PRD IR.61

Title   WLAN Roaming Guidelines (also known as Inter-Operator Handbook)

Version   3.0.0
Date   April 2003

GSM Association Classifications

Non-Binding

Non-Core

Security Classification Category:	Please mark with "X" where applicable
Unrestricted - Public	**X**

Information Category	Roaming & Interworking – Technical

Document History		
Revision	**Date**	**Brief Description**
0.0.1	June 6th, 2002	First draft created in WLAN TF ("version A")
0.0.2	June 7th, 2002	Version after WLAN TF Stockholm meeting ("version B")
0.0.3	July 4th, 2002	Version after WLAN TF conference call (4th of July) ("version C"
0.0.4	August 22nd, 2002	Version after WLAN TF conference call ("version D"), presented to IREG plenary in Singapore
0.0.5	September 19th, 2002	Version based on discussions and agreements in WLAN TF /(IREG) Singapore meeting ("version E")
0.0.6	September 27th, 2002	Version approved by WLAN TF in Portland ("version F"), presented to Packet WP in Madrid (November 2002)
0.0.7	January 17th, 2003	Version after Packet WP ad-hoc in Düsseldorf
0.0.8	February 11th, 2003	Version after Packet WP Yokohama meeting (IREG Doc 026/03 Rev 1)
3.0.0	April 23rd, 2003	Approved by EMC

TOC

1.   Abbreviations and Terminology

Abbreviation	Term	Description
WLAN	Wireless Local Area Network	Usually referred to the IEEE 802.11 product family.
WISP	Wireless LAN Internet Service Provider	
MNO	Mobile Network Operator	
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.
WO	WLAN Operator	Owner and/or Provider of WLAN network infrastructure. This entity could be a Mobile Network Operator (MNO) or a Wireless Internet Service Provider (WISP).
AC	Access Controller	
	Roaming Service	Roaming Service in this document means provision of Internet service over WLANs for customers of another WO, a.k.a 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
	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.
	RADIUS Roaming Proxy (WLAN Roaming Proxy)	RADIUS Roaming Proxy (or WLAN Roaming Proxy) shall mean a component transporting RADIUS messages from visited WLAN operator to home WLAN operator (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.
	Customer	A business entity or an individual with a direct contractual relation to receive the Service from the Home WLAN Operator.
	User	The individual receiving the Service.
Home WO	Home WLAN Operator	The Party contracting to provide the Service to its own Customers and which authenticates and charges the customer.
Visited WO	Visited WLAN Operator	The Party providing the Roaming Service to the Customer of the other Party.
PLMN	Public Land Mobile Network	

	Accounting	The process of collecting resource usage measurements and apportioning charges for joint service between interworking an/or co-operating service/network providers.
	Billing	A function whereby Call Detail Records generated by the charging function are transformed into bills requiring payment
	Settlement	
AP	Access Point	Interface between the radio network part and the wired network part of a WLAN network, offering wireless connectivity to MTs
	Home WLAN	The network operated by the H-WLAN Operator.
	Visited WLAN	The network operated by the V-WLAN Operator.
BARG	Billing, Accounting, and Roaming Group	Working Group within GSMA.
IREG	International Roaming Experts Group	Working Group within GSMA.
TADIG	Transferred Account Data Interchange Group	Working Group within GSMA.

2. Basic Information

2.1. Scope

The main purpose of this document is to specify a common technical solution for Roaming Service between WLAN operators (WO) from an inter-operator perspective. This document is to be used as a baseline for work in GSMA.

It shall cover the following aspects:

- Access interfaces including connection procedures 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)

The scope of this document is to describe an interoperable way to implement RADIUS based roaming using username/password authentication. Thus, the current scope of this document is focused on RADIUS based roaming.

In the future, there will most likely be an interoperable way to implement SIM based authentication. 3GPP is working to define such a mechanism. 3GPP has also decided to implement inter-operator interface based on AAA protocol (DIAMETER). This means that also SIM based authentication can be implemented without using MAP between operators. 3GPP will not (in WLAN context) define how MAP protocol should be used between operators. In the future, WLAN TF aims to release a document detailing developments of SIM based roaming solutions.

GSMA / WLAN Task Force acknowledges the value of using SIM in WLAN environment. Currently, username/password + RADIUS based is more complete in this document than SIM based roaming.

The scope of this document includes interoperable solutions, which can be deployed before 3GPP Release 6 specifications become available. It is understood that, the current solution for authentication is Web based login using Username and Password with RADIUS as the backend protocol. This document therefore discusses roaming using Web based Username/Password procedures in detail. **It is foreseen that SIM based roaming would be needed using EAP/SIM over 802.1X. This work is in progress within WLAN TF inter-operator handbook group.**

As 3GPP is independently developing SIM/USIM based authentication solutions for WLAN. WLAN TF needs to address co-existence and migration issues with respect to the different solutions in the future.

2.2. Description of Service

The term 'Roaming Service' in this document refers to provisioning of Internet service over WLANs for customers of a 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. The service is described in a roaming agreement between the Roaming Partners. The Home WO charges the customer and the Visited WO charges the Home WO for providing the Roaming Service.

3.   Roaming Network Architecture

The WLAN reference roaming architecture described here defines open interfaces for Access and Inter-operator roaming. This architecture when implemented enables users to globally access WLANs as long as roaming agreements are in place between the WOs (MNOs providing WLAN or WISPs).
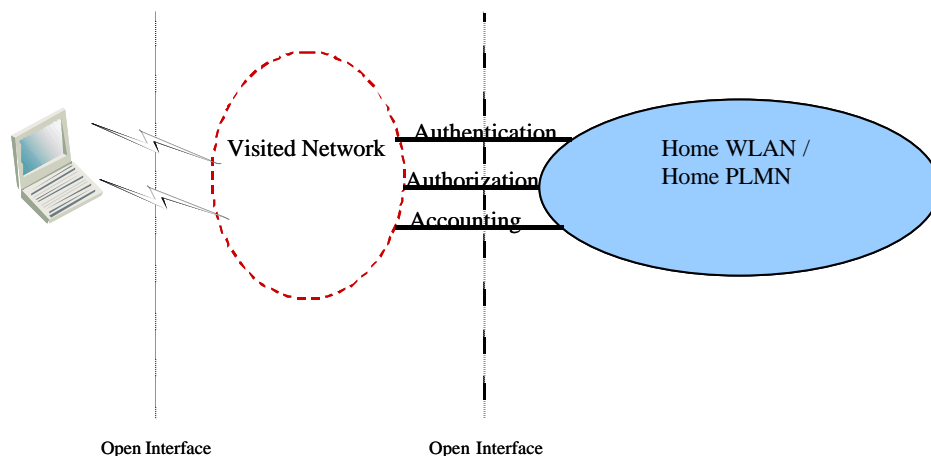

Figure 1: WLAN Roaming Reference Architecture.

Note that although authorization is referenced in Figure 1, it is not addressed in detail within this document. This is done in other specifications, for example RADIUS and IPsec related RFCs specify how authorization is handled.

Two sets of interfaces are required to support the roaming, one between the MT (Mobile Terminal) and the Visited WLAN and another set between Visited WLAN and Home WLAN. These interfaces are based on standard protocols defined by IEEE and IETF and available in most industry implementations.

The first set of interfaces as a minimum is required to provide authentication of the user and optionally *authorization*. The User authentication mechanism being proposed is Web based login, using Username/Password over a SSL link with a Web Server hosted by the Visited WLAN.

The second set of interfaces is between the Visited WLAN and the Home WLAN. This set of interfaces shall perform at least two functions: Authentication and Accounting. In addition, *Authorization* may also be supported. For Username/Password roaming the protocols are following:

-    Authentication protocols: RADIUS

-    Accounting protocols: RADIUS, TAP

-    *Authorization protocols: RADIUS*

Accounting based on RADIUS or TAP is possible and they can even co-exist for WLAN roaming within GSMA. RADIUS accounting messages shall always be transferred between Home WO and Visited WO especially for fraud monitoring and other requirements. TAP is the recommended method for billing and settlement of WLAN

Roaming Services. Hence, this document currently does not recommend any billing and settlement procedures for RADIUS accounting.

An inter-operator network is needed when WLAN roaming between WOs is used. This is due to the fact that RADIUS Roaming Proxy in visited network needs to be able to connect to RADIUS Server in home network, since RADIUS Server located in home network is always responsible for e.g. actually authenticating the user, regardless of whether he is roaming or not. This inter-operator interface is always based on IP. Note that home network generally can be considered to be either home WLAN or PLMN, in any case it is where the home AAA Server is located.

GRX is the preferred solution for IP based Inter PLMN network (between RADIUS Servers) roaming between WO which are MNOs, as it is for other inter-operator IP traffic purposes, e.g. GPRS roaming and MMS interworking. For traffic between WISP, or between WISP and WO-MNOs alternative solutions such as IPSec should be used. Issues such as quality of service, security, control of interworking networks, overall reliability and issuing of new network features are easier handled inside GRX than when using public internet to relay RADIUS based roaming traffic between WOs. It should be noted that this does not in any way prevent WOs from using also e.g. public Internet as a inter-PLMN network, if needed. Security issues related to RADIUS based roaming need to be addressed (e.g. RFC 2607).

4. Access Interface

This section describes how the roaming user connects to the WLAN, and the related procedures and the messaging flow.

4.1. MT Association to the WLAN

For association to the WLAN, the minimum requirement is knowledge of the Visited WLAN SSID. There are three basic methods for this association to occur:

- Manual configuration of the MT with the right SSID

- Media sensing, browsing and selecting the right SSID

- Automatic selection of SSID (Supported by some MTs. e.g. Windows® XP™)

The other possible ways to associate needs to be studied in the usability paper, see GSMA WLAN TF "Services & Ease of Use in Interworked WLAN-Cellular Systems" document for further information.

4.2. Sign-on Procedure

The user performs a login to the WLAN using the login page provided by the Web browser. The user needs to provide the Username, which is of the form of an Network Access Identifier NAI as defined in RFC 2486. 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 needs to be a fully qualified domain name, which signifies the Home WLAN. After the Username@realm entry, a password is entered for authentication process. The login page shall mask the password entered.

The visited WO 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).

4.3. Secure Login

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

4.4. 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 an HTTP Get, using the WLAN, the browser is redirected to the login page. The user enters the Username/Password and this is sent using a HTTP 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 WLAN Radius Server. The rest of the key messages are shown in the figure.
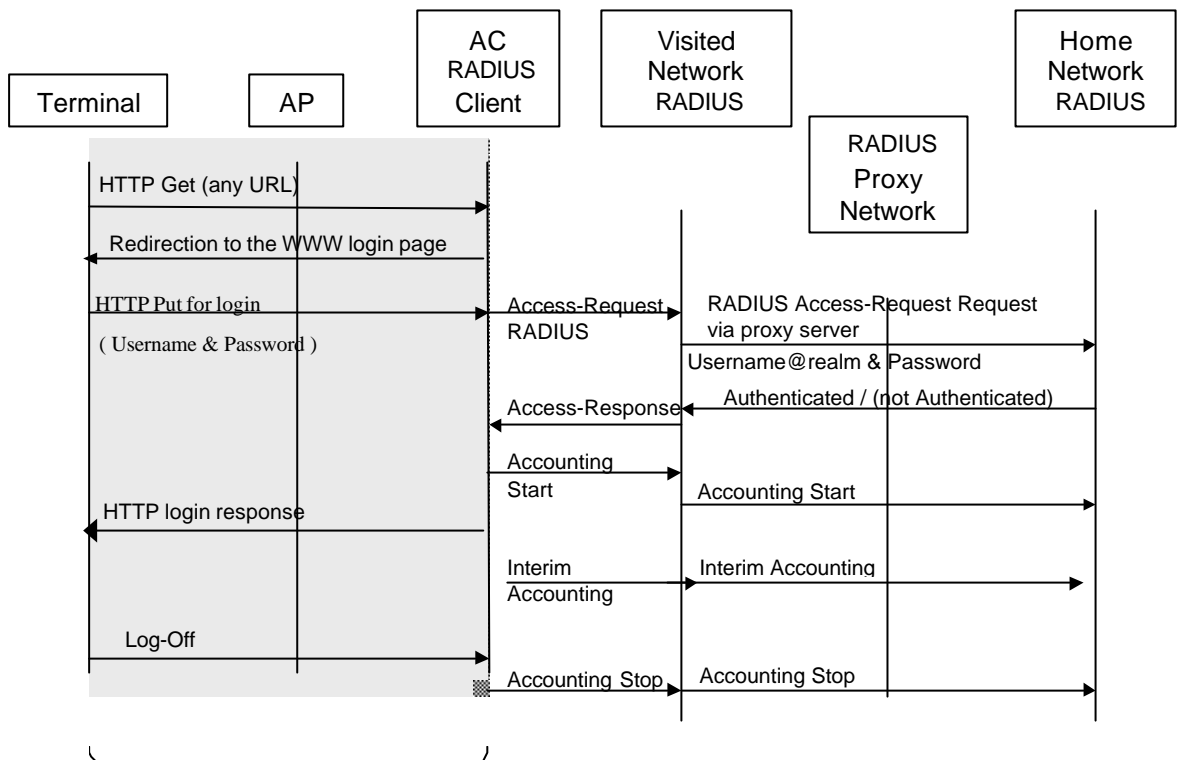
Figure 2: Web Based Login Message Flow Overview

Note: All RADIUS accounting messages are acknowledged even though this is not presented in Figure 2.

There is no mandatory behaviour for the HTTP login response. Depending on business considerations the visited 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

- Portal page from either the visited network, home operator, or hotspot location

- Any other page

5.   Inter-operator Interface

Inter-operator interface is required to transfer authentication information to the correct authentication elements between WOs. This chapter describes the RADIUS Roaming Network.

5.1.   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 3 gives a logical overview how RADIUS roaming traffic is routed to different Roaming Partners based on Realms. Local user database in Figure 3 is an informative entity used only when inter-operator roaming is not used, i.e. user locally accesses WLAN service. It is therefore not directly related to actual inter-operator roaming as such.
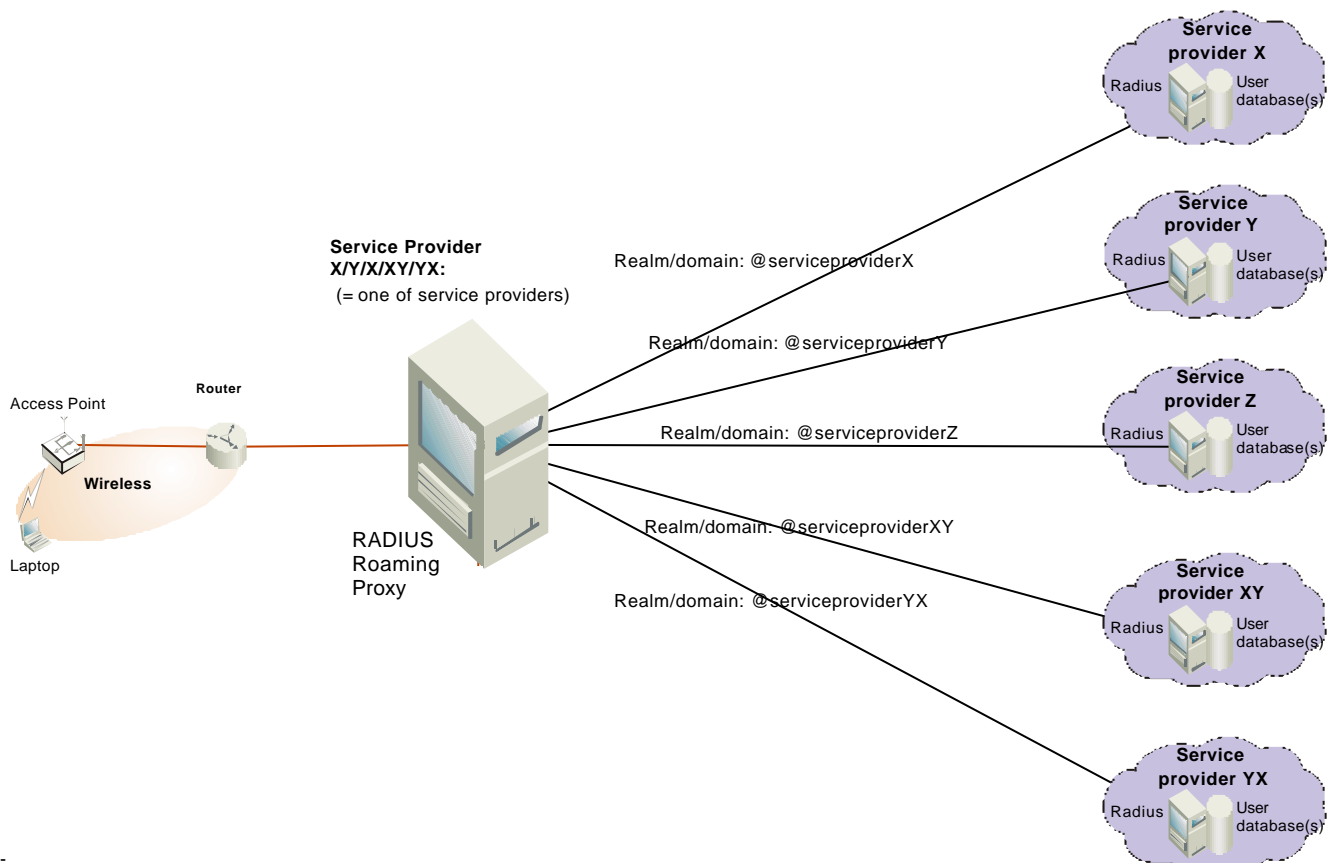

Figure 3: Logical overview from one provider's point of view how connection is made to the Roaming Partner networks. Service Provider X can represent any of the Roaming Partners.

Figure 4 shows how local login and roaming login differ, it also demonstrates how Roaming Partners actually connect to each other via inter-operator network. Case 1 is an example of normal local login, where user inserts his username & password and is authenticated in local user database. In this case RADIUS Roaming Network is not utilized.

Case 2 in Figure 4 refers to roaming bgin, where user inserts his 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-PLMN network, e.g. GRX.
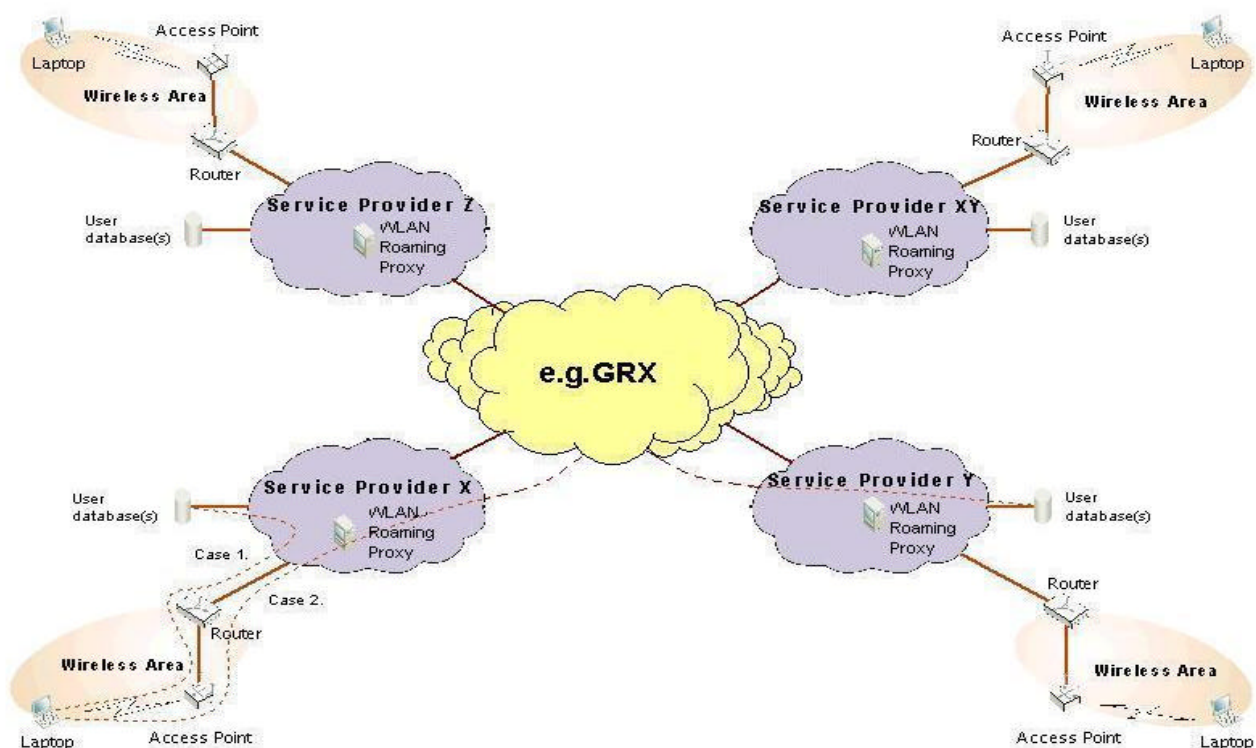
Figure 4: Roaming Network Overview

GRX network is used for transporting RADIUS authentication and accounting messages for WLAN roaming services. At this stage, WLAN user data is not carried over GRX.

When using GRX network for the WLAN roaming, IP the address of the WLAN Roaming Proxy must be reachable via GRX.

5.1.1. Authentication and Authorisation

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

Local validation is ignored and Access-request is routed to the Home WLAN authentication server.

The Home WLAN receives the Access-request and authenticates the user.

2. Home WLAN RADIUS Server authenticates the user and sends an Access-Response to the Visited WLAN RADIUS server. It should be noted, that Home WO carries out subscriber specific barring or prevention of WLAN access. If Home WO sends a successful RADIUS Authentication Accept to Visited WO, then the Visited WO can assume that this subscriber is allowed to use the WLAN service.

3. If the authentication was successful, the Visited WLAN RADIUS Server enables session.

4. Since the user id may not correspond to some TAP chargeable subscriber types (IMSI), techniques may need to be defined to allow the home operator to provide a unique chargeable subscriber identity to be subsequently used in TAP procedures. TADIG has also extended TAP specifications to support WLAN roaming (both username@realm and IMSI is supported). If home WO does not want to send IMSI in plaintext, the RADIUS message can be ciphered using IPsec (as described in section 5.1.4).

5.1.2. Accounting and Log-out

When a new session starts following actions are performed:

1. Visited WLAN RADIUS Server starts session statistics recording and sends **RADIUS Accounting Start** message to the Home WLAN.

2. During connection the Visited WLAN RADIUS Server checks if the connection is disconnected e.g. by radio connectivity loss or user inactivity timer expiry. If this should happen, **RADIUS Accounting Stop** message must be sent to the Home WLAN.

3. Interim accounting messages shall be supported according to the requested time interval set by the Home WLAN (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 WLAN roaming agreement).

4. Log-out session window is provided by Visited WLAN.

5. When the user log-offs, the connection is terminated and the Visited WLAN RADIUS Server completes session statistics recording and sends **RADIUS Accounting Stop** message to the Home WLAN.

6. TAP records may be generated using the TAP chargeable identity provided during RADIUS authentication and authorization (as

described in previous chapter).

5.1.3. RADIUS Attributes

Basic RADIUS authentication & 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 used in GSMA WLAN roaming concept:

Required Attribute	#	Type	Auth-Request	Auth-Response	Accounting start	Accounting stop	Accounting 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	Can be used to transfer GPRS chargeable subscriber for TAP (i.e. IMSI). May be also used for e.g. fraud detection. Preferred way is to utilize Class instead of User-name field to transfer GPRS chargeable subscriber. TAP 3.10 can support both IMSI and username@realm. Thus, this parameter is optional. Some operators do not want to send IMSI in RADIUS messages due

								to security reasons.
Session-timeout	27	Integer		X				Forced logout once timeout period reached (seconds). Can be used e.g. for pre-paid subscribers.
Acct-status-type	40	Integer			X	X	X	1=start, 2=stop, 3=Interim update
Acct-Input-Octets	42	Integer				X	X	Volume of the downstream traffic of the user.
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
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
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.

Note (1): If NAS-IP-Address is a private address, correlation of Radius-Account messages is not possible. Therefore this address should be a public one.

5.1.4. Configuration

Configuration parameters:

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

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

  However, if inter-operator network is based on public Internet, it is recommended that RADIUS messages should be protected by VPN instead of Shared Secret encryption, since VPN offers a higher level of security (see next bullet).

- RADIUS Message Encryption
  It is beneficial to secure RADIUS messages between Home WO and Visited WO. If GRX is used as an inter-operator network, then Shared Secret (see previous bullet) could offer enough security since GRX 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 must be bilaterally agreed on, thus both parties should have identical configuration.

  Note that this VPN is deployed only between RADIUS Roaming Proxies of Visited WO and Home WO, 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.

5.1.5. Realms

The user needs to provide the Username, which is of the form of a Network Access Identifier NAI as defined in RFC 2486. 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 WLAN.

5.1.6. Roaming Implementation

This informative section lists issues that are needed in order to implement WLAN roaming using RADIUS:

1. IEEE 802.11b WLAN shall be open and WEP encryption not to be used.

2. Inform each Roaming Partner about:
   - Shared Secret
   - RADIUS Roaming Proxy/DNS
   - Ports (UDP)
   - Realms

3. 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.

4. 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.

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

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

7. Define Test Instructions.

8. Perform tests according to Test Instructions.

6.   Co-Existence and Migration

6.1.   Web based authentication and 802.1x authentication

Web based login using username/password authentication shall be considered as an existing first phase solution for the WLAN authentication. However, there shall be a target solution in the future (EAP based solutions). It is important that it is possible for existing solutions to work as long as justified from a business perspective beside the target solution.

However, as soon as feasible, GSMA supports the intelligent introduction of 802.1X in its WLAN roaming concept. The introduction of 802.1X compliant Access Points and Clients are expected to create the necessary foundations for increased security.

The migration path from the present Web based login (username/password authentication) and 802.11b based access towards to full 802.1X environment should be done gradually ensuring co-existence of both solutions. GSMA endorses the notion of building access zones that are both 802.11b and 802.1X compliant. Note that this might require an upgrade to access points, access controllers and client software.

7. Commercial roaming framework for WLAN

In order to support WLAN Roaming between WOs, a Roaming Agreement is needed. BARG has followed the agreement structure used in GPRS roaming: to have an addendum to existing GSM roaming agreement. This addendum is covering the WLAN specific issues. BARG is also aiming to create a stand-alone document for WLAN roaming agreement.

This document concentrates on direct inter-operator WLAN Roaming, but it should be noted that this does not in any way prevent anyone from using e.g. roaming brokers. This means that there can be other kind of roaming agreements in addition to direct bilateral inter-operator WLAN Roaming Agreement, if necessary.

The charging principles for WLAN are defined in BARG PRDs (e.g. BA.27).

BARG and TADIG have defined TAP procedure to support WLAN roaming billing. This is available in TAP version 3.10.

Radius accounting messages can be transferred between Home WO and Visited WO. This might have a value e.g. for early roaming trials and fraud detection. Currently, there are no GSMA defined inter-operator billing and settlement procedures for RADIUS accounting.

Roaming Agreement issues with external entities (e.g. WISPs) should also be taken into account by GSMA.

8.   References

Title	Subject	Source	Destination
Remote Authentication Dial In User Service (RADIUS)	Internet standards track protocol	IETF	http://www.rfc-editor.org/rfc/rfc2865.txt
RADIUS Accounting	RADIUS Accounting protocol	IETF	http://www.rfc-editor.org/rfc/rfc2866.txt
RADIUS Extensions	AAA attributes	IETF	http://www.rfc-editor.org/rfc/rfc2869.txt
PPP Extensible Authentication Protocol (EAP)	EAP	IETF	http://www.rfc-editor.org/rfc/rfc2284.txt
EAP SIM Authentication (draft-haverinen-pppext-eap-sim…)	EAP/SIM	IETF	http://www.ietf.org/internet-drafts/
IEEE 802.1X RADIUS Usage Guidelines (draft-congdon-radius-8021x…)	802.1X	IETF	http://www.ietf.org/internet-drafts/
The ESP Triple DES Transform	ESP VPN with 3DES	IETF	http://www.ietf.org/rfc/rfc1851.txt
Security Architecture for the Internet Protocol (RFC 2401)	IPsec	IETF	http://www.ietf.org/rfc/rfc2401.txt
GPRS Roaming Guidelines (PRD IR.33)	GRX	GSMA	https://infocentre.gsm.org/cgi-bin/prdind.cgi?IR
Inter-PLMN Backbone Guidelines (PRD IR.34)	GRX	GSMA	https://infocentre.gsm.org/cgi-bin/prdind.cgi?IR
Charging and Accounting Principles (PRD BA.27)	IOT rules	GSMA	https://infocentre.gsm.org/cgi-bin/prdind.cgi?BA
Transferred Account Procedure Data Record Format Specification Version Number 3 (PRD TD.57)	TAP3	GSMA	https://infocentre.gsm.org/cgi-bin/prdind.cgi?TD