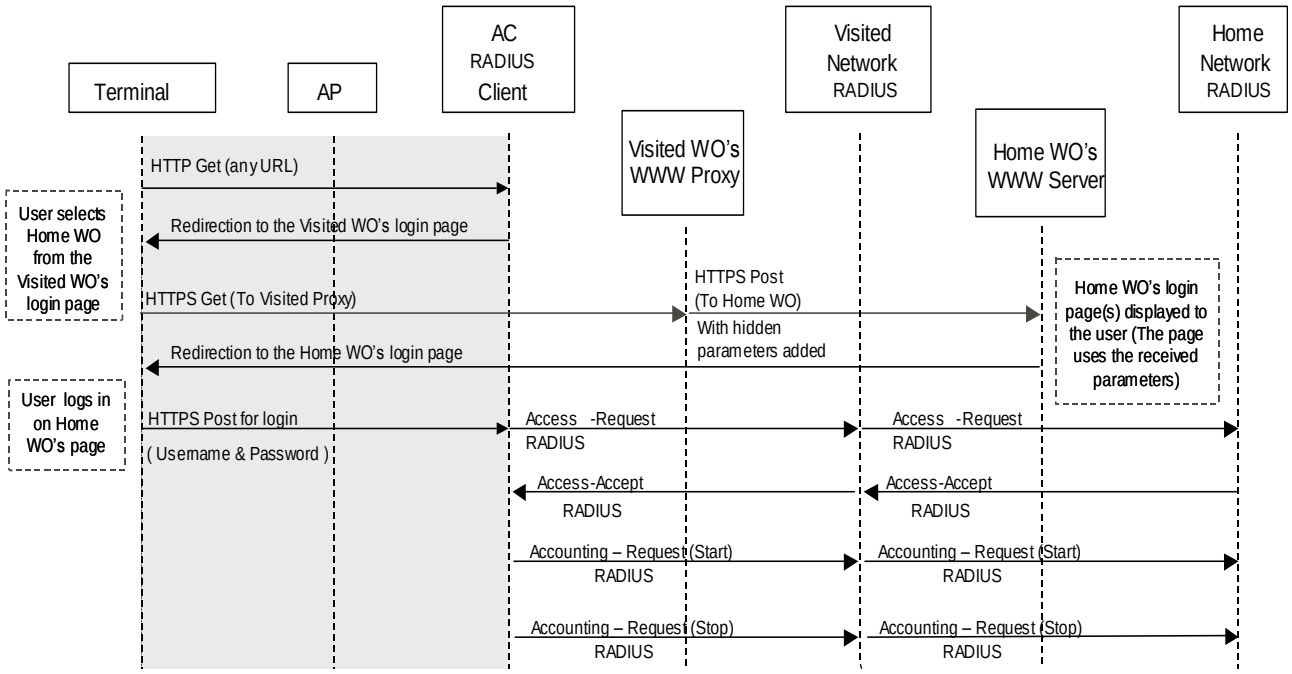

Figure 15: Overview of Login Message Flow Using Home WO Web-Page

NOTE: All RADIUS accounting messages are acknowledged even though this is not presented in Figure 11.

There is no mandatory behaviour for the HTTP login response. Depending on business considerations the Visited Wi-Fi SP Network may decide to push as a HTTP response to the logon procedure one or multiple pages. Those pages could be any of the following:

- Simple login result page
- Status
- Portal page from either the Visited network, Home operator, or hotspot location or
- Any other page

The Visited Wi-Fi SP is the master of the user's session and status. Therefore it is up to the Visited Wi-Fi SP how this information is displayed to the user.

A.6.1.5 Home Wi-Fi SP Information-Page (optional)

If bilaterally agreed on, the Home operator can provide an additional info-page for its users.

The info-page could inform the user about, but not limited to, the following items:

- Context Help
- User Information

- Additional Session Information (for example price)
- Helpdesk Information
- Logout-Button for the Visited WO

The info page should be called by a HTTP-Get request with the following parameters:

Variable Name	Variable's function	Example
Username	Stores the username of the user requesting status information.	$username = "user@realm"
LogoutPostURL	Stores the address to which the HTML-Form is submitted	$logoutPostURL = "192.168.1.1/cgi-bin/login"

Table 2: Recommended Format for Info Page Parameters

Annex B Document Management

B.1 Document History

Version	Date	Brief Description of Change	Approval Authority	Editor / Company
0.0.1	June 6th, 2002	First draft created in WLAN TF ("version A")	EMC/IREG	
0.0.2	June 7th, 2002	Version after WLAN TF Stockholm meeting ("version B")	EMC/IREG	
0.0.3	July 4th, 2002	Version after WLAN TF conference call (4th of July) ("version C")	EMC/IREG	
0.0.4	August 22nd, 2002	Version after WLAN TF conference call ("version D"), presented to IREG plenary in Singapore	EMC/IREG	
0.0.5	September 19th, 2002	Version based on discussions and agreements in WLAN TF /(IREG) Singapore meeting ("version E")	EMC/IREG	
0.0.6	September 27th, 2002	Version approved by WLAN TF in Portland ("version F"), presented to Packet WP in Madrid (November 2002)	EMC/IREG	
0.0.7	January 17th, 2003	Version after Packet WP ad-hoc in Düsseldorf	EMC/IREG	
0.0.8	February 11th, 2003	Version after Packet WP Yokohama meeting (IREG Doc 026/03 Rev 1)	EMC/IREG	
3.0.0	April 23rd, 2003	Approved by EMC	EMC/IREG	
3.0.1	November 3rd, 2003	Incorporated PACKET Doc 074_03 (NCR 001 on IR.61)	EMC/IREG	
3.0.2	October 24th, 2003	Incorporated IREG Doc 46_028 (NCR 002 on IR.61)	EMC/IREG	
3.0.3	October 24th, 2003	Incorporated IREG Doc 46_029 (NCR 003 on IR.61)	EMC/IREG	
3.1.0	August 25th, 2004	Incorporated IREG Doc 47_019 (SCR 005 on IR.61) and IREG Doc 47_016 (NCR 004 on IR.61)	EMC/IREG	
4.0	June 25th, 2007	Incorporated IREG Doc 52_038 (3GPP Release-6 WLAN interworking)	EMC/IREG	
5.0	February 15th, 2012	DAG documents 088_028rev1, 88_029rev1, 88_030rev1, 88_031rev1, 88_032 and 88_033 incorporated	EMC/IREG	Marko Onikki TeliaSonera
6.0	2013	DAG Docs 99_016, 99_017	DAG99	Marko Onikki TeliaSonera
7.0	2014	Incorporated CR1001 (Support for EPC integrated Wi-Fi	IREG	Marko Onikki TeliaSonera
8.0	July 28th, 2014	Incorporated CR1002 and CR1003	IREG	Marko Onikki TeliaSonera
9.0	November 19th, 2014	Incorporated CR1004	IREG	Marko Onikki TeliaSonera

Version	Date	Brief Description of Change	Approval Authority	Editor / Company
10.0	May 5th, 2015	Incorporated CR1005, 1006 and 1007	IREG	Marko Onikki TeliaSonera

Other Information

Type	Description
Document Owner	IREG
Editor / Company	Marko Onikki / TeliaSonera

Feedback

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

Your comments or suggestions & questions are always welcome.