

---

**Title:** LS on Request for Comments on Wi-Fi Alliance Public Access MRD draft v1.0  
**Work Item:** WLAN-3G Interworking  
**Source:** SA2  
**To:** CN1, CN3, CN4, SA3, SA5/SWG-B  
**Cc:**

**Contact Person:**  
**Name:** Nicolas Martiquet (Orange)  
**Tel. Number:** +33 1 45 29 51 69  
**E-mail Address:** [nicolas.martiquet@francetelecom.com](mailto:nicolas.martiquet@francetelecom.com)

**Attachments:** Incoming Liaison Statement from Wi-Fi Alliance (s2-041110.zip)

---

## 1. Overview

SA2 received a Liaison Statement from Wi-Fi Alliance, including a Request for Comment on the Marketing Requirement Document Draft Version 1.0.

SA2 believe that CN1, CN3, CN4, SA3 and SA5/SWG-B are in a position to make useful comments on this Liaison Statement, too. Hence, although SA2 have already made an answer from our point of view (so that we meet the deadline on April 30<sup>th</sup>), we believe that it would be useful that the groups above also comment this Marketing Requirement Document, even if the deadline cannot be fulfilled due to the 3GPP meeting schedule.

Please note that SA2 have already informed Wi-Fi Alliance that they would receive other answers after the deadline.

## 2. Action

SA2 kindly asks CN1, CN3, CN4, SA3 and SA5/SWG-B to consider the attached Liaison Statement and to provide an answer to Wi-Fi Alliance.

## 3. Next SA2 meetings

<b>SA2</b>		
S2#40	17-21 May 2004	Sophia Antipolis, France
S2#41	16-20 August 2004	Montreal, Canada

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](mailto:greg_hayes@infonet.com) and Joel Short, [jshort@nomadix.com](mailto: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.

The information contained in this document is confidential and proprietary to the Wi-Fi Alliance. It may not be copied, reproduced or distributed without the prior written consent of the Wi-Fi Alliance.

1  
2  
3  
4  
5  
6  
7  
8  
9  
10  
11  
12  
13  
14  
15  
16  
17  
18

**TABLE OF CONTENTS**

**Document History**.....3  
**1 Overview**.....3  
**2 Scope**.....3  
    2.1 Target Markets.....5  
    2.2 Applications.....5  
**3 Reference to Underlying Standards**.....5  
**4 Requirements**.....5  
    4.1 Mandatory Requirements .....5  
    4.2 Optional Requirements .....12  
    4.3 Out of Box (OOB) Requirements..... **Error! Bookmark not defined.**  
**5 Impact on other WFA Documents** .....12  
**6 Roll Out Schedule** .....12  
**7 Glossary** .....12

DRAFT

18  
19  
20 **Wi-Fi Alliance Marketing Requirements Document**  
21

22 **Document History**

23 Date	Name	Reason for Document History	Version
24 6-17-03	Greg Hayes	Original Draft	0.1
25 6-18-03	GH	Changes from task group meeting	0.2
26 6-24-03	GH	Specific edits from reflector comments	0.3
27 6-25-03	GH	Approved draft from conference call	0.35
28 8-6-03	GH	Incorporated section updates	0.4
29 8-7-03	GH	Added language to section A	0.45
30 8-8-03	GH	Refinement to Section D outline	0.5
31 8-11-03	GH	Added contributions to Sec. A & B	0.51
32 8-13-03	GH	Added Section B&C updates	0.52
33 9-5-03	GH	Updated B, C & D	0.6
34 9-17-03	JH	Updated section B	0.65
35 9-30-03	GH & JS	Added reference diagram	0.7
36 10-13-03	GH	Updated outline, diagram & reqs	0.8
37 10-22-03	GH & JS	Updated Section 4.1	0.85
38 11-5-03	GH	Consolidated submissions to date	0.9
39 11-12-03	GH	Finalized 4.1.1 and updated all	0.91
40 11-24-03	GH	Updates from conf call issue resolution	Tent 1.0
41 12-3-03	GH	Final issues resolved and incorporated	1.0
42 3-16-04	GH	Included IPRD feedback	1.1
43 3-21-04	GH	Included 3GPP2 feedback	1.2

44  
45  
46  
47  
48 **1 Overview**

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

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

58  
59 **2 Scope**

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

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

66  
 67 The public access market is several years old and legacy methods for access control  
 68 and authentication have been deployed – including browser based login (also called  
 69 the universal access method – UAM) and so-called “smart clients” that ease the login  
 70 process.

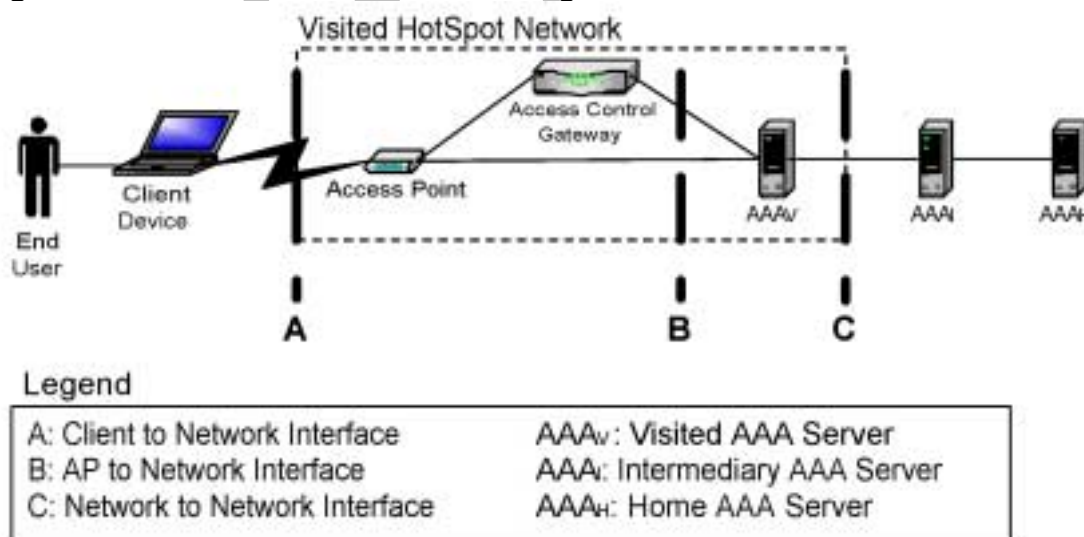
71  
 72 Emerging access methods using Wi-Fi Protected Access (WPA) to better secure and  
 73 prevent fraud in public access environments have been developed and will be outlined  
 74 under a separate white paper being drafted by the WFA. As WPA becomes the  
 75 standard for Wi-Fi security and for enterprise security, users and IT administrators  
 76 will expect and demand the same level of security in public access environments.  
 77 Thus, it is necessary for both access methods to be supported and migration to the  
 78 more secure WPA access method encouraged.

79  
 80 This MRD outlines requirements for public access that mandate coexistence between  
 81 the following techniques for AAA:

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

84  
 85  
 86 This scope and these network interfaces are illustrated in the figure below:

87  
 88 **Figure 1: Public Access Reference Diagram**



89  
 90  
 91 Interface A deals with the access method used to associate and connect to the local  
 92 hotspot network. The function of interface B is to provide access control while interface  
 93 C deals with interoperator roaming. The B and C interfaces broadly describe network  
 94 access server (NAS) functionality but not a specific architecture (for example the access  
 95 control functions can reside in the AP or in the access controller).

96

97 **2.1 Target Markets**

98 This MRD refers to products that are targeted to the public access Wi-Fi market. This  
99 market is defined as any public Internet access application of Wi-Fi – examples include  
100 public Internet access in airports, coffee shops, gas stations as well as in  
101 corporate/enterprise sites, such as a building lobby or common area in a campus.  
102

103 **2.2 Applications**

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

- 105 A. Ad-hoc hotspot access (localized access control and
- 106 accounting, no roaming)
- 107 B. Access via a pre-arranged account through an operator or
- 108 carrier (including pre- and post-paid accounting)
- 109 C. End-user of another carrier roaming onto a visited operators’
- 110 hotspot infrastructure (including pre- and post-paid accounting)
- 111 D. Free of charge access within an enterprise, “amenity-based”
- 112 service providers or freenets  
113

114 **3 Reference to Underlying Standards**

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

- 118 A. 3GPP SA2– TS 23.234 3GPP System to WLAN Interworking System Description
- 119 B. 3GPP TS 33.234 3GPP 3G Security WLAN Interworking Security
- 120 C. 3GPP2 TSG-S - S.P0087-0 WLAN Interworking Stage 1
- 121 D. GSMA – IR61
- 122 E. IEEE 802.11 a/b/g
- 123 F. IEEE 802.1X
- 124 G. IETF – RFC 2284 “Extensible Authentication Protocol”
- 125 H. IETF – RFC 2865 “RADIUS Authentication”
- 126 I. IETF – RFC 2866 “RADIUS Accounting”
- 127 J. IETF – RFC 3576 “Dynamic Authorization Extensions to RADIUS”
- 128 K. IETF – RFC 3579 “RADIUS support for EAP”
- 129 L. IETF – RFC 3580 “802.1X RADIUS usage guidelines”
- 130 M. IPRD.ORG WLAN Accounting and Settlement Service Specification v1.0
- 131 N. Wi-Fi Alliance – Wi-Fi Protected Access (WPA)  
132

133 **4 Requirements**

134 **Mandatory Requirements**

135 Requirements that must be met in order to pass the certification tests that shall be  
136 developed based on the MRD. Not meeting these requirements shall prevent the use of  
137 the public access certification granted by the WFA.  
138  
139

140 4.1.1 General Requirements

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

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



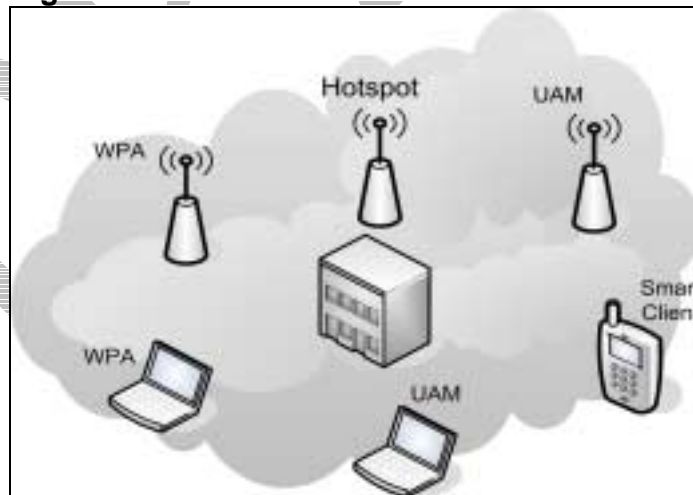
- 180 a. Each UAM or WPA network shall allow for overlap of the Wi-Fi  
181 coverage.
- 182 b. The hotspot network shall accommodate encrypted and unencrypted traffic  
183 in the same environment.
- 184 c. Subscriber initiated IPsec/VPN for UAM must be supported.
- 185 5. The Access Point must be capable of supporting any IETF-compliant EAP  
186 method when operating in “pass-through” mode.
- 187
- 188 6. All system components must provide a mechanism to support migration path from  
189 the legacy AAA UAM to WPA in both the client and the hotspot network.

#### 190 4.1.2 Interface A: Client to Access Point Interface

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

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

200  
201  
202  
203 **Figure 2: Co-existence of UAM and WPA**



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

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

- 210 4. Multiple provider Wi-Fi networks representing multiple access methods are  
211 allowed to overlap  
212 5. Multiple provider Wi-Fi network supporting multi-SSID  
213 6. Multiple provider Wi-Fi network using Virtual APs  
214

215 User Experience

216 A user enters a public hotspot. Once their laptop is booted, an association with the local  
217 Wi-Fi network is established. This may be achieved automatically by the operating  
218 system, a smart client or through the intervention of the user using a suitable application  
219 on the laptop (e.g., manual entry of an SSID into a Wi-Fi configuration utility or smart  
220 client). The authentication procedure then commences. The user's perception of this will  
221 depend on the access method and associated security model available within the hotspot.  
222 Whatever access method is chosen, it should remain transparent to the user. The possible  
223 ranges of user authentication experience may go from being undetectable by the user, to  
224 having a Welcome Page displayed within a browser that allows an unregistered user to  
225 register with that hotspot. It is highly likely that some intermediate experience will be the  
226 norm.  
227

228 A Welcome Page may cover the following range of authentication options:  
229

- 230 1. New user enrolment  
231 2. Authentication directly with hotspot operator or via roamed partner  
232 3. No authentication required  
233

234 "New user enrolment" could involve entry of credit card credentials, whereas  
235 "authentication directly with hotspot" could include user name and password, or initiate  
236 authentication using a token such as a SIM card.  
237

238 The initial options presented will depend upon the configuration of the hotspot. It may  
239 also be possible that by choosing a specific option, such as authentication with a roaming  
240 partner, further pages may then be displayed based on network authentication  
241 requirements.  
242

243 The "no authentication required" option may be provided by the hotspot operator for  
244 unauthenticated access to local services. If the user is unable or unwilling to associate for  
245 paid services, it is essential that the hotspot owner still provide some service where the  
246 user is encouraged to connect.  
247

248 The option to force a welcome page is a requirement for UAM and WPA connections for  
249 the display of disclaimer (indemnification or terms of service) information.  
250

251 In addition, it should also be considered that by increasing the range of authentication  
252 options, as outlined above, the potential market of users would also increase.  
253

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

#### 260 Network discovery and selection

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

##### 271 4.1.2.1 Universal Access Method

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

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

##### 284 Requirements:

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

##### 292 4.1.2.2 Wi-Fi Protected Access

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

297

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

301

302 Requirements:

303

304 1. As required for UAM, the WPA access method must support:

305

306

307

308

309

310

311

312

313

314

315

316

317

- 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.

318

319

320

321

322

323

324

325

326

327

328

329

330

331

332

333

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.

333 Requirements:

334

335

336

337

338

339

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.

340

341

342

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

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

345

#### 346 4.1.3 Interface B: Access Point to Network Interface

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

350

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

354

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

357

#### 358 4.1.4 Interface C: Network to Network interface

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

364

365 Requirements:

366

367

368

369

370

371

372

373

374

375

376

377

378

379

380

381

382

383

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

- 384 11. The NNI must support anonymous authentication tunnels (including PEAP  
385 and TTLS)  
386 12. The NNI shall support at a minimum the following set of standard RADIUS  
387 attributes: Please refer to Appendix A.  
388 13. Must be compliant with roaming and settlement standards from GSMA,  
389 3GPP, 3GPP2, and IPDR. (See Appendix A)  
390 14. Required Session-Timeout and Termination-Action:  
391 a. Upon expiry of the timer set by the Session-Timeout attribute, the  
392 WLAN system shall either terminate the user session or re-  
393 authenticate the user session (and for example, possibly extend the  
394 duration of pre-paid service) based on the value of the Termination-  
395 Action attribute.  
396 15. For Accounting purposes, Interim update records are sent by the WLAN  
397 system for prepaid as well as "postpaid" user sessions.  
398 16. RADIUS communication must be protected and secured.  
399  
400  
401

## 402 **5 Optional Requirements**

403 No optional requirements are requested in this document.  
404

## 405 **6 Impact on other WFA Documents**

406 As shown in section 3, above, this MRD draws directly from and may influence the  
407 future requirements of the behavior of WPA and 802.1X access methods techniques to  
408 accommodate the public access use case.  
409

## 410 **7 Roll Out Schedule**

411 The anticipated certification program for public access has several phases:

- 412 1. Upon approval of this MRD and review by liaison organizations, immediate creation  
413 of a test plan and certification program for Wi-Fi Access Points for "public access"  
414 certification.  
415 2. Evaluation of a system-level certification program to create a "generic" Wi-Fi public  
416 access hotspot.  
417 3. Evaluation of an extension of public access certification to devices beyond access  
418 points – such as AAA servers and access controllers.  
419

420 No capabilities label requirements are requested at this time, since this will be a  
421 commercial-grade, infrastructure certification – not a consumer certification.  
422

## 423 **8 Glossary**

424 **Access Method:** The method that the user employs to first connect and authenticate to  
425 the hotspot network. For the purpose of this document, there are two access methods –  
426 UAM and WPA.  
427

428 **BSSID:** A unique MAC address of the access point or virtual access point.  
429

430 **Smart Client:** A software agent (located on the user's mobile device) that assists the  
431 user in locating, associating and authenticating to a Wi-Fi network. Smart clients  
432 automate and mask the user interface complexities associated with the UAM technique  
433 (as defined in the WISPr Best Common Practices document).  
434

435 **Mediating Network:** any network which operates an intermediary AAA server and  
436 provides authentication authority for a visited hotspot network. Mediating networks are  
437 typically network aggregators and clearinghouses.  
438

439 **"Pass Through" Mode:** 802.1x implementation as defined in RFC 2284. The compliant  
440 methods are described in informational RFC XXXX.  
441

442 **Subscriber:** any user of a public access is called a subscriber, whether or not they are  
443 paying for network usage.  
444

445 **UAM:** Universal Access Method, as described in the WISPr Best Current Practices  
446 document.  
447

448 **Virtual Access Point:** Multiple appearances of an AP tied of a single physical radio.  
449 This is a fully functional AP as defined by the IEEE Specification 99.  
450

451 **WPA:** Wi-Fi Protected Access

APPENDIX A: RADIUS Attributes

Attribute	#	Type	WA MRD Interface				Access	Access	Acct	Acct	Acct	Comments
			B.UAM	B.WPA	C.UAM	C.WPA	Req	Resp	Start	Intrm	Stop	
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 RADIUS 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 RADIUS 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:API"	
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-Output-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	
<b>WISPr Vendor Specific Attributes</b>												
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.



DRAFT

