3GPP TSG SA WG3 Security — S3#34 **S3-040464**

July 6 - 9, 2004

Acapulco, Mexico

NOTE: THIS LS WAS APPROVED BY E-MAIL ON 7 JUNE 2004.

Title:	**Reply LS on Request for Comments on Wi-Fi Alliance Public Access MRD draft v1.0**
Work Item:	**WLAN**
Source:	3GPP SA WG3
To:	Wi-Fi Alliance
Cc:	CN1, CN3, CN4, SA2, SA5/SWG-B

Contact Person:

Name: David Mariblanca (Ericsson)
Tel. Number: +34 913393422
E-mail Address: david.mariblanca@ericsson.com

Attachments: Incoming Liaison Statement from Wi-Fi Alliance (S2-041110)

1. Overview

SA3 received a Liaison Statement from Wi-Fi Alliance, via 3GPP SA2 WG, including a Request for Comment on the Marketing Requirement Document Draft Version 1.0.
SA3 has requested comments to all members and the only one given is the following:

In 4.1.2 "User experience", the MRD seems to give recommendations rather than mandatory requirements. It should be stated that the most secure mechanism must prevail, instead of giving always the choice to the user which has no idea about security mechanisms. In the case “authentication directly with hotspot”, the user should be forced to authenticate with the most secure method (if available): for example, if the user has a (U)SIM, it should use an authentication method associated to it, instead of authenticate with user/password.

2. Action

SA3 kindly asks Wi-Fi Alliance to consider the comment expressed above.

3. Next SA3 meetings

SA3		
S3#35	5-8 Oct 2004	Malta
S3#36	23-26 Nov 2004	Shenzhen, China

Wi-Fi Alliance

3GPP TSG-SA WG2 meeting #39 **Tdoc S2-041110**
Shenzhen/China, 19th – 23rd April 2004

To: 3GPP, Chairman of SA2
Magnus Olsson, magnus.m.olsson@ericsson.com

From: Greg Hayes, Chairman Wi-Fi Alliance Public Access Task Group

Subject: Request for comment and liaison statement

Date: March 30, 2004

As you know, the Wi-Fi Alliance established a task group to address market requirements for public access Wi-Fi connectivity – with the goal of accelerating this market by standardizing and reducing the costs of deploying Wi-Fi infrastructure for hotspot access. The Public Access task group completed its 1.0 draft of this market requirements document (MRD) and is seeking comment on it.

As a strategic organization that we seek to maintain a current liaison relationship with, the Wi-Fi Alliance formally requests your review and comments on this document. We welcome feedback on all aspects of the document with special attention on:

- Applicability and accuracy of these market requirements for your application and constituency
- Significant omissions of relevant reference materials (from your or other influential organizations)
- Potential for alignment of the work of our organizations, leveraging the efforts and work completed by both

Although our MRD draft is marked confidential, this letter gives 3GPP permission to openly post it in the regular manner that we understand documents are shared with your participants.

We have created a simple form for communicating your feedback, which will be sent with the MRD. Use this form as a guideline, but please amend it as necessary to suit your needs in giving a full response.

As we agreed, the deadline for feedback that can be included in our documents is April 30, 2004.

Comments or questions may be forwarded to the chairmen of this task group – Greg Hayes greg_hayes@infonet.com and Joel Short, jshort@nomadix.com.

We look forward to your feedback and stand ready to work together to accelerate the public access market.

MARKETING REQUIREMENTS DOCUMENT
FOR
Public Access Wi-Fi Services

REVISION # 1.2

AS OF March 21, 2004

Edited by Greg Hayes

MRD distribution for comment and feedback.

TABLE OF CONTENTS

Wi-Fi Alliance Marketing Requirements Document

Document History

Date	Name	Reason for Document History	Version
6-17-03	Greg Hayes	Original Draft	0.1
6-18-03	GH	Changes from task group meeting	0.2
6-24-03	GH	Specific edits from reflector comments	0.3
6-25-03	GH	Approved draft from conference call	0.35
8-6-03	GH	Incorporated section updates	0.4
8-7-03	GH	Added language to section A	0.45
8-8-03	GH	Refinement to Section D outline	0.5
8-11-03	GH	Added contributions to Sec. A & B	0.51
8-13-03	GH	Added Section B&C updates	0.52
9-5-03	GH	Updated B, C & D	0.6
9-17-03	JH	Updated section B	0.65
9-30-03	GH & JS	Added reference diagram	0.7
10-13-03	GH	Updated outline, diagram & reqs	0.8
10-22-03	GH & JS	Updated Section 4.1	0.85
11-5-03	GH	Consolidated submissions to date	0.9
11-12-03	GH	Finalized 4.1.1 and updated all	0.91
11-24-03	GH	Updates from conf call issue resolution	Tent 1.0
12-3-03	GH	Final issues resolved and incorporated	1.0
3-16-04	GH	Included IPRD feedback	1.1
3-21-04	GH	Included 3GPP2 feedback	1.2

1 Overview

The public access task group (phase three) was chartered with the mission of establishing Wi-Fi as the standard for public WLAN access. To achieve this mission, there are several key issues in public access that the Wi-Fi Alliance (WFA) can take a leadership role in to establish the dominance of Wi-Fi in this market.

- Make it faster, easier and more cost affective to deploy for operators and carriers
- Improve security and ease-of-use for nomadic Wi-Fi users
- Support various Roaming capabilities to enable the evolution toward single-bill roaming

2 Scope

This Marketing Requirements Document will identify requirements of components of Wi-Fi public access systems that provide a) client to access point (AP) interfaces b) AP to network interfaces (inclusive of authenticator functionality) and c) network to network interfaces that support secure, easy to use, single-bill roaming Wi-Fi public access. This

document also addresses co-existence with legacy, browser-based public access methodologies.

The public access market is several years old and legacy methods for access control and authentication have been deployed – including browser based login (also called the universal access method – UAM) and so-called "smart clients" that ease the login process.

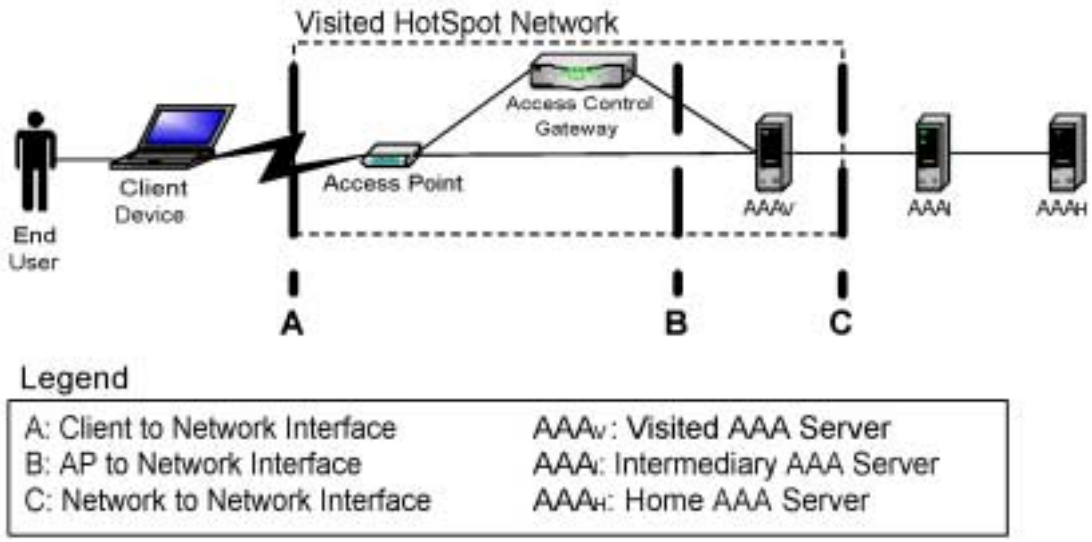
Emerging access methods using Wi-Fi Protected Access (WPA) to better secure and prevent fraud in public access environments have been developed and will be outlined under a separate white paper being drafted by the WFA. As WPA becomes the standard for Wi-Fi security and for enterprise security, users and IT administrators will expect and demand the same level of security in public access environments. Thus, it is necessary for both access methods to be supported and migration to the more secure WPA access method encouraged.

This MRD outlines requirements for public access that mandate coexistence between the following techniques for AAA:

a. UAM (browser-based, HTTP technique for authentication)
b. WPA

This scope and these network interfaces are illustrated in the figure below:

Figure 1: Public Access Reference Diagram



Interface A deals with the access method used to associate and connect to the local hotspot network. The function of interface B is to provide access control while interface C deals with interoperator roaming. The B and C interfaces broadly describe network access server (NAS) functionality but not a specific architecture (for example the access control functions can reside in the AP or in the access controller).

2.1 Target Markets

This MRD refers to products that are targeted to the public access Wi-Fi market. This market is defined as any public Internet access application of Wi-Fi – examples include public Internet access in airports, coffee shops, gas stations as well as in corporate/enterprise sites, such as a building lobby or common area in a campus.

2.2 Applications

This MRD will accommodate the following applications of public Wi-Fi access:

A. Ad-hoc hotspot access (localized access control and accounting, no roaming)
B. Access via a pre-arranged account through an operator or carrier (including pre- and post-paid accounting)
C. End-user of another carrier roaming onto a visited operators' hotspot infrastructure (including pre- and post-paid accounting)
D. Free of charge access within an enterprise, "amenity-based" service providers or freenets

3 Reference to Underlying Standards

References to any standards to which the products need to comply with (in part or in whole). The correct document identification shall be included (may include revision number, draft number, date, or any other clear identification).

A. 3GPP SA2– TS 23.234 3GPP System to WLAN Interworking System Description
B. 3GPP TS 33.234 3GPP 3G Security WLAN Interworking Security
C. 3GPP2 TSG-S - S.P0087-0 WLAN Interworking Stage 1
D. GSMA – IR61
E. IEEE 802.11 a/b/g
F. IEEE 802.1X
G. IETF – RFC 2284 "Extensible Authentication Protocol"
H. IETF – RFC 2865 "RADIUS Authentication"
I. IETF – RFC 2866 "RADIUS Accounting"
J. IETF – RFC 3576 "Dynamic Authorization Extensions to RADIUS"
K. IETF – RFC 3579 "RADIUS support for EAP"
L. IETF – RFC 3580 "802.1X RADIUS usage guidelines"
M. IPRD.ORG WLAN Accounting and Settlement Service Specification v1.0
N. Wi-Fi Alliance – Wi-Fi Protected Access (WPA)

4 Requirements

Mandatory Requirements

Requirements that must be met in order to pass the certification tests that shall be developed based on the MRD. Not meeting these requirements shall prevent the use of the public access certification granted by the WFA.

4.1.1 General Requirements

The following mandatory requirements are necessary to support public access deployments:

1. The hotspot network shall support simultaneous operations of subscribers visiting the venue using:
    a. UAM (no smart client), non-WPA clients, and WPA clients simultaneously
    b. WPA-only clients
2. The hotspot must accommodate the following access scenarios:
    a. Ad-hoc hotspot access (localized access control and accounting)
    b. Access via a pre-arranged account through an operator or carrier (including pre- and post-paid accounting). The most prevalent techniques include:
        i. Pre-paid scratch cards or pre-paid purchase of time (down to the minute) in advance of network usage
        ii. Paid in advance subscription from a service provider (also capable of being billed per minute)
    c. End-user of one carrier roaming on another's operators hotspot infrastructure (including pre- and post-paid accounting)
    d. Free of charge access within an enterprise, "amenity-based" service providers or freenets (including optional AAA)
3. The hotspot shall communicate the authentication methodology capabilities of the network.
    a. Subscribers shall be informed via UAM if WPA is available on the network in order to encourage migration to the WPA access method.
    b. The subscriber shall not be able to simultaneously access overlapping UAM and WPA networks.
        i. The subscriber shall not be able to first authenticate via WPA and then maintain the prior session when the client device encounters a UAM network with lesser security.
    c. Subscribers encountering a scenario where overlapping networks with differing UAM and WPA access methods are allowed to access the network based upon the service profiles determined by the subscriber's home entity. The home entity is defined as the authentication and authorization owner of the user. If the service profile does not specify an access method prioritization, the user must be allowed to manually select their desired access method.
4. Each Wi-Fi network shall not interfere with the Wi-Fi and authentication functionality of the other co-located networks.

a. Each UAM or WPA network shall allow for overlap of the Wi-Fi coverage.

b. The hotspot network shall accommodate encrypted and unencrypted traffic in the same environment.

c. Subscriber initiated IPSec/VPN for UAM must be supported.

5. The Access Point must be capable of supporting any IETF-compliant EAP method when operating in "pass-through" mode.

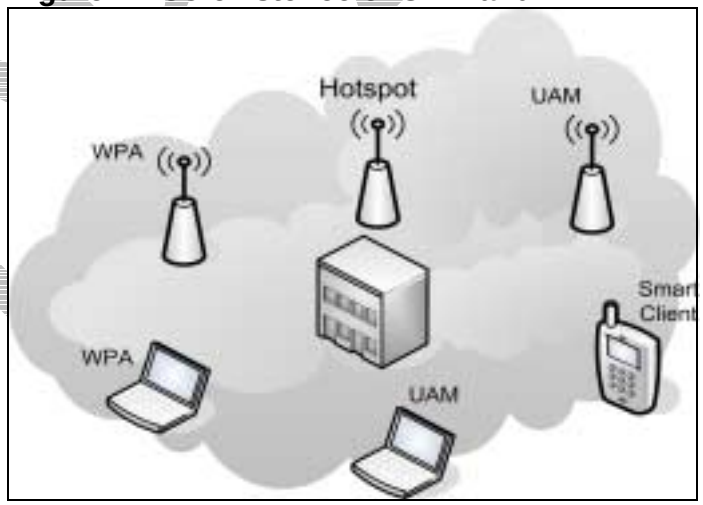
6. All system components must provide a mechanism to support migration path from the legacy AAA UAM to WPA in both the client and the hotspot network.

4.1.2 Interface A: Client to Access Point Interface

The Client to Access Point Interface is the first touchpoint that the user has to the public access network. This interface handles the initial attachment and association of the user to the wireless network as well as authentication.

As described in section 4.1.1, Wi-Fi public access networks must support both legacy browser-based access methods (known as the universal access method or UAM) and WPA. This interface and action between the client and the access point must support users' needs to discover and select the appropriate network connection as well as support ad-hoc account creation or even free access.

Figure 2: Co-existence of UAM and WPA



The following use cases must be supported under both UAM and WPA techniques:

1. Single provider Wi-Fi network supporting one access method
2. Single provider Wi-Fi network supporting multiple access methods
3. Multiple provider Wi-Fi networks supporting multiple access methods

4. Multiple provider Wi-Fi networks representing multiple access methods are allowed to overlap
5. Multiple provider Wi-Fi network supporting multi-SSID
6. Multiple provider Wi-Fi network using Virtual APs

User Experience

A user enters a public hotspot. Once their laptop is booted, an association with the local Wi-Fi network is established. This may be achieved automatically by the operating system, a smart client or through the intervention of the user using a suitable application on the laptop (e.g., manual entry of an SSID into a Wi-Fi configuration utility or smart client). The authentication procedure then commences. The user's perception of this will depend on the access method and associated security model available within the hotspot. Whatever access method is chosen, it should remain transparent to the user. The possible ranges of user authentication experience may go from being undetectable by the user, to having a Welcome Page displayed within a browser that allows an unregistered user to register with that hotspot. It is highly likely that some intermediate experience will be the norm.

A Welcome Page may cover the following range of authentication options:

1. New user enrolment
2. Authentication directly with hotspot operator or via roamed partner
3. No authentication required

"New user enrolment" could involve entry of credit card credentials, whereas "authentication directly with hotspot" could include user name and password, or initiate authentication using a token such as a SIM card.

The initial options presented will depend upon the configuration of the hotspot. It may also be possible that by choosing a specific option, such as authentication with a roaming partner, further pages may then be displayed based on network authentication requirements.

The "no authentication required" option may be provided by the hotspot operator for unauthenticated access to local services. If the user is unable or unwilling to associate for paid services, it is essential that the hotspot owner still provide some service where the user is encouraged to connect.

The option to force a welcome page is a requirement for UAM and WPA connections for the display of disclaimer (indemnification or terms of service) information.

In addition, it should also be considered that by increasing the range of authentication options, as outlined above, the potential market of users would also increase.

Once authenticated, the user can then access his originally desired home page such as "www.wi-fi.org." In addition, there may be an optional window which pops up detailing session information and providing a button which, when clicked, will terminate the user session. This then allows the user to use the facilities of the hotspot until they have finished their activities. Alternatively, the facilities of the hotspot may be terminated based on some other trigger mechanism, such as that based on time duration.

Network discovery and selection

When a user roams into a hotspot network, he must be able to select the appropriate service provider to authenticate with and who will capture his accounting information. There are several possible ways for a user to discover and select the networks. Before listing these possibilities, it is important to note that the term "network" in this context does not necessarily refer only to the hotspot wireless network. Rather, it refers to the entity representing the service provider with which the user has an account or wants to establish an account. This service provider either is the hotspot owner or has a roaming agreement with the hotspot network. The user will use his credentials to authenticate himself to the service provider in order to gain access to the hotspot network.

4.1.2.1 Universal Access Method

The Universal Access method is the "least common denominator" in public access networks, as they have been most widely deployed in the market as of this writing. This method of redirecting a user's browser to a login screen allows users with pre-configured accounts as well as new users to set up service to the public Wi-Fi service.

In this method, the hotspot network manages its own wireless network, (i.e. hosts its own SSID). Each hotspot network has a single SSID that identifies the hotspot itself. The roaming user first associates with the hotspot wireless network. The user's browser is then redirected to the local welcome page on which a list of service providers is presented. The user can then select from this list the service provider of his choice for authentication.

Requirements:

1. Each virtual access point in the hotspot network should be configured to respond to the "Probe Request" frame with the SSIDs it supports. The goal is for the AP to respond to open authentication as defined in clause 8.1 of the IEEE 802.11 specification.
2. The local welcome or portal page must contain a list of service provider networks, roaming intermediaries or a link to such a list.

4.1.2.2 Wi-Fi Protected Access

WPA users must be able to be authenticated and billed via: local hotspot operator, an aggregator or trusted intermediary, or home service provider and secure end-to-end authentication as stipulated in RFC 2284 (EAP) and by extension the RADIUS protocol RFC 2865 and RFC 2866.

Within this subsection, requirements are stated which refer to clients and access networks utilizing WPA. This list of requirements should match those of Interface C (4.1.4) below, thus providing requirements for the WPA end-to-end system.

Requirements:

1. As required for UAM, the WPA access method must support:
    a. Ad-hoc hotspot access (localized access control and accounting, no roaming)
    b. Access via a pre-arranged account through an operator or carrier (including pre- and post-paid accounting)
    c. End-user of another carrier roaming onto a visited operators' hotspot infrastructure (including pre- and post-paid accounting)
    d. Free of charge access within an enterprise, "amenity-based" service providers or freenets
2. Network access control shall support WPA, thus mitigating security attacks on the WPA enabled Access Point or subscribers, from the WAN network.
3. The interface should enable the end-user to use the optimal WPA/EAP authentication method when roaming to different providers.

In addition, there are additional network discovery and selection requirements for WPA access that will help a Wi-Fi client using EAP for authentication to decide whether or not to connect to a Wi-Fi access network. The purpose of these is to help the user to select the most appropriate Mediating Network as a next hop for routing AAA packets in roaming situations where the Wi-Fi access network has agreements with more than one Mediating Network affiliated with the client's Home Service Network.

SSID-based network selection is the most commonly used method in the current practice. In this method, each service provider is represented by a unique SSID, e.g., "ABC_wireless." Multiple service providers may share the same wireless infrastructure by using the multiple SSID feature in the access point. A user may use a specific service provider's SSID in his wireless LAN card manager. If such an SSID does exist in the hotspot network, the user device will be associated with the corresponding access point. Authentication can then take place.

Requirements:

4. Each Access point (virtual or real) shall present a unique BSSID per SSID that is to be used for the hotspot access.
5. The access points in the hotspot network should be configured to respond to the "Probe Request" frame with the SSID "ANY" with "Probe Response" frames that correspond to all the SSIDs it supports.

It is desirable that the beacon frame or the "Probe Response" frame is augmented with information related to public access for the corresponding service provider. Such information may include the authentication method that is supported (e.g., UAM and/or

WPA), the rate that will be charged to the user and the data rates that can be provided – prior to authentication.

4.1.3 Interface B: Access Point to Network Interface

In order to support both UAM and WPA authentication, a minimum set of RADIUS attributes must be supported. As shown in Appendix A, different RADIUS attributes are used for different access methodologies.

To clarify the way that the RADIUS requirements map to Figure 1, all interface B RADIUS requirements must be supported either on the Access Point, the Access controller or some combination of both. These represent RADIUS client functions.

AAA Attributes that must be supported: Please refer to Appendix A for RADIUS AAA requirements.

4.1.4 Interface C: Network to Network interface

Requirements in this section relate to the Network – Network Interface (NNI) between the WLAN system and Service Provider network. There may be intermediaries between the WLAN and the home service provider such as aggregators and clearinghouses. However, this does not impact the Network – Network Interface. The NNI must support the following required RADIUS capabilities.

Requirements:

1. Provide roaming service for both UAM-only clients and WPA-only clients or clients equipped with both (co-existence).
2. Support EAP protocol over RADIUS.
3. Support for binding requirements for EAP sessions to RADIUS transactions.
4. Provide volume based accounting for users.
5. Provide time-based accounting for users (based on the duration of the session)
6. Communicate the coverage and location of an AP.
7. Communicate user bandwidth received during a session (uplink and downlink).
8. Indicate any special “class of service” for the session. For example, a publicly routable IP address.
9. Identify the underlying hotspot operators (provider ID, etc.)
10. Support RADIUS Interim Update Messages. Interim updates are used for all user sessions to decrease the chances of losing accounting information in the case a Stop record is lost in the network. The default value of an interim update interval shall be 900 seconds. The WLAN system shall override the default value with any value received from the Service Provider network in an Acct-Interim-Update attribute

11. The NNI must support anonymous authentication tunnels (including PEAP and TTLS)
12. The NNI shall support at a minimum the following set of standard RADIUS attributes: Please refer to Appendix A.
13. Must be compliant with roaming and settlement standards from GSMA, 3GPP, 3GPP2, and IPDR. (See Appendix A)
14. Required Session-Timeout and Termination-Action:
    a. Upon expiry of the timer set by the Session-Timeout attribute, the WLAN system shall either terminate the user session or re-authenticate the user session (and for example, possibly extend the duration of pre-paid service) based on the value of the Termination-Action attribute.
15. For Accounting purposes, Interim update records are sent by the WLAN system for prepaid as well as "postpaid" user sessions.
16. RADIUS communication must be protected and secured.

5 Optional Requirements

No optional requirements are requested in this document.

6 Impact on other WFA Documents

As shown in section 3, above, this MRD draws directly from and may influence the future requirements of the behavior of WPA and 802.1X access methods techniques to accommodate the public access use case.

7 Roll Out Schedule

The anticipated certification program for public access has several phases:

1. Upon approval of this MRD and review by liaison organizations, immediate creation of a test plan and certification program for Wi-Fi Access Points for “public access” certification.
2. Evaluation of a system-level certification program to create a “generic” Wi-Fi public access hotspot.
3. Evaluation of an extension of public access certification to devices beyond access points – such as AAA servers and access controllers.

No capabilities label requirements are requested at this time, since this will be a commercial-grade, infrastructure certification – not a consumer certification.

8 Glossary

Access Method: The method that the user employs to first connect and authenticate to the hotspot network. For the purpose of this document, there are two access methods – UAM and WPA.

BSSID: A unique MAC address of the access point or virtual access point.

Smart Client: A software agent (located on the user's mobile device) that assists the user in locating, associating and authenticating to a Wi-Fi network. Smart clients automate and mask the user interface complexities associated with the UAM technique (as defined in the WISPr Best Common Practices document).

Mediating Network: any network which operates an intermediary AAA server and provides authentication authority for a visited hotspot network. Mediating networks are typically network aggregators and clearinghouses.

"Pass Through" Mode: 802.1x implementation as defined in RFC 2284. The compliant methods are described in informational RFC XXXX.

Subscriber: any user of a public access is called a subscriber, whether or not they are paying for network usage.

UAM: Universal Access Method, as described in the WISPr Best Current Practices document.

Virtual Access Point: Multiple appearances of an AP tied of a single physical radio. This is a fully functional AP as defined by the IEEE Specification 99.

WPA: Wi-Fi Protected Access

APPENDIX A: RADIUS Attributes

Attribute	#	Type	WA MRD Interface				Access Req	Access Resp	Acct Start	Acct Intrm	Acct Stop	Comments
			B.UAM	B.WPA	C.UAM	C.WPA	WA	WA	WA	WA	WA	
User Name	1	String	✓	✓	✓	✓	✓	✓	✓	✓	✓	User's NAI, Case Sensitive
User Password	2	String	✓		✓		✓					Case Sensitive; Must only be used if client authenticating via UAM
NAS-IP Address	4	IP Addr	✓	✓	✓	✓	✓		✓	✓	✓	IP Addr of RADIUS client
NAS-Port	5	Integer		✓		✓	✓		✓	✓	✓	Is the Association ID between client & AP per RFC 3580
Service Type	6	Integer	✓	✓	✓	✓	✓					Various Service Types used for UAM are described in RFC 2865. Service types for use with 1x are described in RFC 3580.
Framed IP Address	8	IP Addr	✓		✓	✓			✓	✓	✓	Client's IP Address. See RFC 3580 - Not used for L2 Authenticators with 802.1x. Attribute required for TAP & IPDR
Framed-IP-Netmask	9	Integer		✓			✓	✓				Netmask of the user; For local use. See RFC 3580 (not used for L2 Authenticators)
Filter-ID	11	String	✓	✓	✓	✓		✓				See Note 1. This is currently being worked in IETF RADIUSEXT Working Group. It may be used to indicate either layer 2 or layer 3 filters as per RFC 3580. May also be used by 3GPP
Reply Message	18	String	✓		✓			✓				Text to display to user, does not affect protocol
State	24	String	✓	✓	✓	✓	✓	✓				Opaque string from AAA in Access Challenge
Class	25	String	✓	✓	✓	✓		✓	✓	✓	✓	See Note 1. This is currently being worked in IETF RADIUSEXT Working Group. Current proposal in IPDR Spec.
Session Timeout	27	Integer	✓	✓	✓	✓		✓				Seconds until forced session termination and re-authentication required (may be used for prepaid subs); See Termination-Action
Idle Timeout	28	Integer	✓	✓	✓	✓		✓				Seconds of idle time before auto-termination of session
Termination Action	29	Integer		✓		✓		✓				0-Default (end of session) 1-RADIUS re-authentication
Called Station ID	30	String	✓	✓	✓	✓	✓		✓	✓	✓	Per RFC 3580=MAC Address of NAS + SSID (if known), in ASCII. Example: "00-50-E8-12-34-C0:AP1"
Calling Station ID	31	String	✓	✓	✓	✓	✓		✓	✓	✓	Per RFC 3580=Client's MAC Address, in ASCII. Example: "00-10-A4-23-19-C0"
NAS Identifier	32	String	✓	✓	✓	✓	✓		✓	✓	✓	Alternative to NAS-IP_Address to identify NAS
Proxy-State	33		✓	✓	✓	✓	✓	✓				Only required on B interface if NAS acting as Proxy
Acct Status Type	40	Integer	✓	✓	✓	✓			✓	✓	✓	1=Start 2=Stop 3=Interim update
Acct Input Octets	42	Integer	✓	✓	✓	✓				✓	✓	
Acct Output Octets	43	Integer	✓	✓	✓	✓				✓	✓	
Acct Session ID	44	String	✓	✓	✓	✓			✓	✓	✓	NAS unique ID to correlate all accounting records in a session; May be used to correlate with Auth Records
Acct Session Time	46	Integer	✓	✓	✓	✓				✓	✓	Session duration in seconds
Acct Input Packets	47	Integer	✓	✓	✓	✓				✓	✓	
Acct Output Packets	48	Integer	✓	✓	✓	✓				✓	✓	
Acct Termination Cause	49	Integer	✓	✓	✓	✓					✓	1=User Request 2=Lost Carrier/Link 4=idle timeout 5=session timeout 6=admin reset 9=NAS error 10=NAS request 11=NAS reboot 19=Supplicant (Client) Restart 20=Re-Auth Failure; See RFC 3580 for more info
Acct-Input-Gigawords	52	Integer	✓	✓	✓	✓				✓	✓	Number of times the Acct-Input-Octets counter has wrapped around
Acct-Ouput-Gigawords	53	Integer	✓	✓	✓	✓				✓	✓	Number of times the Acct-Output-Octets counter has wrapped around
Event Time Stamp	55	Integer	✓	✓	✓	✓			✓	✓	✓	Seconds since Jan 1 1970 UTC
NAS Port Type	61	Integer	✓	✓	✓	✓	✓		✓	✓	✓	15=Ethernet 19=802.11
EAP-Message	79	String		✓		✓	✓	✓	✓	✓	✓	Required per RFC 3579
Message Authenticator	80	String		✓		✓	✓	✓	✓	✓	✓	Required per RFC 3579
Acct Interim Interval	85	Integer	✓	✓	✓	✓		✓				Interval in seconds between Acct updates
WISPr Vendor Specific Attributes												
MS-MPPE-Recv-Key		String		✓		✓		✓				.1x Encryption Key
MS-MPPE-Send-Key		String		✓		✓		✓				.1x Encryption Key
WISPr Location ID	1	String			✓	✓	✓		✓	✓	✓	Hotspot Location Identifier
WISPr Location Name	2	String			✓	✓	✓		✓	✓	✓	Hotspot Location
Hotspot Operator's Name		String			✓	✓	✓		✓	✓	✓	Operator's name (separate from Location name to address size issues
WISPr Bandwidth Min Up	5	Integer			✓	✓		✓	✓	✓	✓	Minimum Transmit Rate b/s
WISPr Bandwidth Min Down	6	Integer			✓	✓		✓	✓	✓	✓	Minimum Receive Rate b/s
WISPr Bandwidth Max UP	7	Integer			✓	✓		✓	✓	✓	✓	Maximum Transmit Rate b/s
WISPr Bandwidth Max Down	8	Integer			✓	✓		✓	✓	✓	✓	Maximum Receive Rate b/s
WISPr Billing Class Of Service	11	String			✓	✓		✓	✓	✓	✓	See Note 1.

Note 1: Additional Market Requirements for use of these attributes are being considered and investigated by WFA.

453

Wi-Fi Alliance Public Access MRD draft v1.0 Comment Form

Document: **WFA_PA_MRD_v1.0**

Comment Period Ends: **Jan. 31, 2004**

<u>Note:</u>

All MRD content and feedback is to be kept confidential

Comment From: <**Organization Name>**

<u>For questions please contact:</u>

Liaison: **<Contact Name**

Joel Short <jshort@nomadix.com> or Greg Hayes <greg_hayes@infonet.com>

Liaison: <**Contact E-mail>**

Line Number(s):	Cmnt Type: E(ditorial) or T(echnical)	Comment / Explaination	Recommended Change