Wi-Fi Alliance – Wireless ISP Roaming (WISPr)
Release Date: February 2003
Version: 1.0

B. Anton – Gemtek Systems, Inc.
B. Bullock – iPass, Inc.
J. Short – Nomadix, Inc.

Best Current Practices for Wireless Internet Service Provider (WISP) Roaming

Purpose and Scope of this Document

This document specifies recommended Best Current Practices for Wi-Fi based Wireless Internet Service Provider (WISP) roaming. This document does not specify a standard of any kind, but does rely on the operational application of standards-based protocols and methodologies. It is beyond the scope of WISPr to develop, monitor or enforce minimum criteria for WISP roaming. Parties to the roaming process are therefore encouraged to follow the recommendations of the WISPr guidelines, but are barred from branding their roaming products and services as Wi-Fi Alliance or WISPr compliant. Definition and adoption of various business models and commercial relationships for WISP roaming are at the discretion of individual companies. Specifically, the retail delivery of roaming service to subscribers, including services definition and charging principles, roaming tariff plans, billing methods, settlement issues and currency matters, are outside the scope of WISPr.

Abstract

WISPr was chartered by the Wi-Fi Alliance to describe the recommended operational practices, technical architecture, and Authentication, Authorization, and Accounting (AAA) framework needed to enable subscriber roaming among Wi-Fi based Wireless Internet Service Providers (WISPs). This roaming framework allows using Wi-Fi compliant devices to roam into Wi-Fi enabled hotspots for public access and services. User can be authenticated and billed (if appropriate) for service by their Home Entity (such as another service provider or corporation).

In order to facilitate compatibility with the widest possible range of legacy Wi-Fi products, it is recommended that WISPs or Hotspot Operators adopt a browser-based Universal Access Method (UAM) for Public Access Networks. The UAM allows a subscriber to access WISP services with only a Wi-Fi network interface and Internet browser on the user's device.

RADIUS is the recommended backend AAA protocol to support the access, authentication, and accounting requirements of WISP roaming. This document describes a minimum set of RADIUS attributes needed to support basic services, fault isolation, and session/transaction accounting.

Intellectual Property Disclaimer

Table of Contents

Table of Figures

1. Introduction

Since the adoption of the IEEE 802.11b standard in 1999, an increasing number of vendors have used this standard in producing Wi-Fi compliant wireless LAN (WLAN) products. Pioneers of high speed Internet access have built WLAN hotspots (zones of public access). Since it is difficult for a single service provider to build an infrastructure that offers global access to its subscribers, roaming between service providers is essential for delivering global access to customers. Roaming allows enterprises and service providers to enhance their employee connectivity and service offerings by expanding their footprint to include network access at Wi-Fi enabled hot spots.

WISPr was formed by the Wi-Fi Alliance to create recommendations that facilitate inter-network and inter-operator roaming with Wi-Fi based access equipment. The dialup Internet roaming protocol selection criteria in [RFC2477], addresses the requirements for a roaming standard but does not address the distinct differences in access methods and protocol support for Wi-Fi based networks that can utilize existing protocols. This document presents the recommended best current practices for enabling WISP roaming.

The figure below graphically depicts a generic model for WISP roaming, including necessary functions and participants.

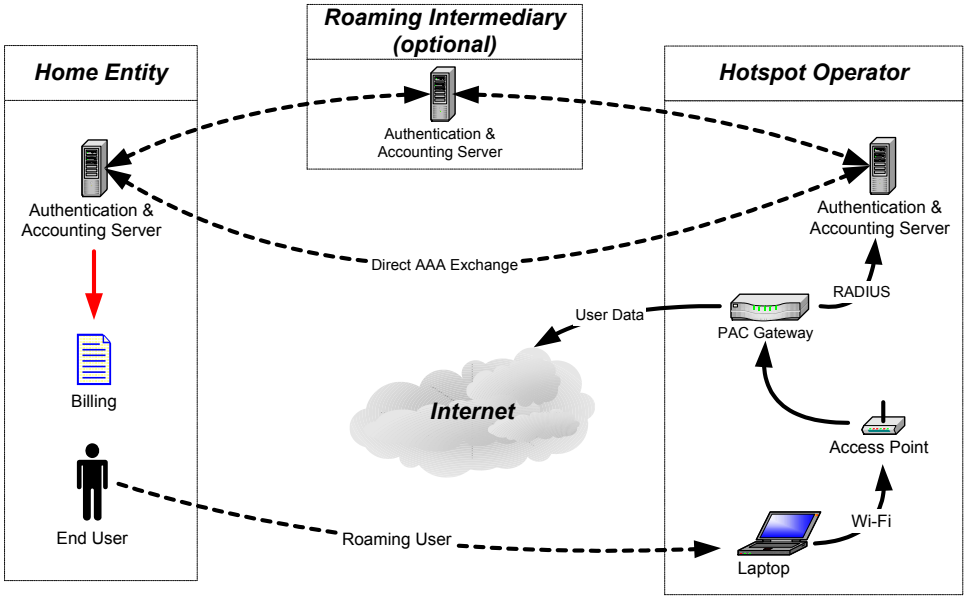


Figure A: WISP Roaming Overview

The participants, and all intermediaries that sit in the AAA flow, must support the recommended AAA attributes. The functional objects/players in the WISP roaming model include:

- Hotspot Operator – Operator of Wi-Fi network for public Internet access at hotspots.
- Home Entity –Entity that owns account relationship with the user. The Home Entity must authenticate their user to obtain roaming access at the hotspot. Examples of home entities include WISPs, other service providers, and corporations.
- Roaming Intermediary - An optional intermediary that may facilitate AAA and financial settlement between one or more WISPs and Home Entities. Examples of AAA intermediaries include Brokers and Clearinghouses.

Parties that do not directly participate in the AAA framework nor have to directly support the AAA attributes of the Roaming Model:

- User - Uses Wi-Fi Roaming at hotspots and has a billing relationship with the Home Entity.
- Content Provider - Content providers provide content and applications to the users of the service. The content provider and the Home Entity have a commercial relationship where the content provider takes

responsibility to make content accessible to the authorized users, and the Home Entity guarantees the commercial terms (i.e., payment).

- Hotspot Property Owner - The hotspot property owner typically controls the density of potential users/customers and provides the Hotspot Operator space for equipment and consumers using the service. If the hotspot property owner is not a Hotspot Operator, it does not participate in the data exchange required to support authentication and accounting for roaming users.

1.1. Terminology

~ AAA ~
Authentication, Authorization and Accounting. A method for transmitting roaming access requests in the form of user credentials (typically user@domain and password), service authorization, and session accounting details between devices and networks in a real-time manner.

~Clearinghouse~
A clearinghouse is a third party that facilitates exchange of authentication and accounting messages between WISPs and home entities, and provides auditable data for settlement of roaming payments. Unlike a broker, clearinghouses do not buy airtime minutes from WISPs for resale, instead providing a trusted intermediary function for implementing roaming agreements made directly between WISPs and home entities. Clearinghouses are typically compensated on a transaction basis for clearing and settlement services.

~ EAP ~
Extensible Authentication Protocol. A general authentication protocol used by Local and Metropolitan Area Networks that supports various specific authentication mechanisms. EAP is defined in [RFC2284] and used by the IEEE 802.1x Port Based Access Control protocol [8021x].

~ Home Entity ~
The entity with which the end-user has an authentication and/or billing relationship. The Home Entity need not be a network provider, but must support the RADIUS functionality required to authenticate and account for usage of their clients that roam. The Home Entity may also be a Hotspot Operator, a service provider that hasn't deployed Wi-Fi access hotspots, an enterprise network, or an independent business entity that the end-user has an account relationship with.

~ Hotspot ~
A location that provides Wi-Fi public network access to Wi-Fi enabled consumers. Examples of hotspots include hotel lobbies, coffee shops, and airports.

~ Hotspot Operator ~
An entity that operates a facility consisting of a Wi-Fi public access network and participates in the authentication process.

~ IEEE 802.11 ~
The Institute of Electrical and Electronic Engineers (IEEE) has developed the 802.11 family of standards for wireless Ethernet local area networks operating in the 2.4 GHz ISM band and the 5 GHz UNII band. The 802.11 standards define the Medium Access Control (MAC) and Physical Layer (PHY) specifications for wireless LANs (WLANs). The 802.11 standards define protocols for both Infrastructure Mode, where all Wireless Stations communicate via at least one Access Point, and Ad-Hoc (peer-to-peer) Mode, where Wireless Stations communicate directly without use of an intervening Access Point. All public and enterprise WLANs operate in the Infrastructure Mode. Further information about the 802.11 family of standards can be found on the IEEE802.11 web site, www.ieee802.org/11/

~ NAI ~
Network Access Identifier. As defined in [RFC2486], the NAI is the userID submitted by the client during authentication and used when roaming to identify the user as well as to assist in the routing of the authentication request to the user's home authentication server.

~ Public Access Control (PAC) Gateway ~
The Public Access Control (PAC) Gateway may be used by Hotspot Operators to provide the access and services control in their Wi-Fi network. The PAC gateway can perform several key functions for the Hotspot Operator in order to support the Universal Access Methodology.

~ RADIUS ~
An Authentication, Authorization, and Accounting protocol defined by the IETF [RFC2865, RFC2866].

~ Roaming ~
The ability of an end-user with a Wi-Fi device to use the services of an operator other than the one with which they have an account relationship. Roaming implicitly indicates a relationship between a Hotspot Operator, possibly a Broker, a Home Entity and the end-user, who has an established relationship with the Home Entity.

~ Roaming Agent ~
A legal entity operating as a representative of a community of Home Entities or Hotspot Operators, facilitating common legal and commercial frameworks for roaming. The agent does not become a party in the roaming agreement between the Home Entities and Hotspot Operators (like Roaming Brokers do) and retains a neutral position with regard to tariffs and service content offered. An agent operates a multilateral roaming model and typically offers multilateral settlement services.

~ Roaming Broker ~
An entity that provides (global) services for Home Entities and Hotspot Operators by operating as an intermediary and trading broadband access between them at a fixed or transactional price (buying and re-selling roaming airtime usage), and performs clearing and settlement services. Brokers may provide centralized authentication services in order to compute and validate the broadband traffic.

~ Roaming Agreement ~
An agreement for access and services between Hotspot Operators, Roaming Intermediaries, and Home Entities. The agreement regulates the exchange of AAA messages that control the delivery of access at a hotspot and also defines the technical and commercial conditions of such access and is a pre-requisite to initiating roaming services.

- **Bilateral Roaming Agreement**: a roaming agreement negotiated directly between two roaming parties.
- **Multilateral Roaming Agreement**: a roaming agreement negotiated between a Home Entity or Hotspot Operator and a roaming agent.

~ Roaming (AAA) Intermediary ~
An entity in the AAA path between the Hotspot Operator and the Home Entity. The AAA intermediaries could be a clearinghouse, an aggregator, a roaming broker, or a roaming agent.

~ Roaming Tariff ~
The various charges set by the Hotspot Operator for usage of its network by roaming users.

~ Secure Authentication Portal ~
A web page where users of the wireless network enter their user credentials to obtain access to the network using an encrypted mechanism.

~ Smart Client ~
A software solution which resides on the user's access device that facilitates the user's connection to Public Access Networks, whether via a browser, signaling protocol or other proprietary method of access.

~ Universal Access Method (UAM) ~
The recommended methodology, described in section 2, for providing secure web-based service presentment, authentication, authorization and accounting of users is a WISP network. This methodology enables any standard Wi-Fi enabled TCP/IP device with a browser to gain access to the WISP network.

~ Wi-Fi Alliance ~
The Wi-Fi Alliance's mission is to certify interoperability of Wi-Fi™ (IEEE 802.11) products and to promote Wi-Fi as the global wireless LAN standard across all market segments. For more information on the Wi-Fi alliance, please visit their website, http://www.wi-fi.org/.

~ Wi-Fi™ ~
A trademark of the Wi-Fi Alliance. This term refers to all Wi-Fi Alliance-certified IEEE 802.11b networking products.

~ WISP ~
Wireless Internet Service Provider. WISP is a general term that can be a Home Entity allowing their users to roam into a Wi-Fi hotspot or a Hotspot Operator that operates a Wi-Fi based infrastructure for public network access. WISPs may also offer additional services such as location based content and services, Virtual Private Networking (VPN), and Voice over IP (VoIP).

~ WISPr ~
Wireless Internet Service Provider roaming. A Wi-Fi Alliance Committee established to identify recommended best practices for support of wireless roaming between providers of networks employing Wi-Fi technology.

1.2. Requirements Specific Language

Several words in this document are used to signify the requirements to follow the WISPr recommendations. WISPr is not a standards body nor does it have any facility for enforcement. As such, a Requirements Language is necessary, for the purposes of this document, only to convey levels of conviction towards the parameters of the WISPr roaming specification.

The Requirements Language refers to the capabilities of standards compliant networking applications and devices to fulfill the intent of the WISPr inter-network roaming specification and not towards the aspect of Wi-Fi hardware compliance. These imperatives are used to communicate where compliance is actually required for interoperation or limit potentially harmful behavior. The intent is not to use these imperatives to impose a particular implementation, but rather to define the recommended best operational practices for the delivery of WISP roaming services.

This document, as it relates to these definition of terms to describe the requirements of the WISPr specification, follows the conventions as outlined in [RFC2119]:

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD, "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" contained in this document are to be interpreted in the following manner:

REQUIRED – This word, or the terms "MUST" or "SHALL", mean the definition is an absolute requirement to follow the WISPr recommendations.

MUST NOT – This phrase, or the phrase "SHALL NOT", means the definition is an absolute prohibition to follow the WISPr recommendations.

RECOMMENDED – This word, or the adjective "SHOULD", means there may exist valid reasons in particular circumstances to ignore a particular item, but the full implications must be understood and carefully weighed before choosing a different course.

NOT RECOMMENDED – This phrased, or the phrase "SHOULD NOT" means there may exist the valid reasons in particular circumstances when the particular behavior is acceptable or even useful, but the full implications should be understood and the case carefully weighed before implementing any behavior described with this label.

OPTIONAL – This word, or the adjective "MAY", means that an implementer may choose to include the item because a particular business objective requires it or because they feel that it enhances the service while

other implementers may choose to omit the item. An implementation, which does not include a particular option, MUST be prepared to interoperate with another implementation that does include the option though with perhaps reduced functionality, and vice-versa.

1.3. Assumptions

This document makes the following assumptions, in no particular order:

- WISPs SHALL utilize Wi-Fi and/or Wi-Fi5 certified networking components.
- All entities involved in roaming must support the RADIUS protocol [RFC2865, RFC2866] and WISPr-defined attributes for exchange of operational and accounting data.
- All issues related to WISP business models are outside the scope of WISPr. Excluded topics include: services definitions and selection, roaming relationships, selection of roaming clearinghouses, charging models, fees, currencies, settlement methods, billing cycles and anything related to these subjects.
- Established industry standards groups are more suitable to defining inter-standard roaming practices. The GSM Association (WLAN Taskforce) and IS-41 (TIA) (EIA/TIA-45 and TR-46 committees) have the industry representation and technical expertise required to address inter-standard roaming. WISPr will cooperate with these organizations in any future discussions of best practices for inter-standard roaming.
- As new technology and methodologies emerge, WISPr will consider their potential application to WISP roaming.

The deployment of 802.11a wireless LANs does not offer significant technical implications on WISPr because of WISPr's limited dependence on the 802.11 PHY layers. Wi-Fi products (including 802.11a and 802.11b) utilize the same MAC layer. The primary differences between them fall within the PHY layers and include varying data rates, modulation types, and transmission frequencies. These are differences that the implementer must take into account when deploying the wireless LAN.

2. Access Methods

WISPr recommends the Universal Access Method (UAM) to facilitate WISP roaming. The UAM allows a subscriber to access WISP services with only an Internet browser and Wi-Fi network interface on the subscriber device, so that all users, regardless of device type or operating system, can participate in WISP roaming. The UAM utilizes an Internet browser-based secure Authentication Portal, user credential entry, and RADIUS AAA. The UAM represents the lowest common denominator for granting access to a WISP network ensuring that all users can share the same experience.

The Universal Access Method may be enhanced by use of a proprietary Smart Client to simplify the user experience. A Smart Client can be used to enhance the subscriber experience by providing features such as a directory listing available public network access hotspots, SSID browsing, automated sign-on or single click launch of additional software (like a remote Virtual Private Network client). These Smart Clients are typically compatible with, and add value over and above the UAM, and are typically provided by the subscriber's Home Entity. Home Entities should be mindful that requiring the use of a proprietary Smart Client could restrict network access. As a result, Home Entities must ensure that use of the Smart Client does not preclude roaming using the UAM.

The recently introduced IEEE 802.1x standard provides a protocol for authentication and port-based access control supporting enhanced access security, but has not been widely deployed in public access environments. Unlike the UAM, the 802.1x access method requires client software on the subscriber device. Further discussion of the 802.1x authentication method and user experience is provided in Appendix A.

2.1. The Universal Access Method User's Experience

The user experience in the following section describes a typical user experience at a Wi-Fi public access hotspot using the Universal Access Methodology to control user access.

"A user visits a public hotspot. He boots up his laptop and associates with the local Wi-Fi network by selecting the available network or entering the correct SSID in his Wi-Fi PC Card Configuration Utility. He then starts his browser, which, for the sake of discussion, is configured to load www.yahoo.com as his home

page. Instead of the browser loading this home page, it loads a Welcome Page from the Hotspot Operator that allows the user to login with a username and password. Once authenticated, a Start Page appears from the Home Entity and the user can access his original home page such as Yahoo. In addition, a smaller window pops up detailing session information and providing a button which, when clicked, will log him out. At this time the user can access the Internet via his wireless connection. When the user finishes, he clicks the aforementioned logout button to disconnect from the network and continues to work on the laptop or shuts down his laptop and leaves."

The minimum HTML-based logon process and requirements for each page are outlined in the following diagram and sections. A collection of the authentication pages provided by the Hotspot Operator may also be referred to as the Secure Authentication Portal (SAP).

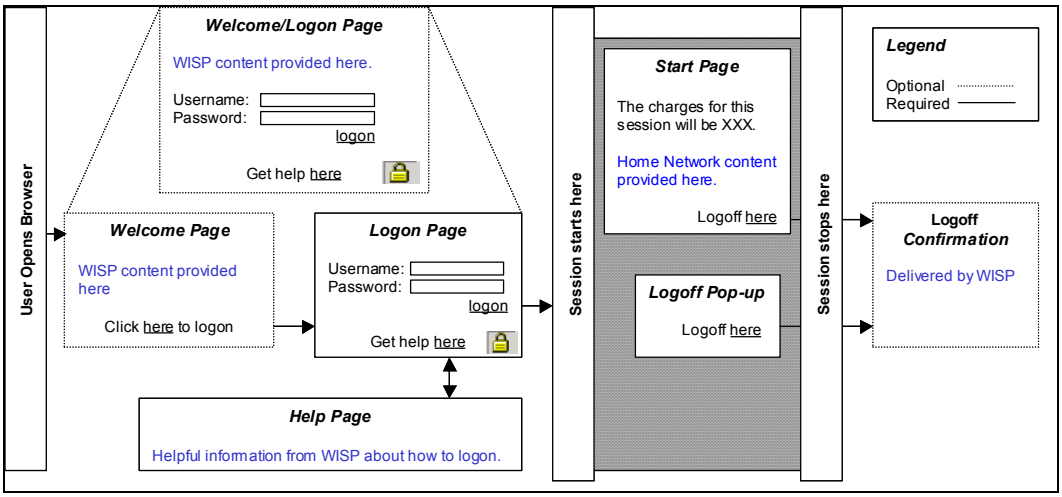


Figure B: Universal Access Method (UAM) User Experience

Welcome Page

The Welcome Page is an OPTIONAL web page provided by the Hotspot Operator. The Welcome Page is the first page that is presented to the user. The Welcome Page MAY contain local content such as maps, local hotel information, baggage and ticketing information, restaurants, etc. The Logon Page and the Welcome Page may be the same page, but in some cases the Welcome Page may only provide a link to the Logon Page or to other network access-specific pages, such as localized text pages for multi-lingual access instructions. At minimum, a clearly identifiable link to the Logon Page MUST be provided on the Welcome Page.

Logon page

The secure Logon Page is REQUIRED and is delivered by the Hotspot Operator. This page is made secure by the use of SSL (Secure Socket Layer). At a minimum, the logon page MUST have space to enter the user's credential. The user's credentials are the same across all WISPr-compliant networks, specifically in the format of username@domain, as specified by the Network Access Identifier (NAI) [RFC2486], extended by allowing the use of embedded spaces in the username, prohibiting case translation by any intermediate parties, and used to assist in the routing of the authentication request. Users who are subscribers of the Hotspot Operator (in this case the Hotspot Operator is the user's Home Entity) are NOT REQUIRED to enter a @domain qualifier (NAI) following the username.

Help Page

Although the Help Page is REQUIRED, the actual content of the Help Page is at the discretion of the Hotspot Operator. In order to facilitate the logon process for first time users, information on how to logon in a roaming environment SHOULD be provided. Additional instructions for new user registration MAY be

provided here.

As with the Logon Page, language localization for the Help Page is helpful, but entirely OPTIONAL.

Start Page

The Start Page functionality is REQUIRED to be supported by the Hotspot Operator, but the Start Page URL address is specified by the Home Entity. Upon successful authentication of a roaming user, the Hotspot Operator MUST redirect the customer to the Home Entity's Start Page as specified in an AAA Vendor Specific Attribute (VSA) transmitted during the user's authorization. If the Home Entity does not provide the Start Page VSA, the Hotspot Operator MAY proceed to the user's originally requested URL (origin server) or a default Hotspot Operator Start Page instead.

The Start Page MAY communicate information to the customer regarding roaming billing, charges that will be incurred as a result of using the service. Roaming users SHOULD be able to cancel the session from this page. An explicit method for logoff MUST be presented on the Start Page to allow for this function. To achieve this, the Hotspot Operator is REQUIRED to specify in an AAA Vendor Specific Attribute (VSA) the explicit Logoff URL for the wireless hotspot the customer is requesting access.

Logoff Confirmation Page

The Logoff Confirmation Page is RECOMMENDED for explicit logoffs and delivered by the Hotspot Operator. The page is intended to provide confirmation to the customer that they have been logged off and MAY contain session statistics in regards to the user's closed session.

2.2. Logoff Functionality

Both implicit and explicit logoff capabilities are REQUIRED to be provided by the Hotspot Operator, even if they are not applicable to the local network provider's own billing methods. The reasoning behind this is that different billing methods will exist from provider to provider. WISPr RECOMMENDS real-time accounting via the appropriate AAA, including connection, time, and usage based information. Even though the Hotspot Operator may be billing the Home Entity or customer owner in megabytes and not require the user to logoff, the customer may be billed in minutes and MUST have the ability to logoff.

It is RECOMMENDED the Home Entity provide an explicit logoff method via the Start page.

Explicit logoff

A clear method MUST be provided by the Hotspot Operator to allow the user to logoff the visited network. This explicit logoff function SHOULD be delivered in several different ways including, but not limited to:

1. A hypertext link from the Start page
2. A small popup window that allows the user to click a logoff button
3. For PDA users, as an alternate to the popup window, a logoff web page could be bookmarked so the user could return to the page to manually initiate the logoff process

Implicit logoff

If a user does not explicitly logoff, a session MUST be guaranteed to eventually end. This implicit logoff protects the user in case of a loss of signal or some other failure. It is RECOMMENDED that the user not be required to login again if they reboot their PC or end up losing signal for a short period of time. However, indefinite time out periods are also undesirable because by the nature of the technology, roaming wireless connections do not have a clear indication of termination of connection.

In order to more accurately measure the actual usage on the Hotspot Operator's network a Hotspot Operator MUST support the idle (or inactivity) timeout specified by the Home Entity in the idle-timeout attribute. If the idle-timeout attribute is not specified, then the Hotspot Operator should utilize an idle-timeout of no more than five minutes. The idle period is determined by the elapsed time since the user has last transmitted a packet, or is no longer accessible on the network. Once this idle-timeout period is reached, the user will have

their session automatically terminated and appropriate accounting mechanisms record the end of session. In the case of an idle-timeout, the Acct-Session-Time sent as part of the accounting record should be reduced by the length of the idle-timeout period in order to prevent the user from being overcharged.

The Home Entity MAY prohibit indefinite connections by providing a maximum session time available to its roaming customers by specifying a Session-Timeout attribute in the roaming user's profile. A user exceeding this time would have his access removed, an account record generated, and would be forced to re-login to gain access.

2.3. HTML/CGI Standardization

To facilitate connections using a Smart Client, WISPr recommends standardization of the HTML/ASP and CGI mechanisms at the Secure Authentication Portal (SAP), the combination of the pages described in the previous section. It is understood there are a wide variety of implementations of Login Pages and providers who wish to implement a Smart Client must know the vendor and method at the hotspot for the SAP. However, if a Hotspot Operator is creating a unique Authentication Portal Logon Page or modifications to the Logon Page are made, care should be taken to consider the following WISPr recommendations:

- Form Post data variables for collecting the user credential should be in the form of "username" and "password" whenever possible. As part of the username, users will be logging into the Home Entity using an NAI to identify the user's home authentication server. The use of the NAI will extend the "username" significantly. In accordance with the Network Access Identifier specification in [RFC2486], devices that handle NAI's, such as the Secure Authentication Portal in this case, MUST support an NAI length (username) of at least 72 characters.
- Use of standardized URLs is RECOMMENDED. When creating Logon and Logout functions, use of a consistent naming convention and CGI implementation network-wide will help facilitate the identification and passing of user credential information directly to the SAP by a Smart Client without the need for the user to manually type in his/her credentials. All login data requirements should be presentable to the hotspot in a single URL.

3. Hotspot Operator's Network Architecture

As outlined in Section 2 above, the Universal Access Method enables public access connectivity to the Hotspot Operator's network while allowing users to retain a billing relationship with their Home Entity. To support the Universal Access Method, a Hotspot Operator must provide Wi-Fi connectivity and support several key Public Access Control functions as described below.

3.1. Public Access Control (PAC) Gateway

The Public Access Control (PAC) Gateway may be used by Hotspot Operators to provide the access and services control in their Wi-Fi network. The PAC gateway can perform several key functions for the Hotspot Operator in order to support the Universal Access Methodology. The primary PAC gateway functions may include:

- IP Address Management
- Home Page Redirection
- Authentication and SSL Support
- Authorization
- Accounting
- Access Control
- VPN Support
- Mail Support
- Authentication Testing Facility

The PAC gateway is a logical entity, and is not necessarily a distinct network component. A range of hardware and software configurations can deliver the functions of the PAC entity, such as:

- A stand-alone networking device,
- As an integrated software gateway function of another networking device such as an Access Point or router, or
- As a distributed array of such devices in a "hybrid" network architecture.

3.2. Access Points, SSID, and Hotspot Network Association

Various methods have been established for facilitating the association of the user's station with the Hotspot Operator's Wi-Fi Access Point. The minimum requirement for association with an Access Point in the Universal Access Method is knowledge of the Hotspot Operator's network SSID. Incorrect selection of the SSID may result in a confusing user experience and a failure to logon. Currently, manual configuration of the Wi-Fi station with the correct SSID or "browsing" the SSID beacons are the preferred methods of SSID determination.

Client Settings

To allow for easy configuration and association with the Hotspot Operator's network when roaming, WISPr strongly recommends that clients set their devices to disable WEP. Since the over-the-air link is completely insecure, WISPr strongly recommends the use of a VPN or other security measures to ensure the privacy of data.

WISPr recommends that clients who may utilize a private WEP key should be informed of the requirement to disable their WEP configuration to access a roaming network. It should be made clear that any private WEP information may be lost in doing so, therefore it is highly recommended that the user note this key (often up to 13 characters for 128-bit WEP encryption) so it may be replaced after the user leaves the Hotspot and returns to his/her "private" environment.

SSID

Users who are unfamiliar with the configuration utilities provided by their Wi-Fi NIC manufacturer and are not comfortable with manually setting the required SSID value should be encouraged to set their SSID to "ANY" as supported by their Wi-Fi Configuration Utility. Use of "ANY" allows the user's station to automatically associate with the "nearest" Wi-Fi network without the need for the user to configure their NIC manually with the correct SSID. Implementation of this form of Wi-Fi network association support varies by Wi-Fi NIC manufacturer.

If ANY is used to automatically associate with Wi-Fi networks as they are encountered, users should be cautioned to be cognizant of the network login pages of the available Wi-Fi networks before transmitting account information. Users should be encouraged to maintain an awareness of the networks to which their station associates with and should never attempt to login or transmit their user credential (NAI) to unknown networks.

Furthermore, Wi-Fi Internet Service Providers and card manufacturers should consider the following SSID issues:

- Each Hotspot Operator SHOULD consider using a unique SSID to differentiate their Access Point from other available Wi-Fi networks by incorporating the Hotspot Operator's name as part of the identifier (e.g., "`ACMEWISP_NewarkAirport`") as described as part of the Location-Name AAA Attribute.
- Inclusion of the SSID in beacon transmissions and response to the broadcast SSID (read as "wildcard SSID") in probe request frames from a client (as required by the 802.11 standard) is RECOMMENDED for all Hotspot Operator access points to allow for SSID browsing and implicit Wi-Fi network associations by the user client station's OS or Wi-Fi Configuration Utility software.

4. AAA

RADIUS is the preferred AAA protocol for Wi-Fi roaming. As other protocols become available for deployment, WISPr will review the technology and make recommendations. Regardless of the access method used, the RADIUS protocol is used between entities to coordinate roaming between service partners.

Given the importance of AAA to inter-WISP roaming, WISPr seeks to clearly identify the critical aspects of AAA that must be considered for a Wi-Fi roaming framework:

- Protection of the user's Identity and credentials
- Proper implementations and practices to support Accounting
- RADIUS protocol compliance

- RADIUS attribute support
- Informational WISPr RADIUS attributes for WISP roaming

4.1. Accounting Support

Specific WISP business practices related to roaming, clearinghouse, settlement and billing are not within the scope of WISPr. However, the minimum technical requirements specified here are required to provide the exchange of the necessary accounting data between Hotspot Operators, Intermediaries, and Home Entities to assure the integrity of billing and settlement processes.

Vendors, Hotspot Operators, and Intermediaries SHOULD NOT implement partial AAA solutions (e.g. only provide authentication and authorization with no accounting). Public Access methods that do not provide complete RADIUS session accounting SHOULD NOT be used in Public Access Networks unless combined with the Universal Access Methodology for AAA or other manner to record usage durations in an acceptable fashion.

4.2. AAA Data Exchange

The Hotspot Operator MUST provide the Home Entity with all generated RADIUS/AAA authorization and accounting messages, including any interim accounting messages.

This document makes no requirements on the transmission path of the AAA data. The AAA data can be sent on the public Internet, over a segregated private network link, or isolated within VPN tunnels. The choice of transmission path is decided on a bilateral basis between operators of the RADIUS/AAA servers.

Exchange Cycle

Real-time delivery of RADIUS/AAA data is REQUIRED. The RADIUS/AAA accounting messages are the basic usage telemetry that allow all service providers to monitor and measure usage of their subscribers. The real-time delivery of RADIUS/AAA accounting messages is necessary and sufficient to support any usage based business model, including Prepaid or Debit card services.

AAA Data Exchange Integrity

Hotspot Operators and Roaming Intermediaries should strive for 100% reliability of AAA message delivery. Experience has shown that 99.9% reliability of AAA message delivery should be routinely achievable under high traffic conditions.

All parties along the transmission path of the AAA data should exercise care in the engineering of the communication links and the capacity of the RADIUS/AAA servers. It is a common fallacy that the reliance on the UDP protocol for transporting RADIUS/AAA data is the cause of RADIUS message loss. The RADIUS protocol employs its own data retransmission strategy for ensuring that packets are delivered reliably over lossy communication paths. Service providers need to exercise care in properly selecting the retransmission parameters appropriate for the bandwidth, path error, and path congestion characteristics between RADIUS/AAA servers. Undersized RADIUS/AAA servers are a common cause for the loss of RADIUS messages. Undersized RADIUS/AAA servers can reliably receive a RADIUS message and then lose the message internally as its internal resources are overwhelmed by traffic. Service providers should characterize the capability of their RADIUS/AAA servers so that they can anticipate and prevent conditions that lead to RADIUS message loss in the servers.

Support for Interim Accounting Messages

Support for RADIUS Interim Accounting Messages is RECOMMENDED to minimize the impact of a lost session start or stop message. It is RECOMMENDED that the Hotspot Operator support generation of interim accounting messages at time intervals set by the Home Entity's RADIUS server. The interval for RADIUS Interim Accounting Messages establishes the minimum measurable interval of usage. If the final RADIUS Accounting Message is lost, the RADIUS Interim Accounting Message limits the maximum amount of measured service delivered without supporting accounting data is limited by the RADIUS Interim

Accounting Message interval. [RFC2869] recommends that the interim accounting interval SHOULD NOT be smaller than 600 and careful consideration should be given to its impact on network traffic. This interval is considered sufficient to support many WLAN applications.

Archiving of Accounting Data

In order to facilitate usage audits and charging reconciliation, the parties at both ends of a RADIUS link SHOULD maintain a log of RADIUS messages exchanged. Complete records of raw RADIUS message data SHOULD be archived for the same periods and with the same care as invoice and accounting data. The archived data must be readily available on request, but need not be accessible on-line. Local laws determine the required storage time for billing-related accounting information. For example, most European countries require 1-year storage of invoicing and billing data. In the United States, cellular carriers are required to keep call detail and roamer settlement records for 7 years, and cellular clearinghouses keep settlement summary reports for 7 years.

5. RADIUS Attribute Support

RADIUS attributes provide for the critical handling of session control, accounting information, and potential implementation of real-time services. As such, Hotspot Operators and Roaming Intermediaries should support the broadest possible set of RADIUS attributes for various services, even though those services are not offered on their networks (i.e., TCP-Clear for legacy support, Session-Timeout for pre-paid Internet access and EAP for wireless security). To prevent loss of data and/or services failure, all Roaming Intermediaries or RADIUS proxy systems are REQUIRED to support the RADIUS Attributes specified in the following section.

5.1. Required Standard RADIUS Attributes

It is RECOMMENDED that Hotspot Operators implement all RADIUS v1 attributes from 1-88 in addition to supplementary attributes for control of specific NAS functions. At a minimum, WISPr REQUIRES the following standard RADIUS attributes be supported for purposes of basic services, fault isolation, and session/transaction accounting:

Required Attribute	#	Type	Auth Req	Auth Reply	Acctg Req	Comment
User-Name	1	String	X		X	User enters full NAI
User-Password	2	String	X			
NAS-IP-Address	4	Ipaddr	X		X	IP Address of the Access Gateway
Service-Type	6	Integer	X			Must be set to Login (1)
Framed-IP-Address	8	Ipaddr	X		X	IP Address of the User
Reply-Message	18	String		X		Text of reject reason if present
State	24	String	X	X		
Class	25	String		X	X	
Session-Timeout	27	Integer		X		Forced logout once timeout period reached (seconds)
Idle-Timeout	28	Integer		X		Implicit logout inactivity timeout period (seconds)
Called-Station-ID	30	String	X		X	This field should contain the MAC address or other information identifying the Access Gateway
NAS-ID	32	String	X		X	
Acct-Status-Type	40	Integer			X	1 = Start, 2 = Stop, 3 = Interim Update
Acct-Delay-Time	41	Integer			X	Delay (seconds) between Acctg Event and when Acct-Req sent (doesn't include estimated network transit time)
Acct-Input-Octets	42	Integer			X	
Acct-Output-Octets	43	Integer			X	
Acct-Session-ID	44	String	X	X	X	
Acct-Session-Time	46	Integer			X	Call duration in seconds (already compensated for idle timeout)
Acct-Input-Packets	47	Integer			X	

Required Attribute	#	Type	Auth Req	Auth Reply	Acctg Req	Comment
Acct-Output-Packets	48	Integer			X	
Acct-Terminate-Cause	49	Integer			X	1 = Explicit Logoff, 4 = Idle Timeout, 5 = Session Timeout, 6 = Admin Reset, 9 = NAS Error, 10 = NAS Request, 11 = NAS Reboot
NAS-Port-Type	61	Integer	X		X	15 = Ethernet, 19 = 802.11
Acct-Interim-Interval	85	Integer		X		Interval (seconds) to send accounting updates

630 **CHAP-Password**

631 CHAP password is not possible with the protocol described above, as there is no challenge-response phase
632 between the client and the access gateway. For this reason, the access gateway does not initiate CHAP in the
633 *Access-Request* message; therefore, the *CHAP-Password* field should not be used.

634 **NAS-Identifier**

635 The *NAS-Identifier* MAY be set to a pre-agreed value identifying the access gateway. *NAS-Identifier* is the
636 preferred attribute for location identification when *NAS-IP-Address* cannot be used for this purpose. When
637 present, *NAS-Identifier* MUST be included in both *Access-Request* and *Accounting-Request* packets.

638 **Idle-Timeout**

639 The *Idle-Timeout* field included in the *Access-Accept* must be used to set the amount of time the user is
640 allowed to stay idle before being disconnected. When the user is disconnected due to an Idle-Timeout, the
641 following *Accounting-Request* message must have the *Acct-Session-Time* reduced by the length of the *Idle-*
642 *Timeout* in order to prevent the user from being overcharged.

643 **NAS-Port-Type**

644 Both the *Access-Request* and *Accounting-Request* must include the *NAS-Port-Type*. The Access Gateway
645 may distinguish between Ethernet (15) and 802.11 (19) when they are present at the same venue.

646 ## 5.2. WISPr Vendor Specific Attributes

647 WISPr RECOMMENDS the implementation of certain Vendor Specific Attributes (VSA). The VSA values
648 are intended to provide the Home Entity and/or Broker with information such as the user's location to
649 facilitate back-end processing of transaction data as well as to provide service-level information. WISPr has
650 obtained an IANA Private Enterprise Number (PEN) of 14122 that is registered to the Wi-Fi Alliance, which
651 will be used to pass *Vendor-Specific* attributes for use with broadband roaming services and can be utilized
652 by various vendors and providers who wish to support WISPr functionality. Any other proprietary *Vendor-*
653 *Specific* attributes should be propagated through the roaming network. *Vendor-Specific* attributes, which
654 should receive specific handling, are detailed below.
655

WISPr Vendor Specific Attributes	#	Type	Auth Req	Auth Reply	Acctg Req	Comment
Location-ID	1	String	X		X	Hotspot Location Identifier
Location-Name	2	String	X		X	Hotspot Location and Operator's Name
Logoff-URL	3	String	X			URL for user to perform explicit logoff
Redirection-URL	4	String		X		URL of Start Page
Bandwidth-Min-Up	5	Integer		X		Minimum Transmit Rate (b/s)
Bandwidth-Min-Down	6	Integer		X		Minimum Receive Rate (b/s)
Bandwidth-Max-Up	7	Integer		X		Maximum Transmit Rate (b/s)
Bandwidth-Max-Down	8	Integer		X		Maximum Receive Rate(b/s)
Session-Terminate-Time	9	String		X		YYYY-MM-DDThh:mm:ssTZD
Session-Terminate-End-Of-Day	10	Integer		X		Flag zero or one indicating termination rule.
Billing-Class-Of-Service	11	String		X		Text string indicating service type.

WISPr Network Location information is to be delivered in the WISPr-Location-ID and WISPr-Location-Name attributes. The intent of this requirement is to provide the information regarding the user's location and connection that is required by the Hotspot Operator and Home Entity for the purposes of facilitating billing processes. WISPr RECOMMENDS a consistent usage of VSAs split between a standardized set of VSA for billing and others to be used as a generic variable content Text Location Identifier.

~ Location-ID ~

A *Location-ID* value SHOULD be included in the *Access-Request* and *Accounting-Request* packet. This *Location-ID* MUST be configurable for each hotspot location and be of the form:

```
isocc=<ISO_Country_Code>,cc=<E.164_Country_Code>,ac=<E.164_Area_Code>,
    network=<SSID/ZONE>
```

Example:

```
"isocc=us,cc=1,ac=408,network=ACMEWISP_NewarkAirport"
```

~ Location-Name ~

The name of the Hotspot Operator and a textual description of the location SHOULD be included in the *Access-Request* and *Account-Request* packet. This value MUST be configurable for each access gateway and be of the form:

```
<HOTSPOT_OPERATOR_NAME>,<Location>
```

Example:

```
"ACMEWISP,Gate_14_Terminal_C_of_Newark_Airport"
```

~ Redirection-URL ~

The *Access-Accept* packet MAY include a *Redirection-URL;* this is the URL of the Start Page that the user's browser is directed to after authentication. When this value is present, the user's browser should be directed to the indicated URL. This will allow the Home Entity to control the user's experience.

~ Logoff-URL ~

The *Access-Request* packet MUST include a *Logoff-URL.* This value is presented to allow the Home Entity to provide a link on their Start Page for the user to Logoff.

~ Bandwidth-Max-Up and Bandwidth-Max-Down ~

These attributes specify the maximum rate at which that corresponding user is allowed to transmit (Up) and receive (Down) data. Since the user may be connected to the hotspot via local LAN connection that has higher bandwidth than the available WAN bandwidth out of that hotspot, when specified, the hotspot should throttle down the amount of data the user can transmit and/or receive.

~ Bandwidth-Min-Up and Bandwidth-Min-Down ~

These attributes specify the minimum guaranteed rate at which bandwidth should be reserve for the user to transmit (Up) and receive (Down) data. Support for guaranteed end-to-end Quality of Service (QoS) is currently not available but being reserved for the future use and is currently only enforced for the traffic flowing through that specific hotspot location.

~ Session-Terminate-Time ~

The *Session-Terminate-Time* VSA indicates the time when the user should be disconnected from the network. The field is a text string formatted according to ISO 8601 format YYYY-MM-DDThh:mm:ssTZD. If the TZD is not included, the user should be disconnected at the time specified in local time. For example, a disconnect on 18 December 2001 at 7:00 PM Universal Coordinated time would be formatted as "2001-12-18T19:00:00+00:00". A disconnect request for midnight local time on the same day would be formatted

"2001-12-18T00:00:00". If the *Session-Terminate-Time* is included, the *Session-Terminate-End-Of-Day* VSA should not be sent. This attribute should be treated as an explicit logoff.

~ Session-Terminate-End-Of-Day ~

The *Session-Terminate-End-Of-Day* VSA is an integer flag of either zero or one indicating whether the user's connection should be terminated at the end of its billing day. If a specified billing day is not provided, this field should be ignored. This attribute should be treated as an explicit logoff.

~ Billing-Class-Of-Service ~

The *Billing-Class-Of-Service* is a free-form text field. It is intended to indicate service variations that would require different charges even though they occurred at the same hotspot. The contents of the field should be negotiated between the Home Entity or Roaming Intermediary and the Hotspot Operator and may indicate, for example, the difference between service obtained in a hotel room versus service obtained in the lobby or conference room.

6. Security

WISPr REQUIRES that Hotspot Operators conform to a minimum level of security in regards to the promotion and support of the following security considerations:

- Authentication of the User and the Hotspot Operator
- Protecting the User's Credentials and Information
- Protecting the User's Data
- Protecting the User's Station
- Protecting the WISP Networks

This section describes the areas vulnerable to attack and special consideration that should be taken when using the Universal Access Method. Different characteristics and challenges for protecting the user's credentials from attack are addressed in Appendix A: 802.1x.

6.1. Authentication

The Hotspot Operator MUST provide a way for a user to authenticate the network as well as a way for a network to authenticate the user. In other words, mutual authentication MUST be supported:

- In order for the network to authenticate the user, username and password is used.
- In order for the user to authenticate the Hotspot Operator, the Login Page MUST use SSL and MUST utilize a certificate for that page so the user's browser can check if the server's Fully Qualified Domain Name (FQDN) is valid before the user enters their username and password.

The ability for the user to authenticate the Hotspot Operator is important for web-based user authentication where a user's login attempt may be redirected to a rogue Authentication Portal that can obtain username and password information. WISPr RECOMMENDS that the Hotspot Operator use Public Key Infrastructure (PKI) certificate-based authentication using HTTPS (HTTP over SSL). In this case, the Hotspot Operator should obtain its server certificate issued by a trusted 3rd-party Certificate Authority that performs strict verification process (i.e., Class 3 authentication) against the Hotspot Operator before issuing the certificate. This provides a way to find out the legal entity of the Hotspot Operator if an identity theft occurs.

6.2. Protecting the User's Credentials/Information

The Wi-Fi Internet Service Provider MUST protect the User Credential when presented at an Authentication Portal. When using Universal Access or browser-based solutions and the user is expected to enter his User Credential into a Authentication Portal, the web URL handling the transmission of the request to the AAA infrastructure MUST be protected, (e.g. SSL, SSH, HTML MD5 Hash, MD5 Challenge). For example, the Logon Page should utilize SSL so the username and password when submitted via the Web Browser are encrypted and protected. This mandatory requirement protects both the user and the Hotspot Operator from account "identity theft" and session hijacking.

To protect the user name and password from being intercepted at any link between RADIUS entities, it is RECOMMENDED that service providers use IPSEC or other VPN technology to protect the RADIUS messages between RADIUS servers. Although RADIUS accounting messages are protected from modification by the message authentication attribute, the use of IPSEC or other VPN technology can be used to hide the contents of the RADIUS accounting message if desired.

It should be noted that even if IPSEC or other VPN technology is used, a service provider could only be sure that the RADIUS message is protected between the sending service provider and the receiving service provider. The sending service provider may not be able to assure to their users that the third-party receiving service provider will similarly protect the RADIUS traffic as it is forwarded to other third-parties.

To prevent the user's identity from theft by a malicious Hotspot Operator, third-party, or system administrator (such as the case if the username and password was stored in a log file at the AAA Server or access gateway), it is possible for the user to use an anonymous username from their Home Entity (e.g., anonymous@MyHomeEntity.com) and use a one-time-password that could also be hashed or encrypted with the users identity that only the Home Entity could identify. The use of one-time passwords also protects the users who otherwise could use a simple password that is vulnerable to dictionary attacks.

These and additional security concerns are being addressed with more advanced security protocols and will be revisited as appropriate technologies (like 802.1x) become more widely available.

6.3. Protecting the User's Traffic/Data

WEP

Due to the current limitations in WEP implementations, such as the requirement of a static WEP key be assigned to the access point and configured in each user's client, WEP is not useful for public access networks. When technologies and methods for dynamic WEP key assignment (such as 802.1x) become more widely available and supported in users clients, WISPr will revisit the support of WEP as part of its recommendations. Instead, SSL is used to encrypt and protect the user's credentials during the authentication phase and the user can utilize VPN software to protect subsequent traffic/data.

Fluhrer, Mantin, and Shamir have described WEP limitations that have been further validated by AT&T Labs [ATT]. As per AT&T recommendations on the implementation of WEP for Hotspot Operators, WISPr concurs with their conclusions:

- Assume that the link layer offers no security.
- Use higher-level security mechanisms such as IPSEC and SSH for security, instead of relying on WEP.
- Treat all systems that are connected via 802.11 as external. Place all access points outside the firewall.
- Assume that anyone within physical range can communicate on the network as a valid user. Keep in mind that an adversary may utilize a sophisticated antenna with much longer range than found on a typical 802.11 PC card.

VPN Software

It is highly RECOMMENDED that Home Entities promote the use of Virtual Private Network software by their users to protect the privacy of all sensitive over-the-air data and Internet transactions. Use of VPN software combined with a Secure Authentication Portal offsets any actual or implied limitations of WEP security. In accordance with the Universal Access Method, the use of VPN Software is not required in order for the user to access the hotspot's content or services, authenticate himself with a Hotspot Operator, gain Internet access, or utilize Home Entity services.

6.4. Protecting User's Client and Home Entity

It is highly RECOMMENDED that all users of WISP networks to install and employ Personal Firewall software. Personal Firewalls protect the user's station from WLAN-based attacks and exploits.

It is highly RECOMMENDED to all users of WISP networks to install and employ Virus Protection agents and programs to protect against WLAN-based exposure to other infected devices and hand carrying the problem back to the Home Entity or private network.

6.5. Protecting the WISP Network

It is highly RECCOMENDED that all WISP networks employ basic firewall protections and/or security methods, either on the network facilities or on the access devices themselves, to protect against intrusion and internet-based Denial-of-Service attacks.

WISP roaming networks should consider their policies on SMTP restrictions and "spam" protections as it relates to their user's roaming services. If a Home Entity protects their SMTP services to known IP address, other means for providing mail services to roaming customers must be considered. Use of the Hotspot Operator's SMTP server by roaming users is generally acceptable when identification is pre-arranged. Proper DNS resolution of all DHCP addresses is RECOMMENDED to facilitate the identification of remote network transactions by a Home Entity and its services.

7. References

[8021x] Congdon, P., Aboba, B., Moore, T., Palekar, A., Smith, A., Zorn, G., Halasz, D., Li, A., Young, A., Roese, J., "IEEE 802.1x RADIUS Usage Guidelines", IETF Internet Draft, July 2001.

[ATT] AT&T Labs, "Using the Fluhrer, Mantin, and Shamir Attack to Break WEP", TD-4ZCPZZ, www.cs.rice.edu/~astubble/wep/, August 6, 2001.

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", IETF RFC 2119, March 1997.

[RFC2284] Blunk, L. and Vollbrecht, J., "PPP Extensible Authentication Protocol (EAP)", IETF RFC 2284, March 1998.

[RFC2477] Aboba, B. and Zorn, G., "Criteria for Evaluating Roaming Protocols", IETF RFC 2477, January 1999.

[RFC2486] Aboba, B., Beadles, M., "The Network Access Identifier", IETF RFC 2486, January 1999.

[RFC2865] Rigney, C., Willens, S., Rubens, A., Simpson, W., "Remote Authentication Dial In User Service (RADIUS)", IETF RFC 2865, June 2000.

[RFC2866] Rigney, C., "RADIUS Accounting", IETF RFC 2866, June 2000.

[RFC2869] Rigney, C., Willats, W., and Calhoun, P., "RADIUS Extensions", IETF RFC 2869, June 2000.

8. Acknowledgements

Thank you to the Wi-Fi Alliance board for your insight and patience.

Many of the definitions and terms contained in this document have been integrated from various IEEE and IETF resources. Thank you IEEE and IETF for providing such a wealth of online information!

Participating Wi-Fi Alliance Committee Members

Thank you to the participating WISPr members. Group document writing is no easy task. We learned a lot from each other.

The following list details the Wi-Fi Alliance membership in attendance of at least one WISPr meeting during the development of this document:

- Agere Systems
- Airwave Wireless, Inc.
- AMD
- Askey Computer Corp.

- Atheros Communications
- Cisco Systems
- Colubris Networks, Inc.
- Compaq
- Dell Computer Corporation
- Enterasys Networks
- Excilan
- Fiberlink Communications
- Funk Software
- Gemtek Systems, Inc.
- GRIC Communications, Inc.
- HereUare Communications, Inc.
- Illuminet
- Intel Corporation
- Interlink Networks, Inc.
- Intersil
- iPass, Inc.
- Jungo Networks
- Lucent Technologies
- Microsoft Corporation
- Mobilestar Network Corporation
- NEC Corporation
- Nokia Networks
- Nomadix, Inc.
- Nortel Networks
- NTT
- Philips
- Proxim, Inc.
- Sprint PCS
- Symbol
- Telia
- Toshiba
- TSI Telecommunication Services, Inc.
- TTS-Linx
- Wayport
- Woodside Networks

WISPr Contact Information

The following individuals may be contacted in regards to WISPr or this document:

Butch Anton (WISPr Chair)
Gemtek Systems, Inc.
Email: butch@butch.net

Blair Bullock (WISPr Vice-Chair)
iPass, Inc.
Email: bbullock@ipass.com

Joel Short (WISPr Vice-Chair)
Nomadix, Inc.
Email: jshort@nomadix.com

Appendices

WISPr has considered several "forward-looking" technologies that may, in the future, be useful in WISP roaming. Some of these technologies and protocols are simple enhancements to the base-line recommendations; others are in still in the early stages of development, while some (such as IEEE 802.1X) are substantially complete but are not widely deployed. As such, it is impossible to make distinct recommendations for the implementation of these technologies and so consideration of these technologies has been placed in the appendices to follow. WISPr is committed to further exploring new technologies and protocols as they emerge and evaluating the issues surrounding future WISPr implementations. In order for an appendix to be formally adopted as an official WISPr recommendation and moved into the main body of this document, new and substantial evidence must be introduced to qualify the technology as having positive field experience in a WISP implementation as it applies to roaming.

Appendix A – 802.1x

Access Method User Experience

"The user starts his laptop (either from boot up or a resume) and provides the 802.1x networking client with a username, a credential, and the Hotspot Operator's SSID. The wireless networking client manages the connection to the Hotspot Operator and establishes networking service through an existing user account. The networking client automatically starts up the users welcome page specified by the AAA server. When the user is finished, he simply disconnects from the wireless network explicitly through the wireless networking client or by simply shutting down his laptop. Either action will result in immediate disconnect of his session."

When 802.1x authentication methods are used, the user service is controlled by the AP. See the figure below, "Figure D: Authentication and Accounting Process for Roaming 802.1x Users."

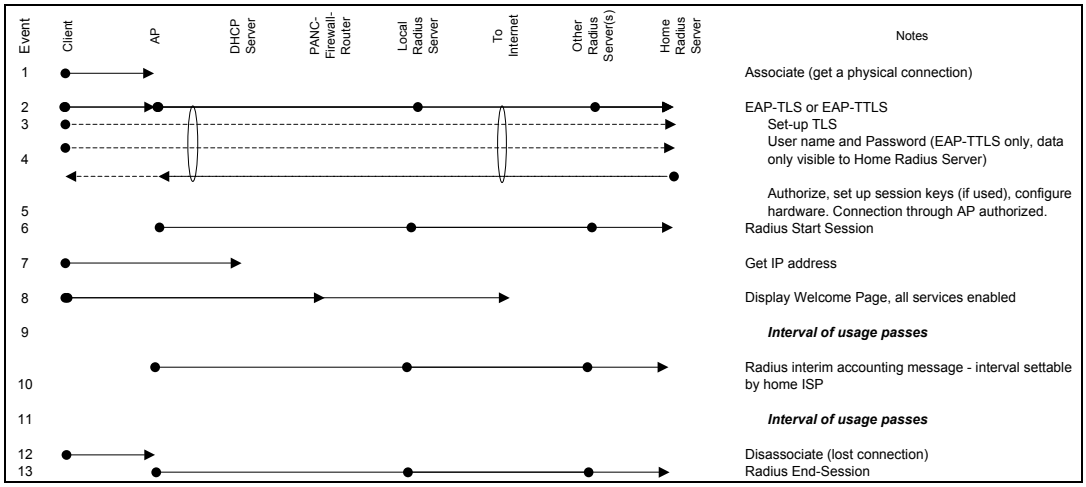


Figure C: Authentication and Accounting Process for Roaming 802.1x Users

Event 1, 2, 3: The access process will begin with the client and AP negotiating the use of an EAP authentication method. In this example, the user is configured for the use of EAP-TLS or EAP-TTLS. In both cases, TLS is used to authenticate the home RADIUS server. This is essential, as the user has a preexisting established business (trust) relationship with their Home Entity. This step is protected from unwanted interactions with the local RADIUS server or any other intermediary RADIUS server.

Event 3: If the Home Entity wishes to use EAP-TLS to authenticate users, each user must have their own certificate.

Event 4: If the Home Entity wishes to use EAP-TTLS to authenticate users, the client provides the user name and password protected by the TLS record phase. The use of the TLS record phase is equivalent to the use of SSL for protecting web pages. Only the Home Entity is able to receive the user name and password. This step is protected from unwanted interactions with the local RADIUS server or any other intermediary RADIUS server.

Event 5: On successful authentication, the home RADIUS server authorizes the AP to provide a connection to the client and can also provide a session specific WEP key and configure the AP with an interval to change the WEP key. If this change occurs at sub-second intervals, WEP is resistant to known WEP attack. It is only at this step that the client has a network connection.

Event 6: The AP acknowledges the service authorization with a RADIUS Accounting-Request message containing an Acct-Status-Type Attribute with the Value field set to "Start" (1). This starts the timing of the user's session.

Event 10: The AP should generate a RADIUS Accounting-Request message containing an Acct-Status-Type Attribute with the Value field set to "Interim-Update" (3) at intervals specified by the home RADIUS server in Event 5. When generated by the AP, this periodic accounting is created without the overhead of additional authentication messages.

Event 12, 13: The AP should generate a RADIUS Accounting-Request message containing an Acct-Status-Type Attribute with the Value field set to "Stop" (2) when the user's client disconnects (disassociates) from the AP. This provides an accurate measure of the connection duration. If the user's disconnection is due to interference or a weak signal, a new authentication process is started when a connection is reestablished.

802.1x Considerations

The credentials required during the 802.1x Authentication and Accounting Process described above will depend to the authentication method selected by the user or as required by the Home Entity. The following issues should be considered:

First Time User

The user will be required to install an 802.1x networking client to use the 802.1x authentication methods. It is expected that the 802.1x client will be (a) provided as part of the networking driver when they purchase an 802.11b adapter, (b) provided as part of the "dialer" from their Home Entity, (c) purchased separately, or (d) provided as part of their operating system. Initially, it is expected that some WISPs will be distributing the 802.1x clients to simplify identifying affiliate Hotspot Operators and making the appropriate SSID entry.

Authentication methods

It is RECOMMENDED that the Home Entity select either 802.1x/EAP-TLS or 802.1x/EAP-TTLS. 802.1x/EAP-TTLS can be used if the users are being authenticated with user names and passwords or 802.1x/EAP-TLS can be used if certificates are used to authenticate the user.

Both methods have the identical technical requirements of the networking hardware, of the RADIUS protocols, and of any RADIUS servers that may exist between the Hotspot Operator and the Home Entity. The distinction between EAP-TLS and EAP-TTLS are handled by the user's wireless networking client and the Home Entity's RADIUS server, both managed by the Home Entity.

The choice of EAP-TLS or EAP-TTLS does affect the user's experience. The use of EAP-TLS requires the Home Entity to distribute certificates to each individual user. The use of the certificate and the safe keeping of the user's private key will depend of the vendor of the wireless client. In the case of EAP-TTLS, individual user certificates are not required. Instead, EAP-TTLS allows the use of passwords, tokens or other legacy authentication methods. The passwords and tokens may be the same ones in use for dial-up Internet roaming.

By encrypting the full NAI (user's identification), EAP-TTLS disrupts services that depend on the ability of a broker to count the number of unique NAI's serviced. Other third-party services that rely on user identification for policy enforcement and service selection will also be disrupted.

Welcome Pages

If specified by the RADIUS/AAA server, the 802.1x-networking client automatically launches the browser to display the welcome page. Since the RADIUS/AAA server may determine the Welcome Page URL, a rich range of welcome pages can be matched to the user's service preferences.

Logoff Functionality

The Hotspot Operator and the Home Entity require a means to measure the time the user is connected to the network. It is REQUIRED that the 802.1x hardware use RADIUS accounting messages to report the subscriber usage. Usage is then automatically reported with RADIUS start sessions at the completion of a successful authentication and a RADIUS stop session marks a disconnect (802.11b disassociate). The end of a session can be triggered by (a) user explicitly logging off through their wireless client, (b) a disconnect triggered by a maximum connection timer at the access, (c) a disconnect triggered by a exceeding the inactivity time limit at the access point, or (d) a loss of connection by the client going out of range.

Automatically Establishing a Connection

It is possible to automatically manage the connection process without user intervention. In general, a higher degree of automation is viewed as an improvement of the user's experience. However, there are a few areas that need careful consideration: (a) will the user be confronted with unexpected usage charges, (b) in a location with more than one Hotspot Operator, will the right Hotspot Operator be selected, and (c) how to prevent unauthorized network usage if the user's laptop is stolen.

Support for Protocol Extensions

If the roaming user is to utilize the 802.1x access method, the hotspot operator must support the 802.1x access method and the entire AAA infrastructure including the Hotspot Operator, Roaming Intermediaries, and Home Entities MUST support implementation of RADIUS/EAP protocol extensions [RFC2869], including EAP messaging as a RADIUS proxy attribute, as part of the AAA infrastructure. Guidelines for implementing RADIUS functionality over 802.1x and 802.11 solutions have been discussed in detail by various IETF working groups [8021x].

Appendix B – Re-Authentication using PANA

Requirements for Re-Authentication using PANA

Connection hijacking may be used not only to impersonate a user by taking over their connection while they're active (a user may leave without performing explicit logout), but also after they leave, an unscrupulous provider may seize that connection and hold it open in order to increase billing time. In order to prevent connection hijacking, periodical re-authentication with mutual authentication SHOULD be performed when performing usage-based accounting. In addition, the periodic re-authentication SHOULD be performed locally between client and the network, if the re-authentication is performed

with a short internal (e.g., less than 5 minutes) in order not to increase AAA signaling traffic exchanged in the core network. The periodic re-authentication can also be used for detection of client disconnection. The following Working Group exists the IETF (Internet Engineering Task Force) to develop a new protocol:

~ PANA ~
(Protocol for carrying Authentication for Network Access), which is able to support such a periodical and local re-authentication capability. One of the possible PANA usage scenarios is described as follows.

- The client obtains IP address via DHCP.

- The client performs PANA with the hotspot network. PANA carries EAP message as does PPP and 802.1X.

  The EAP message carried in PANA message is extracted at the hotspot network and passed to the RADIUS entity. Similarly, the EAP message created by the Home Entity and carried in the RADIUS message is extracted at the hotspot network and passed to PANA entity.

  Some EAP algorithm such as EAP-GSS-IAKERB and EAP-SRP supports, in addition to authentication, distribution of a session key that is created by the Home Entity to the client. A copy of the session key is also distributed from the Home Entity to the hotspot via RADIUS.

- Based on the session key temporarily shared between the client and hotspot, PANA re-authentication is periodically performed between them without going all the way back to the Home Entity.

Note that the PANA solution can work even for a browser client if the PANA software is written in JAVA script and the client downloads the script from the hotspot via HTTP and runs it.

Appendix C – Enhancing the User Experience: The Smart Client

The Universal Access Method enables a wireless user with an ordinary web browser to log in and use the network of an arbitrary Hotspot Operator. However, the UAM User's Experience described in the Access Method section depends heavily upon the user presiding over the login process to make decisions, click buttons, and manually enter credentials into web pages. There are many situations where this amount of user interaction is undesirable. 802.1x promises to greatly simplify this process in the future, but few client platforms currently support 802.1x. Therefore, it is important to define how a more simplified and seamless user experience can be achieved based on current client platforms.

If a WISP creates a customized client, that client can automatically configure the SSID, login to the WISP's network, and access other WISP-specific services without user intervention. Such a customized client can provide a "one click" experience to the user. However, if a customized client roams onto another WISP's network, it is unlikely to work correctly. Many "tacit" assumptions about how to log in to the Home Entity's network may be invalid on the WISP.

The solution to this problem is for WISPs to adopt common mechanisms to support a Smart Client capable of "one click" login to arbitrary WISP networks. There are two viable approaches for defining such mechanisms. One possibility is to define separate login mechanisms from the Universal Access Method, using whatever protocols are deemed appropriate. Another possibility is to use the same Universal Access Method mechanisms but to programmatically drive use of those mechanisms on the user's behalf. In other words, the Smart Client would use the same HTTP interface as an interactive user would. Because current practice already supports the Universal Access Method, WISPr recommends the

latter approach.

Given that the Smart Client will use the UAM HTTP interface, there are some additional architectural choices to be made. Since the user is not available to guide navigation through the login pages, the Smart Client must be configured to understand the structure of the login process to complete it successfully. There are at least three possibilities:

- WISPs adopt a single common login process using standard, universal login and logout URLs that the WISP automatically redirects onto its site-specific URLs.
- WISPs standardize the login process but publish WISP-specific login and logout URLs. The Smart Client becomes responsible for obtaining and using the correct URL for the WISP. This in turn requires the Smart Client to be able to discover the identity of the WISP prior to login.
- The Smart Client extracts descriptive data from the welcome and/or login pages. It subsequently uses that information to configure and direct its login process. Such descriptive data would likely be encoded in XML and advertised through a reference on the welcome and/or login page. The XML protocol is specified in The Smart Client to Access Gateway Interface Protocol Appendix.

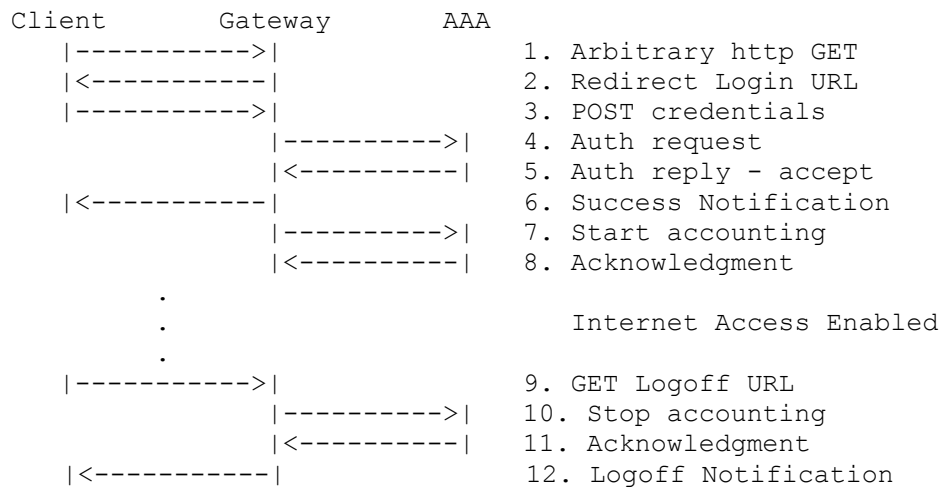
Appendix D – The Smart Client to Access Gateway Interface Protocol

Client Integration

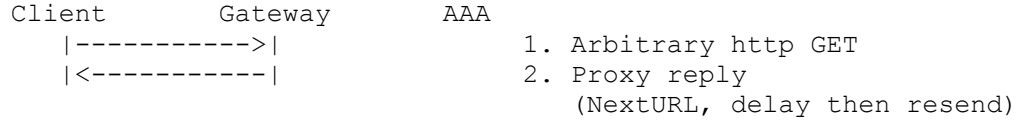
This appendix discusses the third of the suggested UAM HTTP interfaces discussed in the Smart Client Appendix, allowing the Smart Client and Access Gateway to negotiate authentication URLs. This interface is implemented through the use of client-initiated, secure HTTP message exchanges. TCP connections are requested to ports 80 and 443 unless otherwise indicated. HTTP version 1.0 is specified due to its simplified header formats.

The following interaction diagrams represent the access procedure protocol from the perspective of the Smart Client.

Login Request: Successful Case



Login Request: Successful Case With Proxy Reply



```
        |----------->|              3. Http GET to NextURL
        |<-----------|              4. Redirect Login URL
        |----------->|              5. POST credentials
                     |---------->|  6. Auth request
                     |<----------|  7. Auth reply - accept
        |<-----------|              8. Success Notification
                     |---------->|  9. Start accounting
                     |<----------|  10. Acknowledgment
              .
              .                        Internet Access Enabled
              .
        |----------->|              11. GET Logoff URL
                     |---------->|  12. Stop accounting
                     |<----------|  13. Acknowledgment
        |<-----------|              14. Logoff Notification
```

Login Request: Successful Case With Polling

```
 Client       Gateway       AAA
    |----------->|              1. Arbitrary http GET
    |<-----------|              2. Redirect Login URL
    |----------->|              3. POST credentials
                 |---------->|  4. Auth request
    |<-----------|              5. Auth Pending
    |----------->|              6. GET to polling URL
    |<-----------|              7. Auth pending, delay then refresh
                 |<----------|  8. Auth reply - accept
    |----------->|              9. GET to polling URL
    |<-----------|              10. Success Notification
                 |---------->|  11. Start accounting
                 |<----------|  12. Acknowledgment
          .
          .                        Internet Access Enabled
          .
    |----------->|              13. GET Logoff URL
                 |---------->|  14. Stop accounting
                 |<----------|  15. Acknowledgment
|<-----------|              16. Logoff Notification
```

Login Request: Reject

```
 Client       Gateway       AAA
    |----------->|              1. Arbitrary http GET
    |<-----------|              2. Redirect Login URL
    |----------->|              3. POST credentials
                 |---------->|  4. Auth request
                 |<----------|  5. Auth reply - reject
    |<-----------|              6. Failure Notification
```

Login Request: Reject With Polling

```
 Client       Gateway       AAA
    |----------->|              1. Arbitrary http GET
    |<-----------|              2. Redirect Login URL
    |----------->|              3. POST credentials
                 |---------->|  4. Auth request
    |<-----------|              5. Auth Pending
    |----------->|              6. GET to polling URL
```

```
|<-----------|                7. Auth pending, delay then refresh
             |<-----------|    8. Auth reply - reject
|----------->|                9. GET to polling URL
|<-----------|                10. Reject Notification
```

Protocol Specifics

The Smart Client to Access Gateway protocol is implemented using XML. Presently, no assumption of standardized URLs is made. Rather, the protocol depends on using URL Redirection. Most access gateways already provide a redirect mechanism for users attempting to access the network via a web browser. Because most browsers do not yet have XML support, it is likely that the access gateway is returning an HTML page. In order to implement the XML protocol, the gateway may implement one of the following options:

- Embed all XML tags within an HTML comment to prevent interpretation by the web browser.
- Embed XML tags on the redirect page in HTML comments which redirect the Smart Client to a URL which implements a true XML protocol.

Due to the inherent weaknesses in present implementations of WEP, SSL is used to protect the subscriber's authentication credentials. In order to further protect the subscriber from rogue access points, it is necessary to have a well-defined certificate at the access gateway that the client can verify.

The protocol messages include a proxy notification message. This is not included in the protocol description, but identified, as some access gateways require it.

All messages from the access gateway to the client will contain both response codes and message types.

The message types shall be one of the following values:

Message Type	Message Meaning
100	Initial redirect message
110	Proxy notification
120	Authentication notification
130	Logoff notification
140	Response to Authentication Poll
150	Response to Abort Login

The response code shall be one of the following values:

Response Code	Response Meaning
0	No error
50	Login succeeded (Access ACCEPT)
100	Login failed (Access REJECT)
102	RADIUS server error/timeout
105	Network Administrator Error: Does not have RADIUS enabled
150	Logoff succeeded
151	Login aborted
200	Proxy detection/repeat operation
201	Authentication pending
255	Access gateway internal error

Smart Client HTTP GET to ORIGIN SERVER

The Smart Client shall perform an HTTP GET to a valid roaming site to initiate the access sequence.

When the client system is already authorized for access at the access gateway, the gateway shall pass the HTTP GET through to the connected public network and return no special response. This behavior is also required whenever a subscriber attempts access using the Smart Client while already authorized for access as a result of accepting the local terms and conditions on the access location web site (i.e., the user agreed to the standard service agreement for service at the access site and the authorized service period has not yet elapsed).

If the subscriber should navigate to the terms & conditions page on the web site at the access location while authorized for access via the Smart Client, the access gateway shall deliver a generic "you are already logged in" or other appropriate rejection in response to an authorization attempt.
When the client device is not currently authorized for access, the access gateway shall return an HTTP redirect (302) status message or an META HTTP-EQUIV="REFRESH" message. It is also possible for the access gateway to return a proxy message in reply to the initial HTTP GET operation. This will be covered in more detail below.

Redirect

When a redirect message is returned it shall contain both the address and the access procedure identification for login and logout as described in the table below. The information shall be contained within a valid HTML message, delimited appropriately with the <HTML> and </HTML> tags. The HTML message may contain other valid HTML message elements (e.g., HEAD, BODY, etc.).

Required Information name	Field format/value
Access procedure	<AccessProcedure> {*Procedure Version*} </AccessProcedure>
Location Identifier	<AccessLocation> *{Location ID}* </AccessLocation>
Location Name	<LocationName> *{User readable location name}* </LocationName>
Login URL	<LoginURL> *https://<site specific login URL>* </LoginURL>
Abort Login URL	<AbortLoginURL> *https://<site specific login URL>* </AbortLoginURL>
Message Type	<MessageType> *100* </MessageType>
Response	<ResponseCode> *{Response Code data}* </ResponseCode>

The location identifier specified uniquely identifies the device through which the access will occur. If this ID is a characteristic of the physical device, replacement of the device could modify the ID received from the access location. Accordingly, any device swaps should be reported to participating roaming network providers. This should be identical to the Location-ID vendor-specific attribute that is part of the *Authentication Request.*

The Smart Client can use the *LocationName* to describe to the user the location being connected to.

When all required parameters are not present, an internal malfunction of the access gateway shall be assumed and the Smart Client shall behave as though an internal gateway response code was received.

The *AbortLoginURL* is used by the client to inform the access gateway that some error has occurred during the login process. When this is received by the access gateway, every attempt should be made to abort the session cleanly and to never generate an accounting record.

{response code} shall be one of the values listed in the following table:

Response Code	Response Message
0	No error
105	Network Administrator Error: Does not have RADIUS enabled
255	Access Gateway internal error

Proxy

When a proxy message is returned it may contain an optional Delay parameter. The proxy message should only occur in response to either the initial HTTP GET at login, or to the initial HTTP GET to the LogoffURL. The information may be contained within a valid HTML message, delimited appropriately with the <HTML> and </HTML> tags. The HTML message may contain other valid HTML message elements (e.g., HEAD, BODY, etc.).

Information name	Field format/value	Required/ Optional
Message Type	<MessageType> *110* </MessageType>	Required
Response	<ResponseCode> *{Response Code data}* </ResponseCode>	Required
Next URL	<NextURL> *http://<site specific URL>* </NextURL>	Optional
Delay in seconds	<Delay> *{Number of seconds data}* </Delay>	Optional

When all required parameters are not present, an internal malfunction of the access gateway shall be assumed and the Smart Client shall behave as though an access gateway internal error response code was received.

When it receives the proxy message, the smart client should sleep for the number of seconds specified in the Delay parameter (none if it is not present) and then resend the HTTP GET. Note: The proxy message may occur multiple times.

If the optional <NextURL> is present, then the Smart Client should replace the URL it is using for the HTTP GET messages to this new URL. It is possible for this URL to be updated on each successive Proxy message. The last known value will be used if no <NextURL> is present in a given Proxy Message.

{response code} shall be one of the values listed in the following table:

Response Code	Response Message

200	Proxy detection/repeat operation

Authentication

The authentication phase of the protocol shall consist of an authentication request POST operation by the Smart Client followed by a HTTP 200 or HTTP 302 reply by the access gateway.

Authentication Request

The Smart Client shall send a secure HTTP POST operation to the login URL returned in the Redirect message. Since the post will be using https, it should be assumed that port 443 would be used if not specified otherwise as part of the LoginURL.

The POST parameters shall be as follows:

- **UserName**: the full user id including appropriate clearinghouse routing prefixes
- **Password**: the user's password
- **Button**: form button identifier
- **OriginatingServer**: the URL of the server to which the activation GET operation was directed

Field name	Field naming/format specification	Required/ Optional
User name input field	name="UserName" max size="128"	Required
Password input	name="Password" max size="128"	Required
Button Identifier	name="button" content="Login"	Required
Form Name	Name="FNAME" content="0" (numeral zero)	Required
Origin Server	Name="OriginatingServer" content={original server GET URL}	Required

Authentication Reply

The access gateway shall return an HTTP 200 meta refresh or HTTP 302 redirect reply to the authentication request. The reply shall contain an XML segment with the fields described in the table below. The information may be contained within a valid HTML message, delimited appropriately with the <HTML> and </HTML> tags. The HTML message may contain other valid HTML message elements (e.g., HEAD, BODY, etc.).

Information name	Field format/value	Required/ Optional
Message Type	<MessageType> 120 </MessageType>	Required
Response	<ResponseCode> *{Response Code Data}* </ResponseCode>	Required
Reply Message	<ReplyMessage> *{Reply Message Text}* </ReplyMessage>	Optional
Login results URL	<LoginResultsURL> *https://<site specific login URL>* </LoginResultsURL>	Optional
Logoff URL	<LogoffURL> *https://<site specific logoff URL>* </LogoffURL>	Optional*

The *LogoffURL* must be present in the authentication reply if the Response (response code) is "Login succeeded". It may contain session specific information if required by the access gateway.

{response code} shall be one of the values listed in the following table:

Response Code	Response Meaning
50	Login succeeded (Access ACCEPT)
100	Login failed (Access REJECT)
102	RADIUS server error/timeout
201	Authentication pending
255	Access Gateway internal error

The optional "*ReplyMessage*" returns text to the client that is taken from the RADIUS attribute *Reply-Message*. This allows the AAA server to provide a human readable reason for rejecting an authentication request.

The access gateway may choose to block on the authentication request and reply immediately to the user if the time-to-authenticate is expected to be low. Alternatively, if there are many concurrent authentication requests and/or the time-to-authenticate is very high, the gateway may choose to immediately return an "Authentication Pending" message causing the client to poll.

If the authentication reply is "Authentication Pending" (response code 201) then the Smart Client will begin polling the access gateway for the authentication results. This requires the inclusion of the optional "*LoginResultsURL*" in the authentication reply message.

Authentication Results Polling

If the authentication reply message returned "Authentication pending" then the client will enter the authentication-polling phase. The authentication-polling phase of the protocol shall consist of a series of HTTPS GET operations by the Smart Client followed by HTTP 200 or HTTP 302 replies by the access gateway. This implements an optional polling mechanism that allows the access gateway to optimize resources.

Authentication Poll

The client shall send a secure http GET to the "LoginResultsURL" that was returned in the authentication reply message. Since the post will be using https, it is assumed that port 443 will be used unless specified otherwise as part of the URL.

Response to Authentication Poll

The access gateway shall return an HTTP 200 meta refresh or HTTP 302 redirect reply to the authentication results poll. The reply shall contain an XML segment with the fields described in the table below. The information may be contained within a valid HTML message, delimited appropriately with the <HTML> and </HTML> tags. The HTML message may contain other valid HTML message elements (e.g., HEAD, BODY, etc.).

Information name	Field format/value	Required/ Optional
Message Type	<MessageType> 140 </MessageType>	Required

Response	<ResponseCode> *{Response Code Data}* </ResponseCode>	Required
Reply Message	<ReplyMessage> *{Reply Message Text}* </ReplyMessage>	Optional
Delay in seconds	<Delay> *{Number of seconds data}* </Delay>	Optional
Logoff URL	<LogoffURL> *https://<site specific logoff URL>* </LogoffURL>	Optional

The LogoffURL must be present in the response to authentication poll if the response (response code) is "Login succeeded". It may contain session specific information if required by the access gateway.

{response code} shall be one of the values listed in the following table:

Response Code	Response Meaning
50	Login succeeded (Access ACCEPT)
100	Login failed (Access REJECT)
102	RADIUS server error/timeout
201	Authentication pending
255	Access Gateway internal error

If the authentication is complete, then the response to the authentication poll will contain the authentication results. If not (response code 201), then it will request the client to delay for the number of seconds specified in the "Delay" field and then resend the HTTP GET to the "LoginResultsURL".

Abort Login

In the event that a protocol problem has occurred during the login process, the client will make a GET operation to the abort login URL followed by a HTTP 200 or HTTP 302 reply by the access gateway.

Abort Login Request

To abort a login, the Smart Client shall send a HTTP GET operation to the AbortLoginURL returned in the initial redirect message.

Abort Login Reply

The access gateway shall return an HTTP 200 meta refresh or HTTP 302 redirect reply to the abort login request. The reply shall contain an XML segment with the fields described in the table below. The information may be contained within a valid HTML message, delimited appropriately with the <HTML> and </HTML> tags. The HTML message may contain other valid HTML message elements (e.g., HEAD, BODY, etc.).

Information name	Field format/value	Required/ Optional
Message Type	<MessageType> 150 </MessageType>	Required

Response	<ResponseCode> {*Response Code Data*} </ResponseCode>	Required
Logoff URL	<LogoffURL> *https://<site specific logoff URL>* </LogoffURL>	Optional*

The *LogoffURL* must be present in the abort reply if the Response (response code) is "Login succeeded". It may contain session specific information if required by the access gateway. The connection should not be terminated in this case. If the client wishes to terminate the connection then it will send a logoff request to the logoff URL.

{response code} shall be one of the values listed in the following table:

Response Code	Response Meaning
50	Login succeeded (Access ACCEPT)
151	Login aborted
255	Access Gateway internal error

Logoff

The logoff phase of the protocol shall consist of a GET operation to the logoff URL by the Smart Client followed by a HTTP 200 or HTTP 302 reply by the access gateway.

Logoff Request

To initiate a logoff, the Smart Client shall send a HTTP GET operation to the Logoff URL returned in either the authentication reply or authentication poll reply message.

Logoff Reply

The access gateway shall return an HTTP 200 meta refresh or HTTP 302 redirect reply to the logoff request. The reply shall contain an XML segment with the fields described in the table below. The information may be contained within a valid HTML message, delimited appropriately with the <HTML> and </HTML> tags. The HTML message may contain other valid HTML message elements (e.g., HEAD, BODY, etc.).

Information name	Field format/value	Required/ Optional
Message Type	<MessageType>130</MessageType>	Required
Response	<ResponseCode>{*Response Code Data*}</ResponseCode>	Required

{response code} shall be one of the values listed in the following table:

Response Code	Response Meaning
150	Logoff succeeded
255	Access Gateway internal error

XML Schema

```
<?xml version="1.0" encoding="UTF-8"?>
<xs:schema xmlns:xs="http://www.w3.org/2001/XMLSchema"
elementFormDefault="qualified" attributeFormDefault="unqualified">
```

```
<xs:element name="WISPAccessGatewayParam">
  <xs:complexType>
    <xs:choice>
      <xs:element name="Redirect" type="RedirectType"/>
      <xs:element name="Proxy" type="ProxyType"/>
      <xs:element name="AuthenticationReply"
                  type="AuthenticationReplyType"/>
      <xs:element name="AuthenticationPollReply"
                  type="AuthenticationPollReplyType"/>
      <xs:element name="LogoffReply" type="LogoffReplyType"/>
      <xs:element name="AbortLoginReply" type="AbortLoginReplyType"/>
    </xs:choice>
  </xs:complexType>
</xs:element>
<xs:simpleType name="AbortLoginURLType">
  <xs:restriction base="xs:anyURI"/>
</xs:simpleType>
<xs:simpleType name="NextURLType">
  <xs:restriction base="xs:anyURI"/>
</xs:simpleType>
<xs:simpleType name="AccessProcedureType">
  <xs:restriction base="xs:string"/>
</xs:simpleType>
<xs:simpleType name="AccessLocationType">
  <xs:restriction base="xs:string"/>
</xs:simpleType>
  <xs:simpleType name="LocationNameType">
    <xs:restriction base="xs:string"/>
  </xs:simpleType>
<xs:simpleType name="LoginURLType">
  <xs:restriction base="xs:anyURI"/>
</xs:simpleType>
<xs:simpleType name="MessageTypeType">
  <xs:restriction base="xs:integer"/>
</xs:simpleType>
<xs:simpleType name="ResponseCodeType">
  <xs:restriction base="xs:integer"/>
</xs:simpleType>
<xs:simpleType name="ReplyMessageType">
  <xs:restriction base="xs:string"/>
</xs:simpleType>
<xs:simpleType name="LoginResultsURLType">
  <xs:restriction base="xs:anyURI"/>
</xs:simpleType>
<xs:simpleType name="LogoffURLType">
  <xs:restriction base="xs:anyURI"/>
</xs:simpleType>
<xs:simpleType name="DelayType">
  <xs:restriction base="xs:integer"/>
</xs:simpleType>
<xs:complexType name="RedirectType">
  <xs:all>
    <xs:element name="AccessProcedure" type="AccessProcedureType"/>
    <xs:element name="AccessLocation" type="AccessLocationType"/>
    <xs:element name="LocationName" type="LocationNameType"/>
    <xs:element name="LoginURL" type="LoginURLType"/>
    <xs:element name="AbortLoginURL" type="AbortLoginURLType"/>
    <xs:element name="MessageType" type="MessageTypeType"/>
    <xs:element name="ResponseCode" type="ResponseCodeType"/>
  </xs:all>
</xs:complexType>
<xs:complexType name="ProxyType">
  <xs:all>
```

```
            <xs:element name="MessageType" type="MessageTypeType"/>
            <xs:element name="ResponseCode" type="ResponseCodeType"/>
            <xs:element name="NextURL" type="NextURLType" minOccurs="0"
                                                          maxOccurs="1"/>
            <xs:element name="Delay" type="DelayType" minOccurs="0"
                                                      maxOccurs="1"/>
          </xs:all>
        </xs:complexType>
        <xs:complexType name="AuthenticationReplyType">
          <xs:all>
            <xs:element name="MessageType" type="MessageTypeType"/>
            <xs:element name="ResponseCode" type="ResponseCodeType"/>
            <xs:element name="ReplyMessage" type="ReplyMessageType"
                        minOccurs="0" maxOccurs="1"/>
            <xs:element name="LoginResultsURL" type="LoginResultsURLType"
                        minOccurs="0" maxOccurs="1"/>
            <xs:element name="LogoffURL" type="LogoffURLType"
                        minOccurs="0" maxOccurs="1"/>
          </xs:all>
        </xs:complexType>
        <xs:complexType name="AuthenticationPollReplyType">
          <xs:all>
            <xs:element name="MessageType" type="MessageTypeType"/>
            <xs:element name="ResponseCode" type="ResponseCodeType"/>
            <xs:element name="ReplyMessage" type="ReplyMessageType"
                        minOccurs="0" maxOccurs="1"/>
            <xs:element name="Delay" type="DelayType"
                        minOccurs="0" maxOccurs="1"/>
            <xs:element name="LogoffURL" type="LogoffURLType"
                        minOccurs="0" maxOccurs="1"/>
          </xs:all>
        </xs:complexType>
        <xs:complexType name="LogoffReplyType">
          <xs:sequence>
            <xs:element name="MessageType" type="MessageTypeType"/>
            <xs:element name="ResponseCode" type="ResponseCodeType"/>
          </xs:sequence>
        </xs:complexType>
        <xs:complexType name="AbortLoginReplyType">
          <xs:sequence>
            <xs:element name="MessageType" type="MessageTypeType"/>
            <xs:element name="ResponseCode" type="ResponseCodeType"/>
            <xs:element name="LogoffURL" type="LogoffURLType"
                        minOccurs="0" maxOccurs="1"/>
          </xs:sequence>
        </xs:complexType>
      </xs:schema>
```

Examples

The messages documented in this section are associated with their *originator*, either client or Access Gateway.

***Authentication Procedure Activation [client] to port 80 at arbitrary IP address* (xxx.yyy.zzz.eee)**

```
GET / HTTP/1.0<CR><LF><CR><LF>
```

Activation - Redirect Reply

```
<?xml version="1.0" encoding="UTF-8"?>
<WISPAccessGatewayParam
   xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
   xsi:noNamespaceSchemaLocation="http://www.acmewisp.com/WISPAccessGatewa
yParam.xsd">
```

```
    <Redirect>
      <AccessProcedure>1.0</AccessProcedure>
      <AccessLocation>12</AccessLocation>
      <LocationName>
        ACMEWISP,Gate_14_Terminal_C_of_Newark_Airport
      </LocationName>
      <LoginURL>http://www.acmewisp.com/login/</LoginURL>
      <AbortLoginURL>
        http://www.acmewisp.com/abortlogin/
      </AbortLoginURL>
      <MessageType>100</MessageType>
      <ResponseCode>0</ResponseCode>
    </Redirect>
  </WISPAccessGatewayParam>
```

Activation - Proxy Reply

```
  <?xml version="1.0" encoding="UTF-8"?>
  <WISPAccessGatewayParam
     xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
     xsi:noNamespaceSchemaLocation=
     "http://www.acmewisp.com/WISPAccessGatewayParam.xsd">
    <Proxy>
      <MessageType>110</MessageType>
      <NextURL>http://www.acmewisp.com/proxypoll</NextURL>
      <ResponseCode>200</ResponseCode>
      <Delay>5</Delay>
    </Proxy>
  </WISPAccessGatewayParam>
```

Authentication Request [client] via SSL

```
  POST /process HTTP/1.0
  …
  <CR><LF><CR><LF>
  button=Login&UserName=WISP1/joseph@company.com&Password=xxxxx&FNAME=0&Orig
  inatingServer=http://xxx.yyy.zzz.eee/
  <CR><LF>
```

Authentication Reply (Login Successful)

```
  <?xml version="1.0" encoding="UTF-8"?>
  <WISPAccessGatewayParam
       xmlns:xsi=http://www.w3.org/2001/XMLSchema-instance
       xsi:noNamespaceSchemaLocation="http://www.acmewisp.com/WISPAccessGate
  wayParam.xsd">
    <AuthenticationReply>
      <MessageType>120</MessageType>
      <ResponseCode>50</ResponseCode>
      <ReplyMessage>Authentication Success</ReplyMessage>
      <LoginResultsURL>
        http://www.acmewisp.com/loginresults/
      </LoginResultsURL>
      <LogoffURL>http://www.acmewisp.com/logoff/</LogoffURL>
    </AuthenticationReply>
  </WISPAccessGatewayParam>
```

Authentication Reply (Login rejected)

```
  <?xml version="1.0" encoding="UTF-8"?>
  <WISPAccessGatewayParam
       xmlns:xsi=http://www.w3.org/2001/XMLSchema-instance
       xsi:noNamespaceSchemaLocation="http://www.acmewisp.com/WISPAccessGate
  wayParam.xsd">
    <AuthenticationReply>
      <MessageType>120</MessageType>
```

```
            <ResponseCode>100</ResponseCode>
            <ReplyMessage>Invalid Password</ReplyMessage>
            <LoginResultsURL>
              http://www.acmewisp.com/loginresults/
            </LoginResultsURL>
            <LogoffURL>http://www.acmewisp.com/logoff/</LogoffURL>
          </AuthenticationReply>
        </WISPAccessGatewayParam>
```

Authentication Reply (Login failed – unexpected RADIUS protocol error)

```
        <?xml version="1.0" encoding="UTF-8"?>
        <WISPAccessGatewayParam
             xmlns:xsi=http://www.w3.org/2001/XMLSchema-instance
             xsi:noNamespaceSchemaLocation="http://www.acmewisp.com/WISPAccessGate
        wayParam.xsd">
          <AuthenticationReply>
            <MessageType>120</MessageType>
            <ResponseCode>102</ResponseCode>
            <ReplyMessage>RADIUS Error</ReplyMessage>
            <LoginResultsURL>
              http://www.acmewisp.com/loginresults/
            </LoginResultsURL>
            <LogoffURL>http://www.acmewisp.com/logoff/</LogoffURL>
          </AuthenticationReply>
        </WISPAccessGatewayParam>
```

Authentication Reply (Login failed – internal access gateway error)

```
        <?xml version="1.0" encoding="UTF-8"?>
        <WISPAccessGatewayParam
             xmlns:xsi=http://www.w3.org/2001/XMLSchema-instance
             xsi:noNamespaceSchemaLocation="http://www.acmewisp.com/WISPAccessGate
        wayParam.xsd">
          <AuthenticationReply>
          <MessageType>120</MessageType>
          <ResponseCode>255</ResponseCode>
            <ReplyMessage>Access Gateway Error</ReplyMessage>
            <LoginResultsURL>
     http://www.acmewisp.com/loginresults/
    </LoginResultsURL>
            <LogoffURL>http://www.acmewisp.com/logoff/</LogoffURL>
          </AuthenticationReply>
        </WISPAccessGatewayParam>
```

Authentication Reply (Polling)

```
        <?xml version="1.0" encoding="UTF-8"?>
        <WISPAccessGatewayParam
             xmlns:xsi=http://www.w3.org/2001/XMLSchema-instance
             xsi:noNamespaceSchemaLocation="http://www.acmewisp.com/WISPAccessGate
             wayParam.xsd">
          <AuthenticationPollReply>
            <MessageType>140</MessageType>
            <ResponseCode>201</ResponseCode>
            <ReplyMessage>Authentication Pending</ReplyMessage>
            <Delay>5</Delay>
            <LogoffURL>http://www.acmewisp.com/logoff/</LogoffURL>
          </AuthenticationPollReply>
        </WISPAccessGatewayParam>
```

Client-initiated Connection Termination (logoff) of Authenticated User

```
        GET {Logoff_URL} <CR><LF><CR><LF>
```

Logoff Reply(Logoff Successful)

```
<?xml version="1.0" encoding="UTF-8"?>
<WISPAccessGatewayParam
     xmlns:xsi=http://www.w3.org/2001/XMLSchema-instance
     xsi:noNamespaceSchemaLocation="http://www.acmewisp.com/WISPAccessGate
     wayParam.xsd">
  <LogoffReply>
    <MessageType>130</MessageType>
    <ResponseCode>150</ResponseCode>
  </LogoffReply>
</WISPAccessGatewayParam>
```

Logoff Reply (Logoff failed – Access Gateway internal error)

```
<?xml version="1.0" encoding="UTF-8"?>
<WISPAccessGatewayParam
     xmlns:xsi=http://www.w3.org/2001/XMLSchema-instance
     xsi:noNamespaceSchemaLocation="http://www.acmewisp.com/WISPAccessGate
     wayParam.xsd">
  <LogoffReply>
    <MessageType>130</MessageType>
    <ResponseCode>255</ResponseCode>
  </LogoffReply>
</WISPAccessGatewayParam>
```