WPA™ Deployment Guidelines for Public Access Wi-Fi® Networks

Wi-Fi Alliance
October 28, 2004

Executive Summary

WPA provides a strong standards-based, interoperable security solution that addresses the known flaws in the original WEP security mechanism. WPA utilizes TKIP to provide data encryption enhancements including a per-packet key mixing function, a message integrity check (MIC), an enhanced initialization vector (IV) with sequencing rules, and a session-based keying/re-keying mechanism. To strengthen user authentication, WPA implements IEEE 802.1X and the Extensible Authentication Protocol (EAP). Cryptographers have reviewed Wi-Fi Protected Access and have verified that it meets its claims to close all known WEP vulnerabilities and provides an effective deterrent against known attacks.

WPA has been acknowledged as a secure WLAN solution for Enterprise-class deployments, and much thought has gone into assessing the practical and theoretical deployment of WPA for use in Public Internet Access services as well. With the strong vendor adoption of WPA, it is time for WPA deployment in Public Access venues. There are many compelling reasons for Wi-Fi Service Providers to adopt WPA. While much of the focus on WPA revolves around enhancements to Wi-Fi security, the technologies that form Wi-Fi Protected Access deliver additional benefit in the form of 802.1X authentication. As a service platform for Public Internet Access, WPA promises:

- Enhanced Security
- Flexibility
- Interoperability
- A Platform for Innovation

This document provides a general reference to best practices, emerging technologies and practical applications of Wi-Fi in Public Network Access with particular emphasis on WPA. This document primarily seeks to educate and inform, but makes specific recommendations in an attempt to facilitate the broad adoption of WPA in Public and Private venues under well-established principles.

This whitepaper represents a consensus view of the Wi-Fi Alliance, an organization created to promote 802.11-based interoperable Wi-Fi products. As such, this document is the result of two primary sources of input -- the Wi-Fi Members themselves and various ‘liaisons’ with other Standards Bodies as mentioned in the Acknowledgements to follow.

The Wi-Fi Alliance has reviewed the recommendations of this document with the standards and recommendations of these various organizations and seeks to endorse and promote the use of existing standards. The Wi-Fi Alliance had been granted permission to reference and in some cases reproduce these organizations’ findings in support of their work. This document represents the product of that work, particularly as it relates to the application of WPA and related features and services. As this document contains both original and referenced content, extensive endnotes of external sources are provided.

The Wi-Fi Alliance is a nonprofit international trade association that developed the Wi-Fi brand in 1999 to certify interoperability of wireless local area network products based on IEEE 802.11 standards. Wi-Fi Alliance product certification began in March of 2000. The primary mission of the Wi-Fi Alliance is to assure a positive user experience through product interoperability.

Acknowledgements

The Wi-Fi Alliance Public Access Committee would like to thank the following Wi-Fi Alliance member companies. We are grateful for their invaluable contributions of time, effort and content into this document:

- Airgo Networks
- AT&T Labs
- Belair Networks
- Calypso
- Colubris
- Connexion by Boeing
- Dell
- Enterasys
- Ericsson
- Funk Software
- Gemtek
- Infonet
- Instant 802
- Intel
- iPass, Inc.
- Motorola
- Nokia
- Nomadix
- Nortel
- Philips
- Proxim
- Siemens
- Sprint
- Symbol
- Syniverse
- Telia Sonera
- Texas Instruments
- TSI

Table of Contents

1. Overview

In 2003, the Wi-Fi Alliance spearheaded an effort to bring to market a standards-based interoperable security specification that would greatly increase the level of data protection and access control for Wi-Fi wireless local area networks. That specification is Wi-Fi Protected Access (WPA).

Most Wi-Fi Public Access networks today utilize a general browser-based method referred to as the Universal Access Method (UAM) for authentication with no WEP or WPA wireless security enabled. This whitepaper describes why and how WPA can be utilized to provide numerous security enhancements and can coexist with the Universal Access Method (UAM).

1.1. Generic Public Access Hotspot Roaming Model [1]

This section introduces terminology and describes generic functional components needed to support this usage model.

Real-world roaming scenarios can encompass a large number of possible scenarios and network configurations. To make this complexity manageable, we define a generic roaming model that ignores nonessential aspects of roaming. Figure 1 illustrates the generic roaming model with post-paid billing. Other billing models such as prepaid and direct billing to the home provider (e.g., for enterprise users) are possible as well. The Mobile Client depicted in the diagram includes devices such as laptops with WLAN connectivity and handsets with dual WLAN and 2G/3G radios.

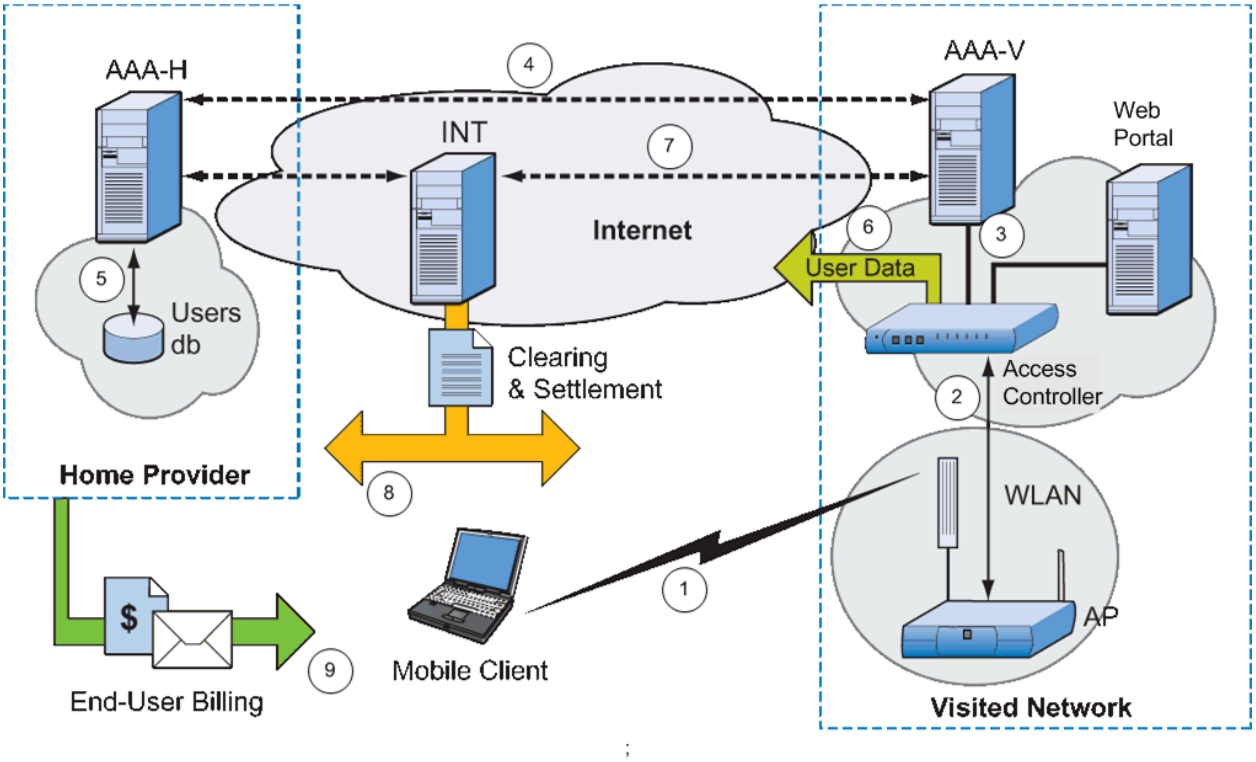

Figure 1: Generic Roaming Model

The numbers shown in Figure 1 correspond to the following steps of a typical WPA-based roaming scenario. The same functional components can also support browser-based authentication (UAM).

1. The wireless station (STA) discovers an IEEE 802.11 access point (AP) and initiates a connection request.
2. The AP (or a network authenticator) responds with a request for the STA identity.
3. The AP forwards the STA identity as an authentication request message to the local authentication server/proxy (AAA-V).
4. The AAA-V examines the STA identity and decides that this is a roaming user. It forwards the authentication request on to the AAA server of the home provider of that user (AAA-H) (sometimes, via an INT) based on the realm name specified in the STA identity. If the mobile user is a subscriber of a cellular network service provider for both his WLAN and cellular-based services (dual-mode), or just for his WLAN-based services only (single-mode), then the authentication of this subscriber will be done with the AAA-H in his home service provider network.
5. The AAA-H authenticates the user via an EAP-based challenge-response method that runs end-to-end between the AAA-H and the STA. A user database is consulted by AAA-H to verify the username and credential provided by the STA. The result of the authentication and session key material are communicated back to the AAA-V, AP and STA.
6. The AP configures link-layer session keys and signals that the STA has been successfully authenticated. Prior to this time, the AP blocks any attempt by the STA to obtain an address or access the Internet.
7. The AAA-V sends accounting messages to AAA-H and possibly to a billing and settlement intermediary as well. When the STA disconnects, an accounting stop message is sent as the last message for that session. The billing and settlement components process the accounting data and generate charging and billing records. AAA-V may also save the accounting records to a log file and send them in batch mode to the billing/settlement provider. Note that a billing/settlement intermediary may also act as an aggregator for authentication. These are independent functions.
8. Charging records are exchanged between business entities involved in this scenario, and settlement occurs.
9. The home provider adds charges to the user's bill for the public WLAN usage.

The dotted lines around the Visited Network in Figure 1 indicate a domain of ownership/management, not a physical boundary. It is likely that one or more of the components shown in the visited network would be centralized and shared across multiple hotspots. The only Visited Network component that must be physically in the hotspot is the AP.

Wi-Fi and the 2G/3G cellular radio technologies are mutually complementary radio access technologies. The combination of Wi-Fi and 2G/3G cellular networks will provide better coverage and service for mobile users. In light of this, the 2G/3G wireless industry standards forums (e.g. 3GPP and 3GPP2) have developed or are developing a number of 2G/3G cellular network-WLAN interworking specifications (see section 10) which will not only enable a user with an STA device to authenticate back to his home cellular network via a WLAN, but may also allow the user to access services provided by

the cellular networks and support roaming and session continuity between the cellular and WLAN networks.

1.2. Functional Components [2]

The following subsections describe the primary functional components in the roaming architecture. It is important to note that these components are logical entities rather than literal components. For example, the INT component (the roaming intermediary) would typically consist of a complex network with multiple subcomponents, possibly managed by several independent business entities. The AC often consists of two separate components (a router plus a special-purpose WLAN access controller or gateway). In other cases, instantiations of this model could combine multiple logical components into a single physical device. Likewise, components such as the AC, AAA proxies and servers, and web portals are often shared across multiple physical hotspots.

1.2.1. Wireless Station (STA) [3]

The STA represents the user's equipment (e.g. a laptop computer, cell phone or PDA) used to access the IEEE 802.11 network. In other forums such as 3GPP, 3GPP2 and GSMA, this component is identified by alternative terms like User Equipment (UE), mobile client or Mobile Station (MS). Its responsibilities include:

- 802.11 network selection - typically by SSID
- Network connection - Users configure their client software on the STA to use the SSID that represents their service provider
- Network authentication - using WPA/EAP or legacy UAM
- Network connection management - according to user preferences.

1.2.2. Access Point (AP) [4]

The AP is the 802.11 access point. It has the following responsibilities:

- RADIUS client - acts as a RADIUS client in 802.1X mode, and sends RADIUS authentication and accounting traffic to the AC or AAA-V
- Link-layer encryption - performs link-level encryption if WEP, WPA or WPA2™ (see section 2 for additional details on WPA2) are used, unless the AP is a thin-AP and the IEEE 802.1X authenticator function and associated link encryption is performed by a centralized controller
- Access Control Enforcement - enforces access control
- Session Accounting - tracks accounting information per session and acts as an AAA client, requesting authentication on behalf of the STA and generating RADIUS accounting records
- Traffic isolation using VLAN tags or IP addresses - may apply VLAN tags to packets
- DHCP Services - the AP may host a DHCP server or serve as a DHCP relay.

1.2.3. Access Controller (AC) [5]

The AC enforces access control for clients accessing the hotspot with the UAM. Its responsibilities include:

- Login Redirect - for users using the UAM, performs the HTTP redirection to the web portal
- Access Control Enforcement - enforces access restrictions on users (via VLAN or IP-based filtering)
- Session monitoring and termination - monitors STA sessions and generates RADIUS accounting records, for UAM users.

The AC may also function as a border gateway and initiate/terminate tunnels to other operator networks. Secondary functions hosted by the AC may include DHCP proxy and firewall.

In some hotspot configurations, APs are lightweight devices that act as simple layer 2 bridges to an AC—the thin-AP model. This model has some advantages in cost and network management overhead compared with a more full-featured APs, but does have security implications. There are no standards for key distribution between the AC and the AP to support WPA in this model. The CAPWAP group in the IETF is working on defining this thin-AP model. Until this model gets completely defined, it is not possible to make a recommendation on its usage. Section 5.1.2.1 discusses this in more detail.

Note: It is also possible to configure a PWLAN network with a centralized access controller shared by multiple hotspots. User traffic is backhauled via a private network to the access controller, which allows authorized traffic to and from the Internet. This is a viable option if the provider has economical backhaul facilities and prefers not to to manage a distributed network of access controllers.

1.2.4. Visited Network AAA Server/Proxy (AAA-V) [6]

This AAA-V functions as an AAA server for customers of the hotspot operator and as an AAA Proxy for roaming customers. In some cases, these two roles (proxy and server) are implemented using separate RADIUS servers, such as when the hotspot operator deploys a local proxy server in communication with the AP/AC and a AAA server that communicates with the local proxy. The AAA-V responsibilities include:

- Authentication processing - proxies RADIUS authentication packets from the AC and/or AP to the AAA-H or to AAA-I servers (the AAA-I designation is used for any AAA proxies of intermediaries)
- Accounting message processing - forwards (and locally logs) RADIUS accounting records associated with sessions to AAA-H and/or billing/settlement INT entities.

1.2.5. Home Provider AAA Server (AAA-H) [7]

The AAA-H component is the RADIUS server that authenticates the STA user. The user's home provider manages the AAA-H. If the UAM is used, AAA-H authenticates the STA using RADIUS authentication with PAP or CHAP (PAP should be avoided as the user's password is transmitted in cleartext, and is open to casual inspection and theft throughout the entire roaming environment. CHAP does not send the password in cleartext, but it is vulnerable to dictionary attacks). If WPA is used, AAA-H authenticates the STA using an EAP method. WPA session keys derived by the AAA-H are distributed back to the AAA-V and ultimately to the AP. The AAA-H may also receive accounting and/or charging records from AAA-V or from INT. The home provider can correlate accounting records with archived records of authentication events

to detect fraud and billing-related problems. Prepaid home providers also use the accounting records to dynamically update the prepaid balance.

Although a home provider may often operate a hotspot, the essential characteristic of the home provider is that it maintains the business relationship with the user and implements an AAA service to authenticate roaming users. Home providers do not need to operate a wireless network to fulfill this role.

The AAA-H may in turn interface to other non-RADIUS backends (such as MAP over SS7 to a HLR or HSS) in a cellular operator's authentication and subscription management infrastructure.

1.2.6. Web Portal [8]

The Web Portal (an optional component) may support browser hijack-based authentication (UAM). It may also be used to provide information to the user to enable configuration of WPA profiles. A web portal may also enable establishment of new subscriptions and specialized services for authenticated and non-authenticated guests. A separate web server is not necessarily required.

1.2.7. Roaming Intermediary (INT) [9]

The INT component represents a wide variety of one or more AAA and billing intermediaries. It may correspond to multiple physical components and networks operated by aggregators, brokers, charging/billing clearinghouses or settlement providers. Note: If the intermediary forwards RADIUS messages, we often use the notation AAA-I instead of INT. Intermediaries perform functions such as:

- Authentication forwarding to a AAA-H (acting as a roaming broker)
- Accounting and storage of accounting records
- Conversion of accounting and billing records to other formats or to add tax information
- Fraud detection
- Billing and reconciliation
- Wholesaling of bandwidth and services.

2. What is WPA?

Wi-Fi Protected Access is a wireless encryption standard based on a subset of IEEE 802.11i that replaces WEP. Designed to run on some existing WEP-based hardware as a software upgrade, Wi-Fi Protected Access is derived from and will be forward-compatible with the upcoming WPA2 standard. When properly installed, it will provide wireless LAN users with a high level of assurance that their data transmitted over the radio link will remain protected through the WPA encryption method and only authorized users can access the network.

WPA utilizes the Temporal Key Integrity Protocol (TKIP). TKIP provides data encryption enhancements through a per-packet key mixing function and a message integrity check (MIC), an enhanced initialization vector (IV) with sequencing rules, and a session-derived re-keying mechanism. To strengthen user authentication, WPA implements 802.1X and the Extensible Authentication Protocol (EAP). Together, these mechanisms provide a framework for strong user authentication, including mutual authentication. [10]

Wi-Fi Protected Access 2, or WPA2, is also based on 802.11i. It adds additional security features, the most important of which are pre-authentication, which enables secure fast roaming, and AES (Advanced Encryption Standard)–the new FIPS standard for data encryption.

2.1. Why Service Providers Should Deploy WPA

There are many reasons to adopt WPA for use in Public Access Wi-Fi, particularly in the areas of flexibility, interoperability, security and privacy. WPA provides a strong, standards-based, interoperable security solution that addresses all known flaws in the original WEP-based security. It allows for safer public WLAN access by supporting a stronger authentication method that will protect users and operators from fraud and man-in-the-middle attacks that are possible in current UAM deployments. It is also now a required feature on all Wi-Fi CERTIFIED™ products.

2.1.1. Security: Data Encryption - Dynamic and Individual Key Management

The Temporal Key Integrity Protocol (TKIP) is part of the IEEE 802.11i (and WPA2) encryption standard for wireless LANs. TKIP is the a successor to WEP, the Wired Equivalency Protocol, which is used to secure 802.11 wireless LANs. TKIP provides per-packet key mixing, a message integrity check and a re-keying mechanism, thus fixing the flaws of WEP. [11]

In WPA, the TKIP key hierarchy starts with the Pairwise Master Key (PMK), which is supplied by an EAP authentication method that is designed to generate key material. The Pairwise Transient Key (PTK) is derived from this PMK. A 128-bit shared secret, the Temporal Key (TK), is formed as a portion of the PTK. The transmitter's MAC address is mixed with TK to produce a Phase 1 key. The Phase 1 key is then mixed with an initialization vector (IV) to derive per-packet keys. Each key is used with RC4 to encrypt one, and only one, data packet. Ultimately, the IEEE is expected to use the Advanced Encryption Standard (AES), a more appropriate cipher for wireless. Unfortunately, AES requires considerably more horsepower than most existing 802.11b cards provide. Keeping RC4 for now means that TKIP can be deployed in firmware updates instead of new chipsets, protecting consumer investment in 802.11b gear. [12]

2.1.2. Security: MIC Data Authenticity

MIC, or Message Integrity Check, is part of the 802.11 standard. In short, MIC prevents the tampering with a packet during transmission over Wi-Fi. As a part of TKIP, MIC provides an additional 8-byte field within the 802.11 frame which protects both the data payload and the packet header from manipulation via a per-packet keyed 64-bit hash.

The algorithm which implements the MIC is known as *Michael*. Michael also implements a frame counter, which discourages replay attacks.

2.1.3. Security: 802.1X – Port-Controlled Access

802.1X is a mechanism for port-based network access control. In the WLAN context, it specifies the use of virtual ports to control access to the network. It ultimately protects the providing network by allowing only legitimate clients to connect to the network.

802.1X authentication, with EAP over LAN (EAPoL), has established itself as the next-generation access method for Public Access WLAN networks. 802.1X provides several notable benefits when compared to the UAM, such as:

- 802.1X is an IEEE standards-based protocol specifically geared for AAA. The current UAM method used for public access relies on HTTP and SSL to control and secure access requests via a standard Internet browser. While this method provides a mechanism for walk-up provisioning and has minimal client requirement (just a web browser), the scheme relies on non-AAA protocols not intended for per-user/per-session access control. 802.1X provides an authentication method suitable for Public Access, but requires the supplicant software be installed on the user's device; this supplicant software is now available on all PC devices sold today.
- It provides secure port-based access control. Since an 802.1X supplicant directly negotiates with an access point at the radio level, the user's device is not given network layer connectivity until AAA is successful. This provides security for both the network itself and end-users since only authorized and accounted devices have an IP Address from which to interact with the network.
    - 802.1X supports a variety of standard EAP Authentication Methods, including password, token-based and SIM-card-based methods, and 3GPP/3GPP2-recommended EAP authentication methods (such as EAP-AKA, EAP-SIM and EAP-TLS).

2.1.4. Security: EAP Methods and Mutual Authentication

One of the most powerful features of WPA as it applies to Public Access Wi-Fi roaming is its capability for Mutual Authentication via 802.1X and EAP methods. In many legacy roaming networks, users trusted aspects of an Internet connection to ascertain whether it was safe to disclose their access credentials, such as a unique phone number or a branded kiosk with a hardwire. The fact that the access equipment was connected by wire to their service provider was trusted to imply that the equipment was under the control of the service provider. The flexibility and availability of Wi-Fi means that anyone can deploy a Wi-Fi hotspot with a familiar SSID. A radio signal with a familiar SSID does not ensure that the user will be connected to equipment operated by a service provider that the subscriber trusts. This places a special emphasis on mutual authentication to ensure the user is connected to a trusted network and that they are transacting with a valid network before disclosing credential information for purposes of network access.

Through 802.1X and RADIUS, EAP messages can be exchanged between the client station requesting service (the Supplicant) and the Home Authentication Server which maintains that user's service profile. In EAP exchanges using TLS-based EAP methods such as EAP-TLS, EAP-PEAP or EAP-TTLS, a TLS handshake (secured by a PKI certificate) is performed. The service provider's public certificate is provided by the Authentication Server and validated by the user's 802.1X supplicant as an authentic, valid and trusted certificate through a signature provide by a known and trusted Certificate Authority. The TLS handshake also generates session keys that are used to create a TLS/SSL encryption tunnel. The 802.1X supplicant uses this private encryption tunnel to disclose its access credentials to the home provider's authentication server. This two-step authentication exchange of first authenticating the authentication server and then authenticating the user is known as Mutual Authentication. Depending on the EAP methods used, credentials can be in different forms, for example username/password combination, token, SIM card or PKI Certificate. In all these examples, the key is protecting the entire process through a strong cryptographic process and a known infrastructure of trust.

Only the home authentication server can make a determination if the user is a valid subscriber for its service. The entire exchange of authentication, authorization and accounting messages is trusted by each AAA server from the visited network, through intermediaries, to the home AAA server because each link between AAA servers is protected by a shared secret. The chain of protected links form a chain of trust that is used to attest to the validity of messages from visited network to the home network.

2.1.5. Flexibility: Support for Various EAP Types

EAP, or Extensible Authentication Protocol, was originally designed for PPP RAS devices. Prior to EAP, Network Access Servers were only able to perform pre-determined authentication methods (PAP or CHAP) which must be supported by the connecting client peer. The implementation of EAP into a RAS device provided a methodology to expand the authentication methods it supports for port-based access without requiring hardware-level upgrades as new methods are introduced. As with PPP, EAP is a fundamental component of 802.1X. Originally designed for LAN devices such as Ethernet switches, 802.1X may also be used to provide port-based access control to Wireless LAN (WLAN) resources such as an 802.11 access point.

With EAP's variety of authentication mechanisms, access authority may be maintained through a network's RADIUS trust chain without compromising the integrity of the user's access credentials or requiring that any particular authentication method be used.

EAP doesn't mandate any particular AAA mechanism or authentication method, but rather allows an access point to facilitate the AAA negotiation between a network peer (802.1X supplicant running on a laptop) and defer the authentication to another back-end device which actually implements the AAA mechanism. In this way, the AP itself acts merely as a "pass-through" which needs only to receive the success/failure from its AAA back-end and report the resulting usage for reconciliation.

2.1.6. Interoperability: A Standards-Based Solution

WPA is a standards-based solution. This means that its adoption and correct implementation by client and network devices would allow for interoperability between a wide variety of clients and hotspot networks operated by different service providers, thus increasing the probability of achieving global roaming.

2.2. Challenges to WPA Deployment

Though WPA provides a number of benefits both to subscribers and service providers for deployment in a public access hotspot environment, there are some challenges to its wide deployment in the near-term.

- Some access points that are currently deployed in public access hotspots may need an upgrade to support WPA. In the best case, this will only need to be a firmware upgrade; if this is not possible, then the AP itself might need to be replaced.
- One of the recommended deployment options in section 3 requires the use of a single AP broadcasting at least 2 SSIDs, each tied to a unique BSSID. This feature is not yet commonly available to AP hardware today.
- New customers to a hotspot location may not be aware that WPA-based access is available by just monitoring the broadcast SSIDs. One way to get around this issue is to provide information on the Welcome Portal page (if a UAM mechanism is also available in that hotspot) to advertise the availability of WPA access.
- Configuration of most wireless client software to connect to a WPA-based network is not trivial. Users will need the appropriate education and customer service help in order to accomplish this when they first want to sign up for an account and set up a profile. Once the profile is set up though, subsequent connection attempts will be seamless. There is a need for good client provisioning software to overcome this issue.

3. Deployment Options for Coexistence

When deploying a public access Wi-Fi network with WPA, care has to be taken to ensure that legacy clients (that only support UAM-based access) can still be used to access the network. This is commonly referred to as "coexistence." The infrastructure must be able to support the coexistence of both UAM and WPA, thus allowing for both types of users to access the network. In deploying coexistent Wi-Fi hotspots, not only should the addition of WPA authentication (with its RADIUS requirements) be considered, but one must also ensure that security of WPA users is not compromised by the less secure UAM access mechanism.

This section highlights different UAM/WPA coexistence deployment options with these requirements in mind.

Of these possible options, the recommended approach is option 3, where a single AP is deployed with at least two unique broadcast SSIDs/BSSIDS, one for UAM and one for WPA. Option 1 allows for construction of coexistence models using currently available hardware, but it is not completely standards-compliant and will cause client compatibility issues. Option 2 uses currently available hardware in a standards-compliant manner, but requires double the number of APs for each coverage area. APs that support option 3 are not widely available as yet; however, work is being done in this area, and this model allows for the cleanest deployment. It does not require double the number of APs and is also standards-compliant. The sections below describe in detail the three deployment options with their respective pros and cons.

3.1. Option 1: One AP for Both UAM and WPA, Single BSSID

This is a deployment option that is available today, but has the risk of not being completely standards-compliant. A single AP is used for both UAM and WPA access in this model. This AP broadcasts an open SSID for UAM, and also supports a hidden SSID for WPA. The figure below depicts this model.

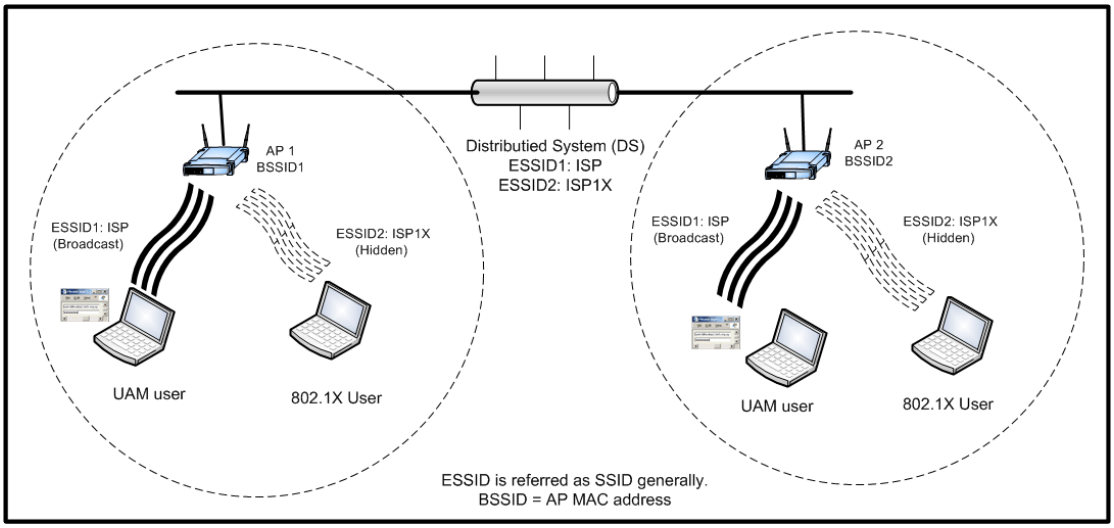

Figure 2a: One AP, single BSSID, broadcast and hidden SSIDs

APs with this functionality are available in the market, but since this deployment option is not completely standards compliant, there are potential client compatibility issues. Since

the WPA SSID is hidden, clients that are not pre-provisioned will have no means of detecting the availability of WPA. Another fundamental issue is the use of shared broadcast domains and shared BSSIDs. Broadcast traffic is sent to the broadcast domain tied to the BSSID, which means that both UAM and WPA clients will receive all broadcast traffic. If different broadcast keys are used for the WPA and UAM SSIDs, the error counters for incorrectly encrypted traffic will increase for every broadcast packet that is received with a wrong key. Manageability of the AP is therefore decreased, as this counter cannot be used to accurately tell if the AP is under attack or not. Another issue is the advertisement of capability sets; each of these SSIDs obviously have different capability sets, since at a minimum the broadcast UAM SSID has the privacy bit turned off, and the hidden WPA SSID has the privacy bit turned on and must also include the WPA IE. However, the AP only supports a single BSSID (single MAC address) and therefore a single capability set; mapping both these SSIDs to the same BSSID cannot be accomplished in a standards-compliant manner. A number of other features in 802.11 (such as the advertisement of QoS, radio settings and power-save settings) are tied to the BSSIDs; sharing a single BSSID across multiple access types therefore leads to compatibility problems.

Existing AP hardware may be used in this deployment option, though it requires functionality beyond what is certified by the Wi-Fi Alliance and what is standards-compliant.

We have noted previously that a client that is not pre-configured with a profile for this network will be able to scan and detect the broadcast UAM SSID, and connect to that; it will be unable to detect the WPA SSID. A client that is pre-configured with the WPA SSID will be able to probe for and detect that SSID, and then connect.

In order to solve the issue noted above, where a non-provisioned client cannot detect the presence of the WPA SSID, a hotspot configuration utilizing multiple alternative AP configurations may be deployed. In this configuration, each hotspot coverage area hosts 2 APs with alternating configurations and overlapping coverage zones. The Tore-Alexander Coexistence Deployment Option [13] relies on overlapping WLAN radio coverage of a single location by access points with different security settings. In this solution, a minimum of two access points are used for each hotspot area. One AP broadcasts an open SSID for UAM access, while the second AP broadcasts a separate SSID with the privacy bit set for WPA users. Each AP has the capability to service either SSID, but only broadcasts one (deployed in an alternating fashion).

AP1	**AP2**
BSSID1/SSID-UAM broadcast	BSSID2/SSID-WPA broadcast
SSID-WPA hidden	SSID-UAM hidden

A minimum of 2 APs is required per cell (hotspot coverage area) with this model. A client that does not have pre-configured profiles will detect both the UAM and WPA BSSID/SSSIDs; the client will be able to differentiate between the two types of access methodologies by detecting the presence/absence of the privacy bit in the beacon. A client with pre-configured profiles for either the UAM or WPA SSID will automatically detect and connect to the appropriate AP. Therefore access points deployed under this methodology will require sufficient overlapping coverage as to allow a wireless station to detect the beacons of any two APs using different security settings at any one time. Once the network is selected and the SSID is set on the wireless station, the closest AP will be used to connect to the network using the appropriate SSID and security mode.

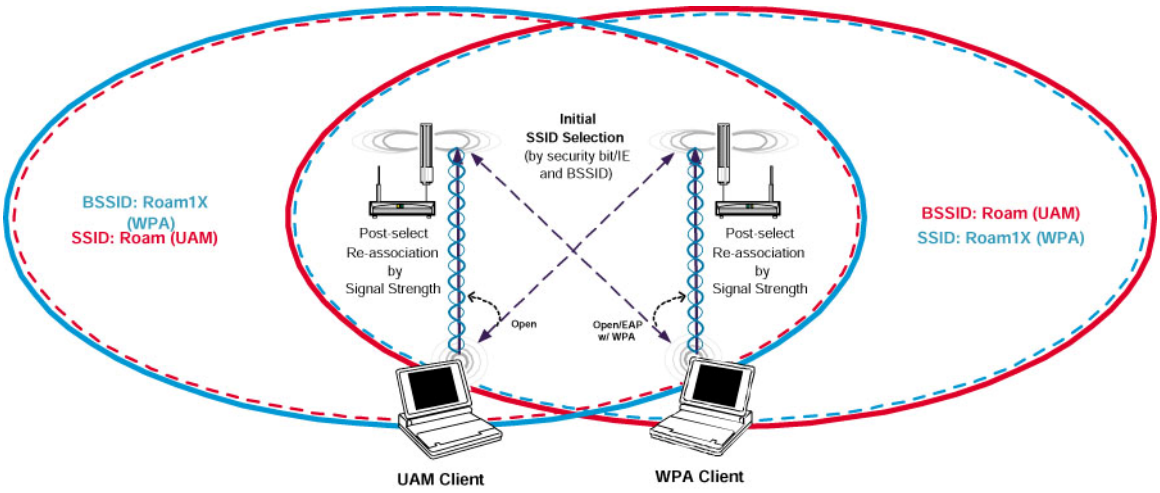

Figure 2b: Tore-Alexander Coexistence

Problems with overlapping cells using the same channel are likely to occur. Once the station associates with either one of the broadcast SSID, it will "switch" to the closest AP for the purposes of data transport.

In this way, a client in a given hotspot coverage area will be able to detect the presence of both the UAM and WPA SSIDs, and select which one he would like to connect to. Once a profile is created for a given SSID, the client will automatically connect to that SSID, whether or not the SSID is broadcast.

3.2. Option 2: Two APs, Each Broadcasting a Single SSID

Two different access points are used for each hotspot area. One AP broadcasts an open SSID for UAM access, while the second AP broadcasts an SSID with the privacy bit set and the appropriate Information Elements (IEs) for WPA access. The SSID broadcast on each of these APs could either be the same or different; each AP, however, will have its own unique BSSID (and MAC address). This model is depicted in the following figure.

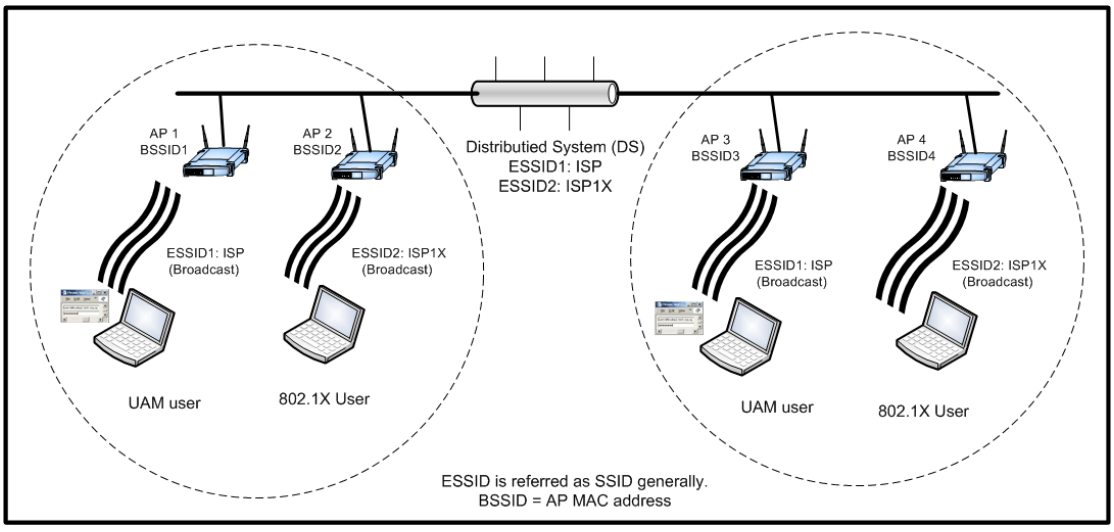

Figure 2c: Two APs, each broadcasting a single SSID

A minimum of 2 APs is required per cell (hotspot coverage area) in full redundancy. A client that does not have pre-configured profiles will detect both the UAM and WPA SSIDs; the client will be able to differentiate between the two types of access methodologies by parsing the information contained in the beacons. A client with pre-configured profiles for either the UAM or WPA SSID will automatically detect and connect to the appropriate AP.

Using the same SSID in the beacons for both APs allows for simplified user experience as the user does not need to deal with multiple SSID names for the same provider. Client software will however need to be able to parse and recognize different BSSIDs with the same SSID. Using different SSIDs for the UAM and WPA access methods has the advantage of not requiring client software to deal with parsing and recognizing different BSSIDs with the same SSID, and therefore provides broader compatibility with a wider range of clients. It however, requires users of clients that have not been pre-provisioned to associate both the SSIDs with the same provider. Hints may be provided by using SSID names such as “operator” and “operator1X.”

This deployment option is completely standards-compliant, and uses low cost APs that are easily available in the market today. This option requires double the number of AP hardware though, as each coverage area will require two APs instead of one. Another issue with this deployment option is that problems with overlapping cells on the same channel are twice as likely to occur.

3.3. Option 3: One AP for Both UAM and WPA, Multiple BSSIDs

This deployment option is similar to option 2, but requires a single AP that emulates multiple APs. Each logical AP that is supported on this physical AP must be capable of broadcasting an SSID associated to a unique BSSID. This model is depicted in the figure below.

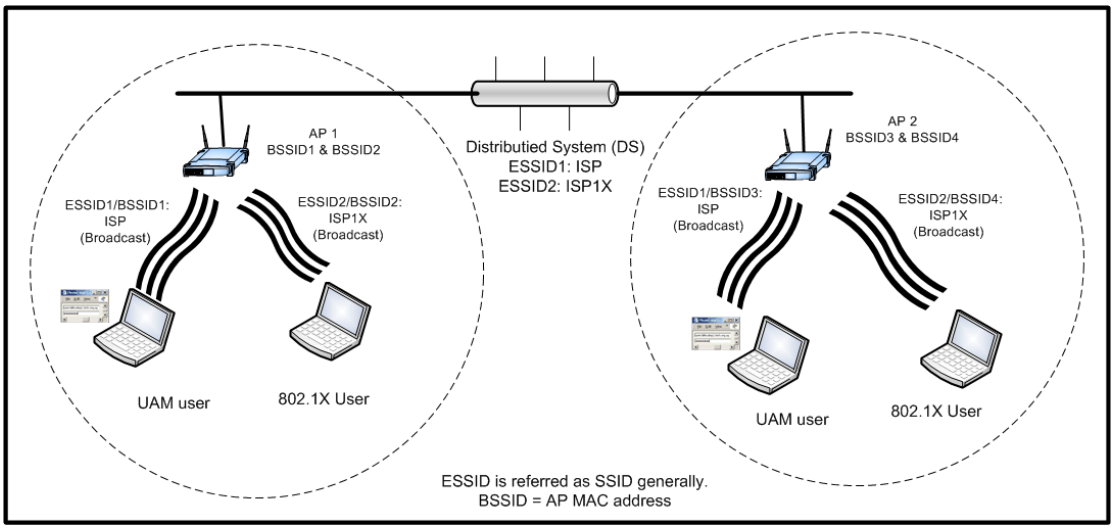

Figure 2d: One APs, multiple BSSID/SSIDs

Each hotspot coverage area deploys a single AP for both UAM and WPA access. This AP supports at a minimum unique BSSID/SSIDs, one for UAM and one for WPA. The AP broadcasts one SSID for UAM access, and another separate SSID for WPA access. Each broadcast SSID is associated with a unique BSSID, and each SSID also advertises the appropriate capability set for the particular method of access (UAM or

WPA) that it supports. The SSID name used in each of these broadcast beacons could either be the same or different, depending on operator requirements.

A client that does not have pre-configured profiles will detect both the UAM and WPA SSIDs; the client will be able to differentiate between the two types of access methodologies by parsing the information contained in the beacons. A client with pre-configured profiles for either the UAM or WPA SSID will automatically detect and connect to the appropriate AP.

Using the same SSID in the beacons for both APs allows for simplified user experience as the user does not need to deal with multiple SSID names for the same provider. Client software will need to be able to parse and recognize different BSSIDs with the same SSID. Using different SSIDs for the UAM and WPA access methods has the advantage of not requiring client software to deal with parsing and recognizing different BSSIDs with the same SSID, and therefore provides broader compatibility with a wider range of clients. It however, requires users of clients that have not been pre-provisioned to associate both the SSIDs with the same provider. Hints may be provided by using SSID names such as “operator” and “operator1X.”

This deployment option is standards-compliant, and is functionally rich. It also allows for extensibility with the minimum amount of hardware infrastructure. One of the challenges of this current model is that implementations of this kind are not yet widely available or deployed, though a lot of work is being done in this area.

4. Use Cases

This section describes certain usage scenarios that are enabled by deploying a WPA-based Wi-Fi Public Access network.

4.1. Dual Authentication: WPA and UAM Coexistence

This is a typical usage scenario that will become commonplace with the increased deployment of 802.1X and WPA-based Wi-Fi networks. When an operator chooses to deploy a WPA network based on one of the options listed in section 3, both WPA and older browser-based clients will be able to use that hotspot.

The legacy UAM clients will associate to the open SSID and subsequently obtain an IP address. The client will then be placed on a guest or unauthenticated segment until a browser session is initiated and the client is redirected to a login page. Once the client successfully authenticates via that login screen, he will then be given access to his subscribed services.

WPA clients, too, will be able to use this network by associating with the WPA SSID. The WPA supplicant on the client will kick-off soon after association, and the pre-configured EAP method will be run for client and server authentication. Once that completes, the WPA user will then be given access to her subscribed services too.

It is expected that such models will become common-place in hotspots around the world with increased WPA deployment. Hotspot operators will deploy WPA for the benefits it brings (as noted in section 2), while at the same time provide continued support for legacy UAM users. This will enable a smooth transition from UAM to WPA-based authentication.

4.2. Mixed-Mode: Public & Private Access

There are certain scenarios where a single hotspot must cater to different types of users. A typical example would be an airport hotspot model, which in the simplest case would support 3 different types of users: guest, authenticated visitors and airport staff.

Guest and authenticated visitors would ideally be given public access to this hotspot network, either via UAM or WPA access. Airport staff, on the other hand, will be given private access to this network, and they would securely access the network using WPA. Segmenting these different types of users can be accomplished either using VLANs or a form of IP filtering, and is an implementation decision.

Once a user authenticates to the network, a combination of the credentials used, as well as the SSID that the client has used for association, will determine the access that is to be granted. As noted in the deployment options in section 3, there are multiple ways this could be implemented. The AP(s) could support multiple SSIDs for the different user classes, and each user could be put on a different VLAN depending on the SSID used for association. Alternatively, all users could associate using the same SSID, and the credentials used for authentication can determine the type of access granted.

This model provides for very powerful access control—the same network could be securely used by different classes of users, for different purposes.

4.3. Support for Multiple Authentication Methods

The use of WPA and 802.1X implies the use of EAP as the authentication protocol. As a result, the network is not limited to supporting only one single authentication method. By virtue of the properties of EAP, more than one EAP method (EAP-MSCHAPv2, EAP-SIM, etc) can be used for authentication on the same network, as long as they are supported by both the client and the AAA server implementations.

The operator can choose to support a given set of EAP methods, based on criteria such as their security properties or availability on client platforms. Traditional WISP operators might choose to use EAP-MSCHAPv2 within PEAP, while 2G/3G cellular network operators might prefer EAP-SIM or EAP-AKA. Various clients that may support only one of these different EAP methods can then connect to the network using the method that each supports.

5. Authentication

5.1. Coexistence of UAM and WPA Methods

5.1.1. Typical UAM Model [14]

Many 802.11 hotspot operators currently use browser connection hijacking to direct unauthenticated users to sign-up pages of the wireless ISP (WISP). The sign-up pages are delivered using SSL for security with the presumption that the user will perform the appropriate validation of the server certificate. This assumption is generally not valid, and this introduces a security vulnerability to man-in-the-middle (MITM) attacks and network impersonation attacks. More discussion on the security problems of UAM are listed in section 6.1.2 below. For additional information on the use of UAM in the context of WLAN roaming, please refer to the Wi-Fi Alliance WISPr document [2].

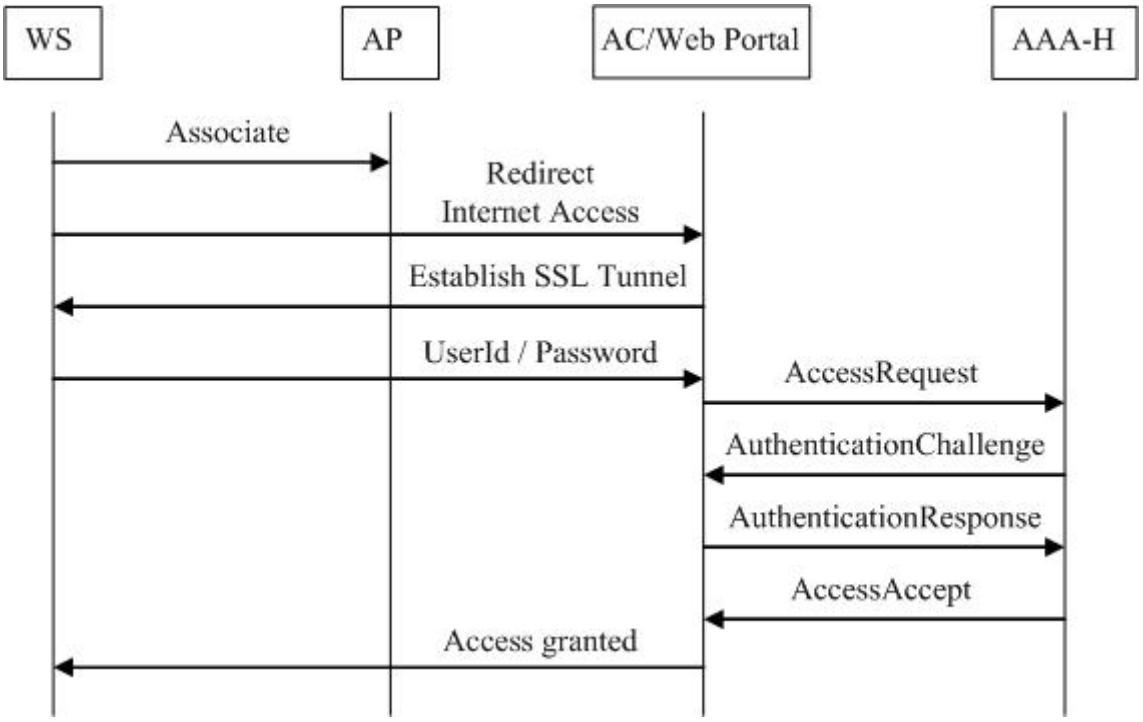

Figure 3: Typical Universal Access Method Model

This UAM model has a number of security risks associated with it, including spoofing the sign-up pages of an operator, man-in-the-middle attacks, availability of the username and password in clear text at the web portal, and snooping traffic over the unencrypted air interface. A summary of these security risks can be found in [1] section 7.2.1.

5.1.2. 802.1X-based Authentication Model [15]

Figure 4 depicts a typical protocol stack for 802.1X-based authentication. The EAP messages are carried over EAPoL (EAP over LAN) frames between the STA and the AP and then reencapsulated in RADIUS messages when sent from the AP to the home AAA Server (via zero or more AAA proxies). In Figure 4, the mobile client acts as the 802.1X supplicant, the AP acts as the authenticator and the RADIUS AAA server acts as the authentication server.

For security reasons, RADIUS is sometimes also carried over IPsec (RFC 3162 describes use of RADIUS over IPv6-IPsec, and RFC 3580 also recommends use of IPsec to protect RADIUS). In the future, Diameter may be used instead of, or in addition to, RADIUS.

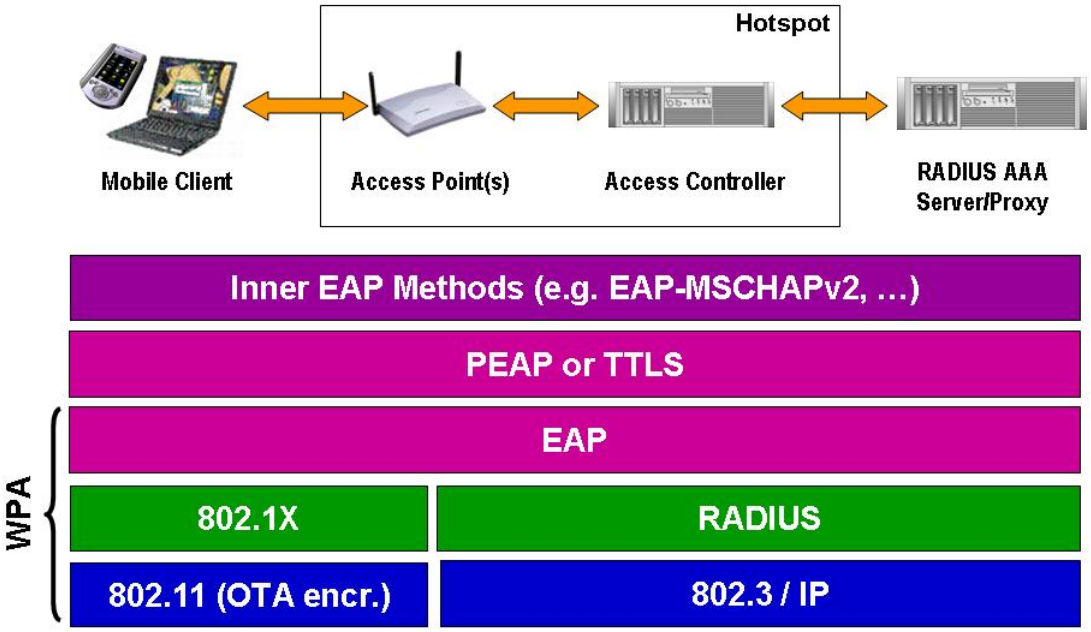

Figure 4: EAP authentication protocol stack

There are significant advantages of the WPA model over the UAM model. One of the most important advantages is that WPA is designed to support extensible authentication between the STA and the home provider's AAA-H that may be protected by an end-to-end TLS tunnel. This is a very significant architectural point, because it enables great flexibility in credential types and authentication methods. The TLS channel established by EAP methods can support arbitrary authentication protocols and credential types, provided an appropriate inner protocol is defined. Furthermore, since the TLS channel is established between the STA and the AAA-H, there is no need for the visited network's AP or AAA proxy to comprehend or support the specific EAP method or credential types used by the home provider. This dialog can be completely private between the subscriber and their home provider, protecting the subscriber-provider relationship from roaming partners who also may be competitors.

With 802.1X, the STA can initially access only the uncontrolled port on the AP (or network switch behind the AP, depending on the implementation). The uncontrolled port limits the STA to using the EAP protocol with the network's authentication infrastructure. If the STA and network successfully authenticate each other, the STA is issued session keys and is granted access to the controlled port. At this point, the STA is typically given access to the Internet.

Figure 5 depicts a typical 802.1X-based roaming scenario. The STA attempts to associate with an AP and is challenged to authenticate. At this point, the STA indicates its user identity. There are two parts to this identity: the user name and the realm. Typically these are combined into a Network Access Identifier (NAI) of the form user@realm. The realm part of the NAI is used to establish a connection with the appropriate AAA-H for that user. This presumes that the visited network's AAA-V recognizes that realm name. If this is not the case, then the visited network will signal an authentication failure back to the STA. The STA can then either try a different account (with a different realm) or can try to establish a new account on the visited network. If those alternatives also fail, the STA will be denied access or will be granted only limited guest access.

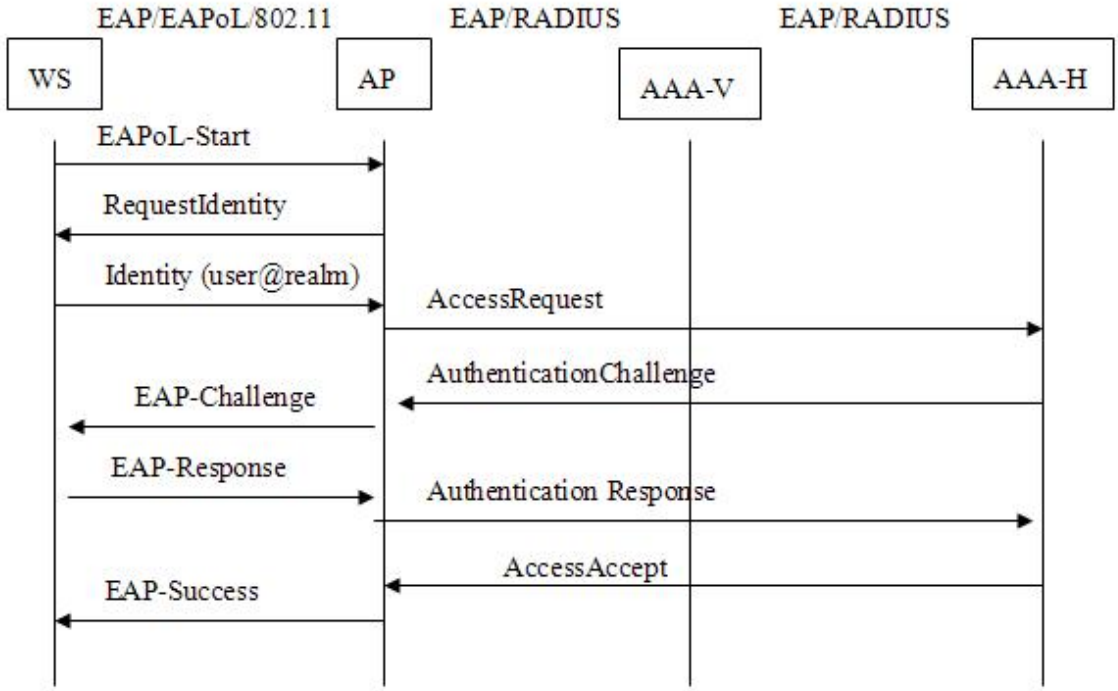

Figure 5: 802.1X-based Authentication

Although the figure appears to show direct communication between the AP and AAA-H, ordinarily the RADIUS connections are established between RADIUS servers and proxies (e.g., AAA-V) on a hop-by-hop basis. Therefore, there is no need for AAA-H to have direct communication with a hotspot's AP devices. Furthermore, the actual number of EAP messages exchanged is variable, and depends on the EAP method used; some methods are more verbose than others.

5.1.3. Thick vs. Thin APs

As noted in the discussion in Section 3.2.3, there is more than one way to develop a hotspot architecture compliant with this generic blueprint. In Figure 5, the AP is acting as the 802.1X authenticator. This requires a comparatively full-featured AP with full 802.1X support. This AP should also be capable of functioning as a RADIUS client, and is traditionally termed a thick-AP.

There exists another deployment option as well with respect to the functionality of the AP. A thin-AP is one that does not perform the 802.1X termination itself, but relies on a

more powerful device further on in the network to act as the 802.1X authenticator and RADIUS client. This type of device is undergoing standardization within the IETF, in the CAPWAP group [3].

If service providers choose to deploy a thin-AP prior to the completion of the CAPWAP standard, it is recommended that the AP-AC entity be considered as one; together, this entity must be able to support all the functionality that a standalone AP and AC would, as described in section 1.2. Specifically, it is also a requirement for clients to unicast all EAPoL messages to the AP, and the AP to forward these messages to the AC (the 802.1X authenticator).

5.1.4. Coexistence of WPA and UAM Methods [16]

Because migration from UAM authentication to WPA authentication is expected to occur gradually over time, it is important to support coexistence of both methods during the transition phase.

Section 3 described the deployment options for coexistence of WPA and UAM methods with respect to the client and the AP. This section will detail how a complete hotspot network supporting coexistence can be deployed using multiple SSIDs and VLANs/IP filtering.

This scenario is described using deployment option 3 as specified in section 3. Figure 6 illustrates how a VLAN-capable AP can partition UAM traffic from WPA traffic. To support both WPA and UAM as listed in deployment option 5, the AP supports two different SSIDs, one corresponding to 802.1X/WPA and one open (for UAM). Each SSID maps to a unique BSSID on the physical AP. The 802.1X SSID supports WPA (and eventually the full WPA2 solution). The open SSID would not require any link-layer security, but the AC would limit user access to the local web portal until the user has obtained authorization to use the network. Subsequent enforcement of access control for the UAM method is typically based on a combination of the IP address and the MAC address, which are vulnerable to spoofing for fraudulent access. Attackers can easily configure their own equipment with the same MAC and/or IP address and masquerade as legitimate users, stealing their bandwidth or fraudulently obtaining service. This creates a business incentive for network providers to migrate users away from UAM as soon as practical. One possible coexistence strategy is conceptually depicted in Figure 6. This strategy includes the following assumptions:

- Access points utilize VLAN tagging per SSID.
- Local AAA server is typically deployed centrally in the WLAN operator network (not in the hotspot).
- Intermediate RADIUS hops are protected. The recommended mechanism for this is to use IPsec (please refer to RFC 3579 and RFC 3580).

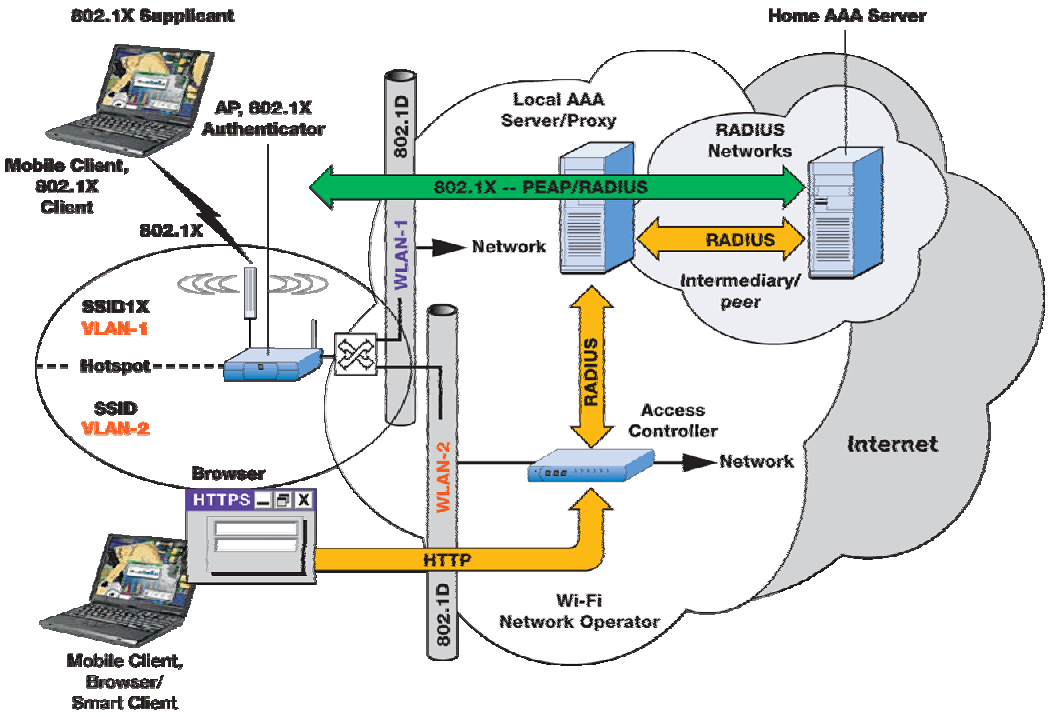

Figure 6: WPA and UAM Coexistence

Since the AP in this scenario is capable of advertising both SSIDs, the STA will be able to detect them and choose the appropriate one. The AP assigns separate VLAN tags to packets according to the SSID the STA is associated with. The VLAN switch in turn routes the packets during authentication so that the WPA traffic gets sent to the AAA-V for authentication and the browser hijack mechanism is used for the non-WPA clients. The web portal for UAM is not shown in the figure (it could be implemented by the access controller). Note also, that although the figure does not show the access controller in the data path for the WPA traffic for simplicity; in reality, the access controller may be in the path for both the UAM and the WPA traffic.

Other coexistence models are possible as well. For example, if traffic from the WPA clients and UAM clients is mixed, the VLAN switch can be eliminated, and the Access Controller can manage both types of clients, e.g. by analyzing the traffic and checking for the EAPoL start frame to determine that the STA wants to use WPA.

There are therefore two basic ways by which access control can be implemented in WLAN deployments—VLANs or IP/MAC address filtering. These methods can be either used separately or in conjunction with each other. It is recommended that these two methods be used in conjunction with each other, as that provides for fine-grained access control.

5.2. Supplicant Network Discovery & Selection [17]

The primary means of network discovery in public WLANs is through 802.11 beacon frames or probes. Beacon frames sent by the AP contain the SSID advertised by the network, and a STA can connect to the network by associating with the AP and attempting to authenticate. SSIDs can be correlated to WISP identities and credentials for authentication.

Beacons and SSIDs meet their designed purpose as noted above. However, there are no global conventions on the format for public SSIDs, and it is also hard to guarantee that every network operator has a unique SSID. A STA client may want to discover whether a previously unknown hotspot is affiliated with that client's home provider. The SSID does not contain this information, and it was not designed to. If the client has a local database that maps SSIDs to roaming partner information, then discovering the SSID would enable discovery of this other information as well. However, if the client does not have such a database, if the database entry is out of date or if the SSID encountered is not in the database, some other means of obtaining information about the network is needed.

Since SSIDs are insecure, limited in length and lack a formal global convention on their format for public use, WLAN operators should not use SSIDs for more than their original use: advertising the presence of the network and giving a hint as to the identity of the WLAN operator.

Note that the 2G/3G wireless industry standards development forums (such as 3GPP and 3GPP2) have also specified mechanisms for WLAN network advertisement, discovery and selection to adapt them to the 2G/3G cellular-WLAN interworking environment. It is recommended that where possible, the relevant 3GPP and 3GPP2 specifications ([3GPP 22.234/23.234] and [3GPP2 X.P0028-0]) be used.

5.2.1. Using Single vs. Multiple SSIDs for Network Advertisement [18]

A significant architectural question for hotspot network advertisement is whether to and how to support multiple SSIDs. Multiple SSIDs can be used to support simultaneous use of browser hijack and WPA. Multiple SSIDs can also simplify sharing of common WLAN infrastructure across multiple logical networks.

Although SSIDs are not managed by any central authority, they are a critical and often highly-visible aspect of the hotspot experience. If only one SSID is visible to the user, then the user will not be faced with a choice as to which SSID to select. This has certain usability benefits, but it can also introduce limitations; for example, the hotspot will only be able to support either UAM or WPA, but not both. There is no standards-compliant way that a hotspot supporting coexistence can be built using an single BSSID/SSID combination.

Multiple SSIDs are especially useful if the WLAN infrastructure is used for both public and private use. For example, an airport might deploy a shared WLAN hardware supporting both public access and private use by airport staff. Rather than deploy redundant WLAN hardware, two virtual WLAN networks with different SSIDs could be hosted on the same physical access points. The private network could be isolated from the public using link layer security and a separate VLAN associated with the private network's SSID.

Furthermore, in many locations, users will naturally detect multiple SSIDs—some from the provider they wish to receive service, and others from other networks in the neighborhood. Increasingly, users must know which SSID they need to associate rather than blindly associating to an SSID and hoping it is the right one.

5.2.2. Discovering and Selecting Roaming Intermediaries

The IETF EAP working group and 3GPP standards groups are collaborating to define a standard mechanism for delivering descriptive information about the network to EAP clients. Although work in this area is preliminary, consensus appears to be building

around use of the EAP-Identity-Request message to convey this information. For example, refer to the work being done in the RADEXT working group in the IETF.

The premise of this work is that given the right information prior to authentication would enable the STA client to modify its network access identifier (NAI) to indicate which roaming intermediary should be used to route the EAP connection. Since this is work in progress, it is only recommended (and not required) that this be supported.

More information on this topic may be found in [1] section 3.1.2.

5.3. Credential Types [19]

WPA uses 802.1X authentication with one of the Extensible Authentication Protocol (EAP) types available today. 802.1X is a port-based network access control method for wired, as well as wireless, networks.

EAP handles the presentation of users' credentials, in the form of digital certificates (already widely used in Internet security), unique usernames and passwords, one-time passwords, smart cards, or any other identity credentials that an IT administrator is comfortable deploying. WPA allows flexibility in both the type of credentials that are used and in the selection of an EAP type, however, the selected EAP method must meet the requirements specified later in this section. A wide number of standards-based EAP implementations are available for use, including EAP-Transport Layer Security (EAP-TLS), EAP-Tunneled Transport Layer Security (EAP-TTLS) and Protected Extensible Authentication Protocol (PEAP).

The EAP authentication framework can readily accommodate a variety of credential types. Despite certain security risks, passwords are currently the most popular form of user credential in public access WLANs. This credential form will continue to see widespread use due to its familiarity and low cost. However, the possibility of using other forms of credentials such as digital certificates or hardware tokens, such as SIM cards used in GSM networks, is gaining popularity. Many cellular operators have extensive charging and billing infrastructures based on SIM authentication. These operators can expand their services to include WLAN access, and can use the same SIM-based credentials that their current customers use for their GPRS service. Other operators could simply issue GPRS or WLAN username/password credentials to their customers and bill them for WLAN use through their cellular account.

The hotspot deployment should be able to support use any EAP method without loss of interoperability, since the choice of credentials is strictly between the user and the user's home operator. The type of credential is transparent to the WLAN operator. We specifically recommend the use of EAP methods that, at a minimum, support the following features:

- Dynamic key derivation for those keys required to protect the air interface
- Mutual authentication.

The cryptographic strength of the EAP method selected should be an issue for the service provider to decide.

Examples of EAP types that meet the above criteria include:

- EAP-TLS
- EAP-TTLS/MSCHAPv2

- PEAPv0/EAP-MSCHAPv2
- PEAPv1/EAP-GTC
- EAP-SIM (Subscriber Identity Module)
- EAP-AKA (Authentication and Key Agreement).

Note: It is required that the visited PWLAN hotspot support WPA and EAP/RADIUS and that all AAA intermediaries also support EAP/RADIUS.

To facilitate seamless Cellular-WLAN interworking, the 2G/3G wireless industry standards development forums (3GPP and 3GPP2) have specified their preferred EAP authentication methods which may include some variations (for example, EAP-TLS with Pre-Shared Key). Additional information can be found in references ([3GPP 33.234] and [3GPP2 X.P0028]).

[1] contains additional information on this topic in sections 3.2.1 and 3.2.3.

5.4. Fast Re-Authentication [20]

As Figure 5 shows, WPA authentication can involve many round-trip messages. In a roaming context, where these round-trips may involve many network hops, this process can be very time consuming. Therefore, there is strong motivation to streamline the re-authentication process, especially if any time-critical applications such as voice connections need to be supported. There are two basic strategies for fast re-authentication:

- Re-authenticate with the home AAA-H but streamline the re-authentication process by taking advantage of state maintained from the prior full authentication. The PEAP and TTLS protocols includes support for faster re-authentication following this strategy. Methods such as EAP-SIM and EAP-AKA also have optimizations to reduce the number of round-trips for re-authentication. However, even in their accelerated modes, these protocols still incur multiple round-trips to the AAA-H to perform re-authentication.
- Avoid communicating with the home AAA-H altogether and re-authenticate only to the local network's infrastructure. Some method for proactive key sharing would be needed in this case to improve inter-AP handoff performance. This strategy is probably the only viable one for time-critical applications. WPA2 (IEEE 802.11i) includes support for PMK caching and pre-authentication.

5.5. Supplicant Disconnection from the Network

When using UAM, the hotspot network must follow the WISPr [2] draft in supporting client-initiated logoff. When using WPA, the client must support client-initiated logoff by implementing a "Disconnect" feature that either disassociates from the AP or sends an 802.1X EAPoL-Logoff message and then disassociates.

In either event, there still exists the possibility that the client may not support proactive client-initiated disconnection. The user's device may also ungracefully terminate the connection in a number of different ways, including going out of range of the hotspot, signal fading due to interference, a power-off event at the client device or unplugging of the WLAN card.

In these situations, the hotspot network will need mechanisms that ensure that the user session is terminated after a reasonably short duration of time, so that the user does not

get billed after loss of the network connection. In the WPA model, an AP must be able to reliably generate a Stop Accounting message when a session is terminated either implicitly or explicitly.

The Idle-Timeout attribute as described in section 7 must be also supported to allow for the correct handling of situations when the user is connected to the network but is not generating any outbound traffic.

5.6. Protection of WPA-Based Authentication [21]

To achieve end-to-end identity protection, a protocol such as PEAP (Protected EAP Protocol, http://www.ietf.org/internet-drafts/draft-josefsson-pppext-eap-tls-eap-07.txt) or TTLS (EAP Tunneled TLS Authentication Protocol, http://www.ietf.org/internet-drafts/draft-ietf-pppext-eap-ttls-03.txt) can be used. Both PEAP and TTLS are authentication tunneling protocols that create a protected channel for other EAP-based authentication methods. Neither of these protocols has achieved RFC status yet. The above references are works-in-progress.

These protocols enable two-phase mutual authentication where the network first authenticates to the client via the digital certificate of the AAA-H, and then the client authenticates to the network using some other EAP method inside a TLS-encrypted channel. The client authentication method need not be based on certificates. This is the same model used by secure data sent to web servers on the Internet.

To avoid revealing the true user identity to untrusted parties, especially across the WLAN radio link or to roaming partners that may also be competitors, the STA can use a generic user name like “anonymous” or “user” in the NAI sent in the initial identity exchange. The realm part of the NAI is the only information the visited network uses at this point. If PEAP or TTLS is used to establish a secure tunnel between the STA and the AAA-H, then the protected identity exchange (generically denoted “GetUserID” in the diagram below) will not be visible to the visited network or to any eavesdroppers. The visited network will eventually need to obtain some identity value for charging and billing purposes if the authentication is successful. The home network can provide the identity that identifies the account for charging. This account identity is used between the visited network and the home network, and need not be the same as that used by the home network to bill the subscriber. Furthermore, this identity can be an alias specified by the home provider rather than information that might compromise the true identity of the STA user. The identity used for charging can be shared only with the AAA infrastructure and never needs to be sent unprotected across the WLAN radio link.

Some EAP methods can provide identity protection without TLS tunneling. For example, EAP-SIM and EAP-AKA support anonymity using temporary identities (called pseudonyms). In this case the AAA-H assigns a temporary pseudonym to the mobile client. The pseudonym is sent in encrypted form to the mobile client during the authentication process and is used instead of the permanent identity at the next authentication. The AAA-H may assign new pseudonyms at subsequent authentications. The permanent user identity will preferably only be used the very first time a mobile client authenticates.

Figure 7 depicts an authentication scenario using PEAP or TTLS with an inner EAP method.

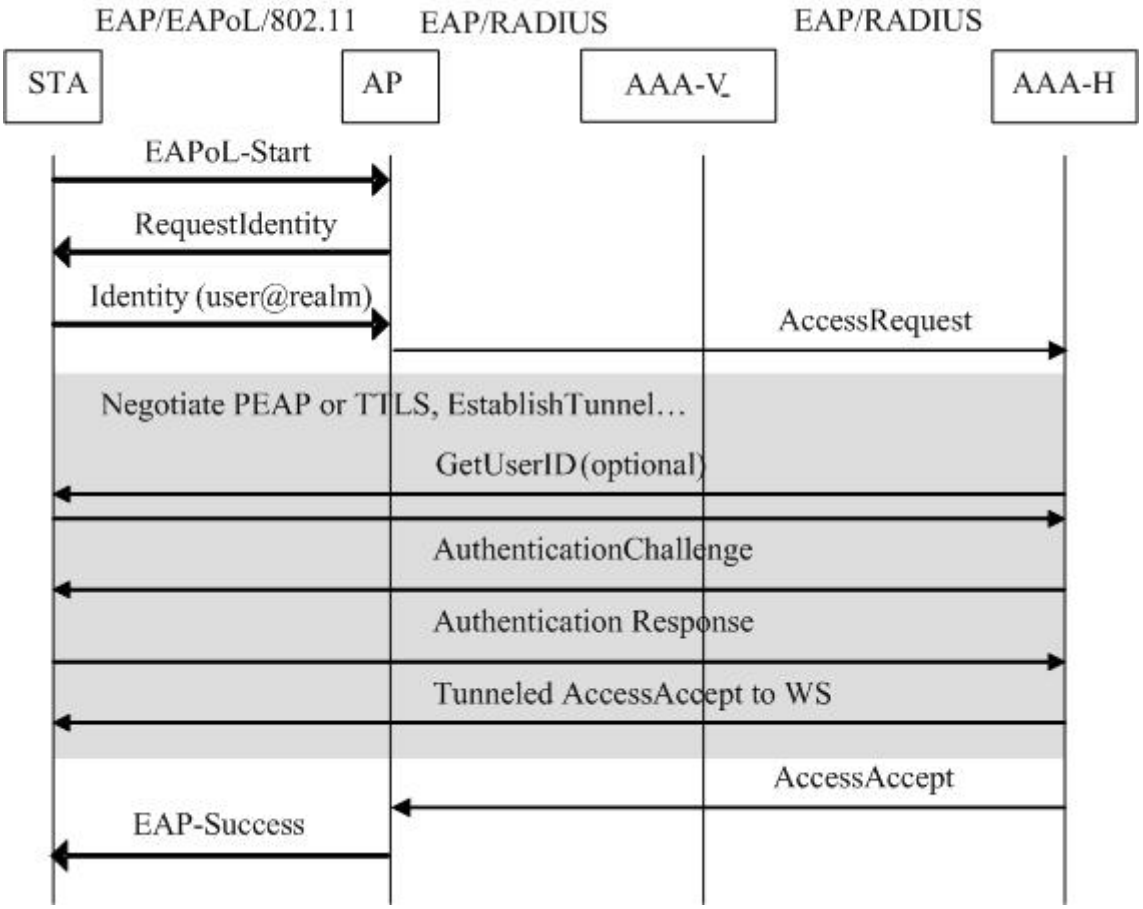

Figure 7: 802.1X with PEAP or TTLS as an example

5.6.1. Early Termination of the TLS Tunnel 22

In some cases, it may be desirable to perform early tunnel termination of the TLS tunnel used by PEAP or TTLS at a trusted intermediary. Early tunnel termination can have performance benefits and may simplify interworking in cases where home provider networks do not yet support PEAP or TTLS. Some geographies with long transport times for the RADIUS messages, the overhead of running PEAP or TTLS end-to-end may cause performance problems during authentication. With early termination, the inner EAP method would still run end-to-end between the STA and the AAA-H (in some cases, the inner method will need to be converted to a non-EAP method for compatibility with the terminating AAA server), and the keys used to protect the WLAN session are derived from a mixture of the PEAP or TTLS session keys and the inner method session keys. Note that inner/outer key binding is part of the solution to the compound authentication binding problem in PEAPv2. It is not available in older PEAP implementations. In the case of TTLS, the use of EAP-MD5-tunnelled as the inner protocol addresses these concerns.

Figure 8 depicts a deployment of WPA with early PEAP or TTLS termination. The PEAP or TTLS server in this case is operated by an AAA intermediary. The STA in this example selects the intermediary by decorating the NAI to indicate the desired intermediary (depicted in the figure as “AAA-I/user@realm”). Once the EAP request arrives at AAA-I, the AAA-I authenticates to the STA based on its digital certificate. The STA must therefore be configured to trust the key of the certificate authority that issued

the certificate to the AAA-I. This configuration is the responsibility of the home provider of the STA's account. Once the PEAP or TTLS tunnel is established, the AAA-I prompts the STA for its identity.

The most significant differences between PEAP and TTLS are that in the case of PEAP, the inner protocol must be an EAP method, where as with TTLS, the inner protocol can be any existing protocol, even legacy RADIUS methods of PAP and CHAP. When early tunnel termination is used at an AAA-I as a service to an AAA-H that is a legacy RADIUS server, protocol conversion must be provided if the inner authentication method is an EAP protocol. Service providers may find it more convenient to use TTLS as it is possible to use an inner protocol that does not need protocol conversion. This simplicity will make scaling easier to manage.

If the transport delay between the AP and the AAA-I is substantially less than the connection between AAA-I and AAA-H, significant performance benefits can be achieved through early termination. However, with early termination, the inner method is run without the protection of a TLS channel between AAA-I and AAA-H. If PEAP or TTLS runs end-to-end, the STA need only trust the AAA-H server. With early termination, the STA will continue to trust just the home provider and will expect to see the AAA-H certificate. The AAA-H must authorize the AAA-I to provide the early termination service by providing the AAA-I with a certificate representing the home provider. This transfer of a certificate from the home provider to the intermediary represents a new trust relationship between AAA-H and AAA-I.

If early termination of PEAP or TTLS is used, the trusted intermediary (AAA-I) must appropriately protect the inner authentication protocol from attack between the AAA-I and AAA-H. Strong methods such as EAP-AKA should be secure from attack without additional protection. However, weaker methods require additional downstream protection. For example, if PAP is the inner authentication method, then this opens up a known plaintext attack on the key stream. Similarly, methods such as MSCHAPv2 become susceptible to dictionary attack if sent in the clear. All these vulnerabilities are addressed by use of RADIUS over IPSec as specified in RFC 3579, section 4.

The choice of inner authentication method can strongly affect the realized benefits of early TLS tunnel termination. If transport delay is an issue, the use of a non-EAP protocol will maximize the performance gain from early TLS tunnel termination.

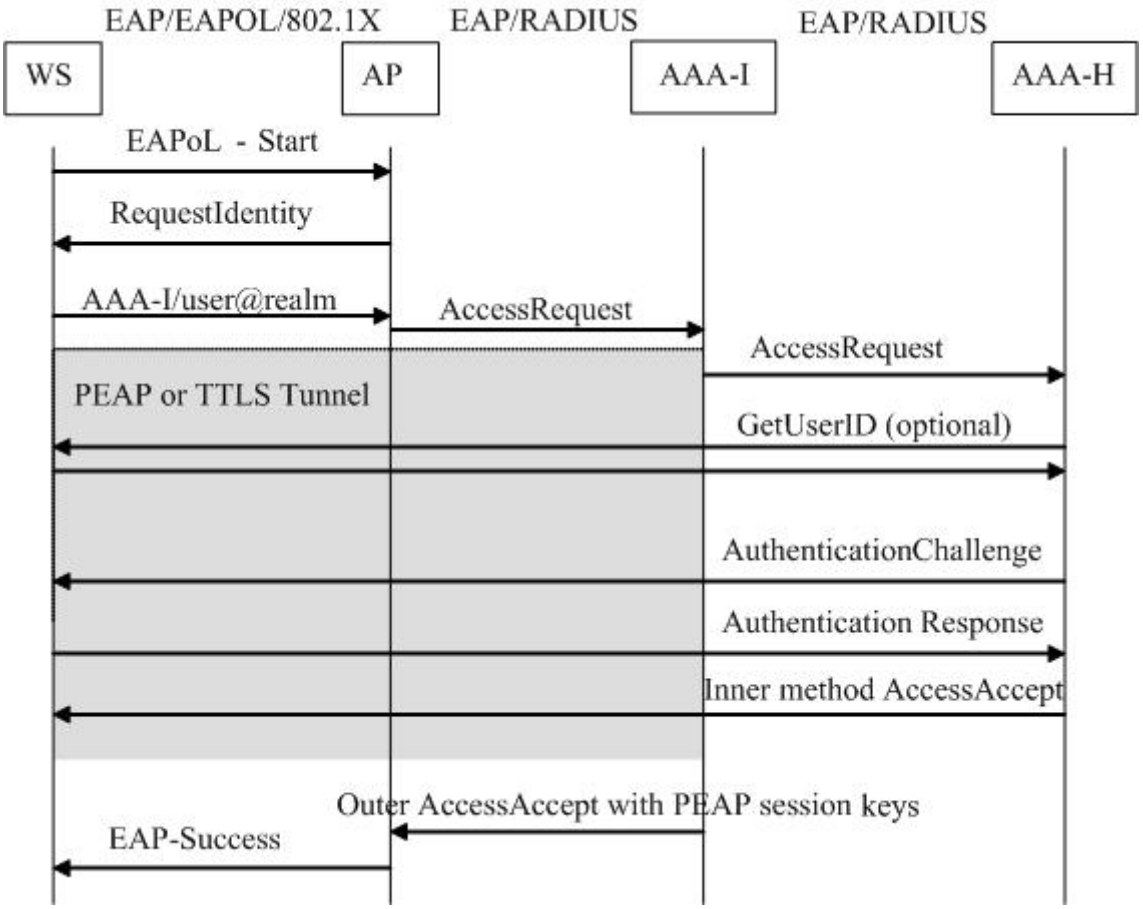

Figure 8: WPA with Early PEAP or TTLS termination

Note: Strong inner methods such as EAP-AKA that do mutual authentication and session key derivation should not be used in conjunction with older PEAP implementations that do not support the key binding feature (for example, the version of PEAP supported by Windows® XP with service pack 1). This is because using older versions of PEAP with those methods introduces new man-in-the-middle attack vulnerabilities.

In general, early PEAP or TTLS termination may be beneficial in the following circumstances:

- long transport times preclude end-to-end PEAP or TTLS with the home provider
- adequate protection of the inner EAP method is provided between the trusted intermediary and the AAA-H
- the session key binding feature of the PEAPv2 or TTLS is supported by both the client and the PEAP or TTLS server.

5.6.2. The Use of Inner and Outer EAP and RADIUS Identities[23]

When WPA-based authentication is deployed with RADIUS, the identity of the STA client is not a simple, singular value. Instead, multiple identifiers are used in different contexts for different purposes, which can be confusing. The following list describes these identity values and where they are used.

- **Initial (outer) NAI**. The initial Network Access Identifier (Identity, in Figure 7) is a value provided by the STA client in its EAP-Identity-Response message. This NAI is sent in the clear across the WLAN radio link (it is not a private value).
- **Subsequent (outer) NAI**. If for some reason there is difficulty in processing the initial NAI, the EAP base protocol allows for additional Identity-Request messages to obtain an alternative NAI from the supplicant. This NAI is logically and functionally equivalent to the initial outer NAI.
- **RADIUS User-Name attribute**. With outbound authentication request messages, the User-Name RADIUS attribute is initialized by copying the value of the NAI returned in the EAP Identity-Response. The User-Name attribute is processed by the hotspot operator and intermediate AAA proxies to route the authentication request to the home provider AAA server. In some cases, a AAA proxy may remove "decoration" from the User-Name attribute if the decoration corresponds to its own domain. Although the RADIUS User-Name may be modified in transit to remove decorations, the NAI in the EAP Identity payload must be delivered unmodified to the AAA-H.
- **Inner EAP method identity**. Once the end-to-end EAP conversation is established with a home provider's EAP server, the EAP method may include a separate identity exchange. This inner identity could be completely different from the outer NAI and RADIUS User-Name attribute. For example, it is recommended that the inner EAP identity not include any decoration indicating roaming intermediaries. If the inner EAP method uses a separate identity exchange inside an encrypted channel, user anonymity can be provided.
- **Billable identity**. Please see section 7.2 for a discussion on user identities in connection with accounting.

5.7. Key Distribution [24]

Figure 5 shows that session keys are distributed from the AAA-H to the AP as part of WPA authentication. The security of this key distribution channel is a critical part of the overall security of provided by WPA. In a roaming context, the STA user typically has no prior relationship with the operator of the AP. The only basis by which the user can have confidence that he is communicating with a legitimate network operator is that the WPA session keys negotiated with the home AAA-H are subsequently known by the AP through which they are communicating. These keys are distributed on a hop-by-hop basis using encrypted RADIUS attributes from AAA-H via zero or more AAA-I to AAA-V and finally to the AP. For additional security, network-layer security such as IPsec can be used to protect the RADIUS traffic. This is commonly done for RADIUS connections that traverse an open network such as the Internet.

From a security protocol standpoint, it is problematic for session keying material to be visible to intermediaries. The security of the entire system is only as strong as the weakest component in this chain. However, no viable alternative to this model has been standardized at this time. For more information on key distribution for WPA, please refer to RFC 3580 and the EAP keying draft in the IETF.

6. Authorization

6.1. Service Authorization

The basic service authorized for an authenticated user is Internet access. Access to this service is implicitly granted by the local service provider once the user is authenticated by the home service provider.

There is no standard way for the home service provider to indicate any advanced types of access, or access restrictions, as the case may be. No standard attributes have been defined as yet that can describe a service consistently across different hotspot hardware deployments. As a result, a successful authentication in most cases results in an implicit authorization of basic internet access. There is currently work in progress in the RADEXT group in the IETF to tackle this issue.

Finer-grained services may be offered for subscriber access within the home service provider's own network; this can be accomplished by defining a set of attributes that may be understood within the service provider's AAA infrastructure. If this method is used, it is recommended that the user be educated about the possibility of seeing different levels of service when roaming between the home service provider's network and other partner networks. These services may be offered from a visited network operator on a bilateral basis between home and visited networks.

Subscribers are usually authorized for different services based on the user identity presented to the network. Other criteria may include time-of-day, capability of the requesting device and so on. When a tunneled method such as PEAP or TTLS is used, the outer user identity may be anonymous; care must be taken to ensure that the inner identity is used for service authorization.

6.2. Fast-Handoff and Service Authorization [25]

Within the EAP framework, "fast-handoff" is defined as a conversation in which the EAP exchange and associated AAA pass-through is bypassed, so as to reduce latency. Depending on the fast-handoff mechanism, AAA-Key transport may also be bypassed or it may be provided in a pre-emptive manner. Bypassing all or portions of the AAA conversation creates challenges in ensuring that the authorization is properly handled. Please see the associated endnote for a detailed discussion on this topic.

6.3. Use of Session Timeout in RADIUS Authorization Message

In order for the Home Provider to control the maximum amount of time his end-user can be authorized for access at a visited hotspot and to support prepaid subscription model, the RADIUS attribute Session-Timeout can be used as part of the RADIUS Authorization. As described in RFC 2865, this attribute specifies the maximum number of seconds of service to be provided to the end-user before some action would be taken. If the client remains connected until the timeout expires, the access network either automatically disconnects that client or requests for a re-authentication, depending on the value of the Termination-Action attribute. If browser hijack authentication is used, expiration of the prepaid time typically results in the user being blocked from Internet access and redirected to the network login page. If the Termination-Action attribute requires client disconnection, an appropriate RADIUS Accounting Stop message must be generated, and the user would be forced to re-login to gain access.

According to RFC 2865, the RADIUS Session-Timeout attribute can also be used to trigger 802.1X re-authentication. In this case, expiration of the timeout does not automatically result in disconnection, but it forces the client to re-authenticate using 802.1X. The service provider can use the 802.1X authentication to control extension of the user's session by granting or denying the re-authentication request. For further information RADIUS timeout attribute semantics and RADIUS-based prepaid support, please refer to RFC 2865, RFC 3580, and the work underway in the RADEXT task group in the IETF.

Extensions to RADIUS protocol, as described in the informational RFC 3576 (Dynamic Authorization Extensions to RADIUS), when supported by the visited network, allows the home provider to make dynamic changes to their user's sessions such as disconnecting the session prior to the Session-Timeout by sending a "Disconnect Message" or changing authorizations applicable to a user session by sending a "Change of Authorization (CoA) message." The Security Considerations (including Authorization Issues, Impersonation, IPSEC Usage Guidelines and Replay Protection) as described in RFC 3576 should be considered when deploying support for these RADIUS Extensions.

The Idle-Timeout attribute (or inactivity timeout) is an important complement to the Session Timeout attribute. This attribute is described in detail in section 7.5.

7. Accounting

7.1. Accounting Attributes

In order to allow a home provider to support different billing models in a roaming scenario, the visited network must provide the accounting data that is needed by the home provider. The Wi-Fi Alliance has defined a list of recommended RADIUS attributes that APs and Access Controllers to be used in public access environments should support. This attribute list may be found in Appendix A of the Public Access Market Requirements Document.

Some attributes require further consideration as described in the following subsections.

7.2. Use of a Billable Identity Attribute

In a roaming scenario, the visited network, the home provider and any roaming intermediaries may all collect and store accounting data. This could for example be done in the AAA-V, INT and AAA-H as described in Section 1. In order to do clearing and settlement of the accounting records between these entities, each entity needs to be able to uniquely identify the billable session.

The RADIUS User-name attribute is always included in accounting messages. In some cases, this value is sufficient as a basis for generating billing data because it corresponds to a specific billable account. However, if the billable identity cannot be derived from the NAI, if it is a temporary identity, or if the outer NAI given by the STA is anonymous, some other means must be used to associate charging records with a billable account. In this case, the home provider must communicate a billable identity back to the visited WLAN to be included in accounting records generated for the session. Unfortunately there is not a single standardized solution for this today as yet, though the RADEXT working group in the IETF is actively pursuing a solution. Different alternatives exist:

- According to RFC 2865, if the AAA server includes a User-name attribute in an Access-Accept message, subsequent accounting records SHOULD use this value rather than the original User-name. This method, called User-name re-write, is one possible mechanism for indicating the billable identity, but it is not recommended, as it has its own set of problems, including causing the Accounting messages to be incorrectly routed due to the rewrite.
- User-name attribute may be augmented with some other attribute(s) in the Access-Accept. This attribute will then be included in all RADIUS Accounting-Requests for that session. The IETF RADEXT group is currently working on standardizing a new attribute used for the billable identity. This approach is the one most free from side effects and compatibility problems with existing systems. This is the method recommended. As an interim solution, the GSM Association has specified a Chargeable-user-Id (CUI) VSA for this purpose. The use of an extra attribute for billable identity is intended to augment, not replace, use of the User-name attribute in the accounting records. The User-name attribute must be included in the accounting records, even if it refers to an anonymous or temporary identity in the home realm. The User-name attribute, in this case, will be used to maintain appropriate routing of the Accounting messages.

Depending on how the billable identity is used, it may impact user anonymity. In the solutions described above, the billable identity is sent to intermediate proxies and to the visited network, but it is not sent over the WLAN air link. To fully preserve anonymity, the permanent user identity should not be sent to the intermediaries or the visited network. To prevent the real user id from reaching the intermediary and visited networks, the billable identity could be any identifier (e.g. a number) that uniquely identifies the billable session but does not reveal the permanent user id. Whether or not a home provider is willing to disclose permanent user identities to other networks is of course dependent on the roaming agreement and the level of trust between the home, visited and intermediary networks.

7.3. Binding Session Accounting Information to Session Authorization Info

Accounting data can be used for many purposes. In a general sense, accounting is used to keep track of a user's activities and resource consumption while accessing the network. Billing of the customer is maybe the most obvious purpose of accounting data, but other uses include fraud detection, auditing, statistics, trend analysis and capacity planning.

Unless a parameter is introduced that binds the authentication data to the accounting data, the two message exchanges are in principle independent and difficult to correlate when stored in, for example, log files. In order to better track user activity for, say, fraud detection, the authentication and authorization information for a session should be correlated with the accounting data generated for that session. The Class attribute, which is sent by the home provider in the Access-Accept and returned by the visited network in all Accounting-Requests, can be used for this purpose. To correlate individual authentication and accounting sessions, a separate correlator needs to be used for each session. Support in the AP for returning the Class attribute is required.

7.4. Use of the Class Attribute

The Class attribute is sent back by the authenticating AAA server (AAA-H) to the originating NAS in the Authentication Response, and is an opaque identifier. The home service provider may use this attribute as it sees fit—one possible use could be to correlate the authentication and authorization information for a session with the accounting data generated for that session.

The AAA-H may send back more than one Class attribute in the Authentication Response message. The NAS MUST include all instances of the Class attribute in any Accounting messages it generates, so that the AAA-H has the opportunity to do the necessary correlation.

7.5. Use of the Idle-Timeout Attribute

There are two common uses for the Idle-Timeout attribute, or inactivity timeout.

(1) Home providers offering unmeasured service (e.g. unlimited subscriptions) could elect to use the inactivity timeout to disconnect inactive roaming users since the home provider may be paying the visited network on a measured wholesale rate.

(2) Home providers may elect to use the inactivity timer to protect users from forgetting to logoff and inadvertently depleting their account. This allows for a fail-safe mechanism to be built into the billing process, so that a client who is logged on to the network but is not actively using it does not accrue unnecessary

billing charges. This mechanism cannot perfectly divine the user's intent (i.e. they really wanted to be continuously connected to wait for incoming messages), so care must be used in determining whether a mechanism for exceptions is also needed.

The definition of the "idle" state can be interpreted in different ways. We have observed that it is in the user's and service provider's best interests to define it as a state when there is no outbound data traffic from the client station. This implies that if a client is logged on to the network but has not generated outbound IP data traffic (other than NETBIOS) for a specific interval of time, and if the AAA server has specified this interval of time via the Idle-Timeout attribute, the NAS must proactively disconnect the client and generate an Accounting-Stop message.

7.6. Use of the Framed-IP-Address Attribute

In 802.1X mode, the AP sends out an Accounting-Start message as soon as authentication completes (when it receives an Access-Accept from the AAA server). At this point, the client does not yet possess an IP address, since the virtual port on the AP has not yet been opened to allow DHCP or other IP traffic. The AP therefore cannot include the Framed-IP-Address attribute (which contains the IP address of the client) in the Accounting-Start. This attribute is required for the generation of TAP 3.10 records.

There are two approaches to solving this problem within the AP, without requiring additional support from an AC;

(1) The AP opens the virtual port after authentication successfully completes and waits until the client receives an IP address. Once it knows this IP address, it generates the Accounting-Start message with the Framed-IP-Address attribute.

(2) The AP generates the Accounting-Start message as before, as soon as authentication successfully completes. Once DHCP completes soon after and the client receives an IP address, the AP can use this IP address in subsequent Accounting-Interim and Accounting-Stop messages. Since the settlement process relies mainly on Accounting-Interim and Accounting-Stop messages rather than the Accounting-Start, the generation of the Start message without this attribute is acceptable as long as it is present in the Interim and Stop messages.

Option 2 is preferred, since it requires minimal change to the AP implementation.

Alternate implementations use the AC to generate accounting messages with the Framed-IP-Address attribute. If this is followed, the session ID used in the accounting messages generated individually by the AP and the AC must be the same, for the separate messages to be correlated back to the same session. If not, the accounting messages from the AP must not be forwarded beyond the AC. This approach is not recommended, as it requires additional coordination between the AP and the AC.

7.7. Use of RADIUS Interim Accounting Messages

The RADIUS interim accounting message protects the home network from loss of a RADIUS start session or stop session accounting message. While it is unlikely that RADIUS messages are lost over the communications link (due to the use of message retransmission and acknowledgements in the RADIUS protocol) it is possible for messages to be lost due by to failures at an AAA-H or AAA-I.

The availability of an accounting message ensures that at least part of a session is billable if the RADIUS stop session message is lost. The interim accounting message is also important to home networks that offer prepaid service. The messages allow the home network to incrementally charge an account for a session.

It is recommended that APs and ACs be configured for sending interim messages every five minutes.

8. Looking Forward

By creating a consistent deployment model for the coexistence of legacy browser-based (UAM) and WPA hotspot login, the Wi-Fi Alliance seeks to accelerate the acceptance of public access Wi-Fi services.

This paper describes three principal options to consider for the deployment of a coexistent UAM and WPA PWLAN hotspot. This paper has also highlighted various architectural considerations and recommendations to take into account when planning to deploy an WPA-based hotspot network. Following these recommendations will increase the ability for different network deployments to effectively communicate with each other, increasing the ease of roaming between different PWLAN hotspots.

This paper also highlights some open topics that are still under development in their respective standards bodies. These include:

- Defining the data interface between client software and access points/access controllers (Wi-Fi Alliance, Public Access Marketing TG)
- Mediating network discovery and selection, RADIUS attribute extensions (IETF, RADEXT WG)
- Public Access certification for Wi-Fi access points (Wi-Fi Alliance, Public Access Technical TG)
- Additional RADIUS attributes (IETF, GeoPriv and RADEXT WGs)
- Cellular to Wi-Fi Roaming (GSMA WLAN TG, Wi-Fi Alliance Cellular Convergence TG, 3GPP/3GPP2).

This work should be followed in these standards bodies and forums, and the final results adopted.

The WFA has more recently begun interoperability tests of WPA2, which includes more robust encryption based on AES (Advanced Encryption Standard). Because of the expense associated with WPA2 upgrades, it is expected to occur gradually over time. This should not be a problem, since WPA2 will be backward compatible with WPA. Newer APs and network cards will support the new standard and will also support legacy compatibility modes.

While the market for public access Wi-Fi continues to develop, the Wi-Fi Alliance will stay ahead of the curve in providing leadership through whitepapers such as this one and certifications that provide the same guarantee of compatibility in Wi-Fi public access infrastructure and roaming as the original Wi-Fi mark did for access points and network cards.

9. Glossary of Terms

Term	Definition
3GPP	Third-Generation Partnership Project, a cellular industry standards group for next-generation GSM networks
3GPP2	The Third Generation Partnership Project 2 (3GPP2) is a collaborative third generation (3G) telecommunications specifications-setting project comprising North American and Asian interests, developing global specifications for ANSI/TIA/EIA-41 Cellular Radiotelecommunication Intersystem Operations network evolution to 3G and global specifications for the radio transmission technologies (RTTs) supported by ANSI/TIA/EIA-41. (www.3gpp2.org)
802.11	WLAN network standard defined by the IEEE standards group
802.11e	Proposed IEEE standard that will define QoS mechanisms for 802.11
802.11i	Proposed IEEE standard for improved security for 802.11
802.1X	Port-based network access control, an authentication framework for fixed and wireless networks, including WLAN
802.3	IEEE standard specification for Ethernet
AAA	Authentication, Authorization and Accounting
AAA Proxy	An intermediary for transparently routing and/or processing AAA messages sent between an AAA client and an AAA server. Multiple AAA proxies can be chained together.
AAA Server	Computer system performing AAA services (authentication, authorization, accounting)
AAA-H	Home provider AAA server
AAA-V	AAA proxy server located within the visited network
AAA-I_r	Roaming Intermediary AAA server
AC	Access Controller
AES	Advanced Encryption Standard defined by U.S. National Institute of Standards and Technology
AP	Access point, the 802.11 wireless transceiver providing connectivity to a wired network

BSS-H	Home provider Business Support System
BSSID	Basic Service Set Identification for 802.11
CA	Certificate Authority
CDMA	Code-Division Multiple Access
CIBER	Cellular Intercarrier Billing and Exchange Roaming Record
DCH	Data Clearinghouse, an intermediary that performs charging and billing services on behalf of network operators and home providers
DHCP	Dynamic Host Configuration Protocol
Diameter	2nd generation AAA protocol (RFC 3588), offering backwards compatibility with RADIUS
DNS	Domain Name System
DMZ	Demilitarized Zone, a neutral area between the enterprise intranet and the public Internet
DSL	Digital Subscriber Line for high speed data services over ordinary phone lines
EAP	Extensible Authentication Protocol
EAP-AKA	EAP Authentication and Key Agreement to be used with USIM
EAP-GTC	EAP Generic Token Card
EAP-MD5	EAP Message Digest 5
EAP-OTP	EAP One Time Password
EAP-SIM	EAP method for SIM card-based authentication
EAPoL	EAP Over LAN
EAP-MSCHAPv2	Microsoft® Challenge Handshake Authentication Protocol version 2
EAP-TLS	EAP with TLS
GTC	Generic Token Card
GPRS	General Packet Radio Services
GMM	GPRS Mobility Management
GSM	Global System for Mobile communication
HLR	Home Location Register (subscriber database for cellular carriers)
Home provider	Provider with direct billing relationship with network service subscribers

Hotspot	Public location such as an airport or hotel where WLAN services have been deployed
HSS	Home Subscriber Server
IDA	Infocomm Development Authority of Singapore
IE	Information Element
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
INT	Roaming Intermediary
IP	Internet Protocol
IPDR	Internet Protocol Detail Record
IPsec	A network-layer security standard providing data privacy, integrity and replay protection.
IPv4	Internet Protocol version 4
IPv6	Internet Protocol version 6
LEAP	Lightweight Extensible Authentication Protocol
MAC	Media Access Control
MAP	GSM Mobile Application Part (protocol for enabling call routing and subscriber database lookup for cellular carriers)
MIC	Message Integrity Check
NAI	Network Access Identifier (in the form username@realm)
NAT	Network Address Translation
NAT Traversal	Protocol that specifies how to tunnel MIP packets over UDP
OTA	Over The Air
PANA	Protocol for carrying Authentication for Network Access
PEAP	Protected EAP - An EAP access method using TLS tunneling and defined by RFC draft http://www.ietf.org/internet-drafts/draft-josefsson-pppext-eap-tls-eap-07.txt. This protocol is similar to EAP-TTLS.
PWLAN	Public WLAN
QoS	Quality of Service
RADIUS	Remote Access Dial In User Service, a network protocol for AAA services

SIM	Subscriber Identity Module. Smart cards used by GSM operators, used with EAP-SIM
SSID	Service Set Identifier for 802.11 access points. The SSID is a 32-character unique identifier of the WLAN network included in packet headers.
SSL	Secure Sockets Layer, a popular protocol for authentication and connection-level privacy and message integrity, often used for securing web pages
TAP	Transferred Account Procedure
TCP	Transmission Control Protocol
TEM	Telecom Equipment Manufacturer
TGi	IEEE 802.11 Task Group I
TKIP	Temporal Key Integrity Protocol, an improved WLAN security mechanism designed to fix known problems in WEP
TLS	Transport Layer Security, a variant of SSL
TTLS	A EAP access method using TLS tunneling and defined by RFC draft http://www.ietf.org/internet-drafts/draft-ietf-pppext-eap-ttls-03.txt. This protocol is similar to PEAP.
UAM	Universal Access Method, name of hotspot access method with Access Controllers using browser hijack
UDP	User Datagram Protocol
USIM	Universal Subscriber Identity Module, smart cards used by UMTS operators, used with EAP-AKA
Visited network	WLAN operator whose network is visited by roaming users of a different home provider
VLAN	Virtual LAN
VoIP	Voice over IP
VoWLAN	Voice over WLAN
VPN	Virtual Private Network
WCDMA	Wideband Code-Division Multiple Access
WEP	Wired Equivalent Privacy, the initial (fatally flawed) security solution for the 802.11 link-layer

Wi-Fi	Wireless Fidelity, refers to 802.11 standards, including 802.11b, 802.11a, and 802.11g
Wi-Fi Alliance	Industry association promoting IEEE 802.11 standards
WISP	Wireless Internet Service Provider
WLAN	Wireless local area network based on IEEE 802.11 and related standards
WPA	Wi-Fi Protected Access, a subset of the 802.11i security standard compatible with existing WLAN hardware. WPA includes per-packet Message Integrity Check (MIC), per-user dynamic WEP keys (TKIP), and 802.1X authentication.
WPA2	The planned name for Wi-Fi Alliance certified implementation of 802.11i
WWAN	Wireless Wide Area Network
X.509	ITU standard for digital public-key certificate issued by a CA

10. References

1. Interworking Study, Draft Revision 0.8, January 12, 2004 http://www.intel.com/technology/IWS.
2. Best Current Practices for Wireless Internet Service Provider (WISP) Roaming, Feb 2003.
3. Architecture Taxonomy for Control and Provisioning of Wireless Access Points (CAPWAP), April 16, 2004, work-in-progress, http://www.ietf.org/internet-drafts/draft-ietf-capwap-arch-02.txt.
4. EAP-SIM based WLAN Roaming Guidelines, GSM Association, work-in-progress.
5. [3GPP 22.234] 3GPP TS 22.234: Requirements on 3GPP system to Wireless Local Area Network (WLAN) interworking (Release 6).
6. [3GPP 23.234] 3GPP TS 23.234: 3GPP system to Wireless Local Area Network (WLAN) Interworking; System Description (Release 6).
7. [3GPP 33.234] 3GPP TS 33.234: Wireless Local Area Network (WLAN) interworking security (Release 6).
8. [3GPP2 X.P0028-0] 3GPP2 X.P0028-0: “WLAN Interworking”.
9. [3GPP2 S.R0087] 3GPP2 S.R0087-0: 3GPP2-WLAN Interworking Stage-1 Requirements.

11. Endnotes

[1] Intel Interworking Study (IWS) Draft Revision 0.8, January 2004, section 2.1

[2] Intel Interworking Study (IWS) Draft Revision 0.8, January 2004, section 2.2

[3] Intel Interworking Study (IWS) Draft Revision 0.8, January 2004, section 2.2.1

[4] Intel Interworking Study (IWS) Draft Revision 0.8, January 2004, section 2.2.2

[5] Intel Interworking Study (IWS) Draft Revision 0.8, January 2004, section 2.2.3

[6] Intel Interworking Study (IWS) Draft Revision 0.8, January 2004, section 2.2.4

[7] Intel Interworking Study (IWS) Draft Revision 0.8, January 2004, section 2.2.5

[8] Intel Interworking Study (IWS) Draft Revision 0.8, January 2004, section 2.2.6

[9] Intel Interworking Study (IWS) Draft Revision 0.8, January 2004, section 2.2.7

[10] "Wi-Fi Protected Access Overview [Wi-Fi_Protected_Access_Overview.pdf]", Wi-Fi Alliance, 2004

[11] Wireless Glossary - http://www.devx.com/wireless/Door/11455

[12] Lisa Phifer, Core Competence, Inc. ISP Planet Article *"Better than WEP",* http://www.isp-planet.com/fixed_wireless/technology/2002/better_than_wep.html

[13] The Tore-Alexander Coexistence Deployment: Alexander Latour, Service Factory & Tore Bjorklund, Telia Sonera AD – Wi-Fi Alliance Public Access Phase III, Hawaii Members Meeting.

[14] Interworking Study (IWS) Draft Revision 0.8, January 2004, section 3.2.2

[15] Interworking Study (IWS) Draft Revision 0.8, January 2004, section 3.2.5

[16] Interworking Study (IWS) Draft Revision 0.8, January 2004, section 3.3

[17] Interworking Study (IWS) Draft Revision 0.8, January 2004, section 3.1

[18] Interworking Study (IWS) Draft Revision 0.8, January 2004, section 3.1.1

[19] Interworking Study (IWS) Draft Revision 0.8, January 2004, section 3.2.1

[20] Interworking Study (IWS) Draft Revision 0.8, January 2004, section 3.2.6

[21] Interworking Study (IWS) Draft Revision 0.8, January 2004, section 3.2.5

[22] Interworking Study (IWS) Draft Revision 0.8, January 2004, section 3.2.7

[23] Interworking Study (IWS) Draft Revision 0.8, January 2004, section 3.2.8

[24] Interworking Study (IWS) Draft Revision 0.8, January 2004, section 3.2.9

[25] http://www.drizzle.com/~aboba/EAP/draft-ietf-eap-keying-02_c.txt, section 2.5