Wi-Fi CERTIFIED Passpoint®
Deployment Guidelines
Rev 1.2

February 28, 2019

WI-FI ALLIANCE PROPRIETARY – SUBJECT TO CHANGE WITHOUT NOTICE

The following document and the information contained herein regarding Wi-Fi Alliance programs and expected dates of launch are subject to revision or removal at any time without notice. THIS DOCUMENT IS PROVIDED ON AN "AS IS", "AS AVAILABLE" AND "WITH ALL FAULTS" BASIS. WI-FI ALLIANCE MAKES NO REPRESENTATIONS, WARRANTIES, CONDITIONS OR GUARANTEES AS TO THE USEFULNESS, QUALITY, SUITABILITY, TRUTH, ACCURACY OR COMPLETENESS OF THIS DOCUMENT AND THE INFORMATION CONTAINED IN THIS DOCUMENT.

© 2019 Wi-Fi Alliance. All Rights Reserved.

Table of Contents

© 2019 Wi-Fi Alliance. All Rights Reserved.

© 2019 Wi-Fi Alliance. All Rights Reserved.

© 2019 Wi-Fi Alliance. All Rights Reserved.

© 2019 Wi-Fi Alliance. All Rights Reserved.

Table of Figures

List of Tables

© 2019 Wi-Fi Alliance. All Rights Reserved.

1. Introduction

This document provides guidelines and recommended best practices for *deployment* of features contained in the Wi-Fi CERTIFIED Passpoint® certification program. The guidelines in this document are not mandatory for equipment certification; however, their use will contribute toward realizing maximum benefit from certified equipment. Readers are referred to the Hotspot 2.0 Specification [2] for requirements on access points, mobile devices, Hotspot Operators and Home SPs.

1.1 Terminology

The Passpoint certification program is based on technology defined in the Wi-Fi Alliance Hotspot 2.0 Specification. Products that have passed certification testing according to the Hotspot 2.0 test plan may use the Passpoint name.

Throughout the paper, the term “mobile device” refers to any mobile device that has been certified under the Passpoint and the Wi-Fi Protected Access® 2 (WPA2™) - Enterprise certification programs, except when the term “legacy mobile device” is used.

1.2 Scope

This guide covers the deployment and operation of infrastructure and mobile devices that have successfully completed testing under the Wi-Fi CERTIFIED Passpoint program. Topics include reference architectures, security recommendations, configuration and provisioning recommendations for hotspot-access network equipment (including Access Network Query Protocol [ANQP] servers) and mobile devices, guidance for interoperability of certified equipment and legacy equipment in the same hotspot deployment.

The Wi-Fi Alliance White Paper describes the market and applications of the Passpoint program (see [1]).

1.3 Related Documents

Document	Date	Location
[1] Wi-Fi CERTIFIED Passpoint™: An essential and strategic solution for service provider Wi-Fi® deployments	October 2014	http://www.wi-fi.org/passpoint
[2] Wi-Fi Alliance Hotspot 2.0 Specification	February 2019	http://www.wi-fi.org/passpoint
[3] IEEE 802.11-2012, Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications	March 2012	http://standards.ieee.org/getieee802/download/802.11-2012.pdf
[4] Wi-Fi CERTIFIED WPA2 with Protected Management Frames	January 2012	https://www.wi-fi.org/certification/programs
[5] 3GPP TS 23.003 Numbering, Addressing and Identification	March 2012	http://www.3gpp.org/ftp/Specs/html-info/23003.htm
[6] International Code Council, Inc., “International Building Code 2006”	November 2006	http://www.iccsafe.org/Store/Pages/Product.aspx?id=3000X06

© 2019 Wi-Fi Alliance. All Rights Reserved.

Document	Date	Location
[7] Authorized OSU Certificate Authority (CA) Vendors		https://www.wi-fi.org/certification/certificate-authority-vendors.
[8] Wi-Fi Alliance Hotspot 2.0 (Release 2) Online Sign-Up Certificate Policy Specification	August 2014	http://www.wi-fi.org/passpoint
[9] Passpoint® Operator Best Practices for AAA Interface Deployment	Feb 2019	https://www.wi-fi.org/discover-wi-fi/wi-fi-certified-passpoint

1.4 Terms and Definitions

The following definitions are applicable to this specification:

Name	Definition
Access	A mobile device has access after it successfully associates and authenticates securely to the Wi-Fi Access Network.
Access Point	The Access Point (AP) is the device or set of devices that instantiate(s) the required logical functions including, security and authentication as defined in IEEE 802.11-2012. Additional control, user and management plane functions can also be included. Note: the term applies to both a single network element implementation and a multiple network element implementation (AP and AP controller).
ANQP Server	An advertisement server in the Hotspot Operator's network containing ANQP-elements or information that can be used to derive the required ANQP-elements. The information in the ANQP server can be obtained by the Access Network Query Protocol. An ANQP server can be co-located with an AP or in an external device. Throughout this specification where the text describes an ANQP-element as being provided by an AP, it is to be understood that the source of the message is an ANQP Server.
Captive Portal	A mechanism for Wi-Fi Hotspot network access where an HTTP request from a mobile device is redirected to a server for authentication.

© 2019 Wi-Fi Alliance. All Rights Reserved.

Name	Definition
Certificate Authority	A collection of computer hardware, software and the people who operate it. The CA is known by two attributes: its name and its public key. The CA performs four basic CA functions: 1. Issues certificates (i.e., creates and signs them). 2. Maintains certificate status information and issues certificate revocation lists (CRLs) 3. Publishes its current (unexpired) certificates and CRLs so users can obtain the information they need to implement security services. 4. Maintains archives of status information about the expired or revoked certificates it issued.
Discovery	A mobile device is performing discovery when it scans for networks with which to associate, and to find related information useful for network selection. During the discovery process, the mobile device is not yet associated to the Wi-Fi access networks it is scanning.
Gratuitous ARP	An ARP request or reply message, transmitted to the broadcast destination MAC address, that is not normally needed according to the ARP specification (see RFC 826) but is useful for other purposes, such as detecting duplicate IP address assignments or notifying other hosts of a change of IP address. Note: if such a message is transmitted with an individual destination MAC address (i.e., broadcast to unicast conversion), it is no longer considered to be a Gratuitous ARP by this specification.
Home SP	The SP with which a mobile device has a subscription and associated credentials. The Home SP bills the user and authenticates the mobile device.
Hotspot	A site that offers public access to packet data services (e.g., the Internet) via a Wi-Fi access network (AN).
Hotspot Operator	The entity that is responsible for the configuration and operation of the hotspot.
Registration Authority	A collection of computer hardware, software and the people who operate it. The RA is known by two attributes: its name and its public key. The RA is responsible for the verification of certificate contents for the CA.
Registration Data	The data necessary to sign up for a subscription; registration data typically includes selection of a rate plan, terms and conditions, subscriber's contact information and payment information (e.g., credit card, bank account number).

© 2019 Wi-Fi Alliance. All Rights Reserved.

Name	Definition
Service Provider	***An entity offering network services (from the perspective of the Hotspot Operator). Service Providers (SPs) are represented in the NAI Realm, 3GPP Cellular Network (in the form of a list of PLMN IDs) or Roaming Consortium ANQP-elements.***
Subscription remediation	The process of fixing a problem in the subscriber's subscription. This includes provisioning new credentials to a mobile device (e.g., due to expiration), updating the PerProviderSubscription MO on a mobile device (e.g., because data needs updating) or performing an online function to update the subscription (e.g., pay a delinquent bill). Note that in the latter example, no new credentials/data are provisioned to the mobile device.
Terms and Conditions Data	The data necessary to accept terms and conditions for network access. The data typically includes subscriber's contact information and an acceptance indication.

1.5 Acronyms

Term	Definition
3GPP	The 3rd Generation Partnership Project
AAA	Authentication, Authorization and Accounting
AES	Advanced Encryption Standard
ANQP	Access Network Query Protocol
AP	Access Point
ARP	Address Resolution Protocol
ASRA	Additional Step Required for Access
BSS	Basic Service Set
BSSID	Basic Service Set Identifier
DHCP	Dynamic Host Configuration Protocol
DLS	Direct Link Setup
DoS	Denial of Service

© 2019 Wi-Fi Alliance. All Rights Reserved.

Term	Definition
EAP	Extensible Authentication Protocol
EAP-AKA	EAP–Authentication and Key Agreement
EAP-AKA'	Improved EAP-Authentication and Key Agreement
EAP-SIM	EAP–Subscriber Identity Module
EAP-TLS	EAP–Transport Layer Security
EAP-TTLS	EAP–Tunneled Transport Layer Security
EPC	Evolved Packet Core
ESS	Extended Service Set
FQDN	Fully Qualified Domain Name
GAS	Generic Advertisement Service
GTK	Group Temporal Key
HD	High Definition
HESSID	Homogeneous Extended Service Set Identifier
HLR	Home Location Register
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
IP	Internet Protocol
IPv4	Internet Protocol Version 4
IPv6	Internet Protocol Version 6
IPsec	Internet Protocol Security
LMD	Load Measurement Duration
MAC	Media Access Control
MAP	Mobile Application Part
MCC	Mobile Country Code
MIB-II	Management Information Base II

© 2019 Wi-Fi Alliance. All Rights Reserved.

Term	Definition
MNC	Mobile Network Code
MS-CHAPv2	Microsoft Challenge-Handshake Authentication Protocol Version 2
MSDU	MAC Service Data Unit
NAI	Network Access Identifier
NAT	Network Address Translation
OCSP	Online Certificate Status Protocol
OI	Organizational Identifier
P2P	Peer-to-Peer
PLMN	Public Land Mobile Network
PMF	Protected Management Frames
PMK	Pairwise Master Key
PTK	Pairwise Transient Key
RADIUS	Remote Authentication Dial In User Service
RF	Radio Frequency
SIM	Subscriber Identity Module
SNMP	Simple Network Management Protocol
SP	Service Provider
SSID	Service Set Identifier
TDLS	Tunneled Direct Link Setup
TKIP	Temporal Key Integrity Protocol
TLS	Transport Layer Security
TTLS	Tunneled Transport Layer Security
UDP	User Datagram Protocol
UICC	Universal Integrated Circuit Card
USIM	Universal Subscriber Identity Module

© 2019 Wi-Fi Alliance. All Rights Reserved.

Term	Definition
VPN	Virtual Private Network
WAN	Wireless Area Network
WEP	Wired Equivalent Privacy
WPA2™	Wi-Fi Protected Access® 2

2. Reference Architectures

Reference architectures for deploying hotspots when using cellular network credentials, when using non-cellular network credentials follow or when the device does not possess a credential which can be used to access the Wi-Fi network.

2.1 Hotspot 2.0 Network Deployment using Cellular Network Credentials for Authentication

Network discovery and authentication includes the following steps (Figure 1):

1. Device detects Hotspot 2.0 indication in access point (AP) beacon frame.
2. Device queries ANQP server for 3rd Generation Partnership Project (3GPP) cellular network information and roaming consortium organizational identifiers (OIs).
3. Device matches the information and OIs received against its list of credentials and preferred networks.
4. Device automatically associates with Passpoint AP.
5. Device performs Institute of Electrical and Electronics Engineers (IEEE) 802.1X authentication to the home authentication, authorization and accounting (AAA) server using Extensible Authentication Protocol–Subscriber Identity Module (EAP-SIM), or EAP-Authentication and Key Agreement (EAP-AKA) or improved EAP-Authentication and Key Agreement (EAP-AKA').
6. Home AAA server communicates with home location register (HLR) using the Mobile Application Part (MAP).

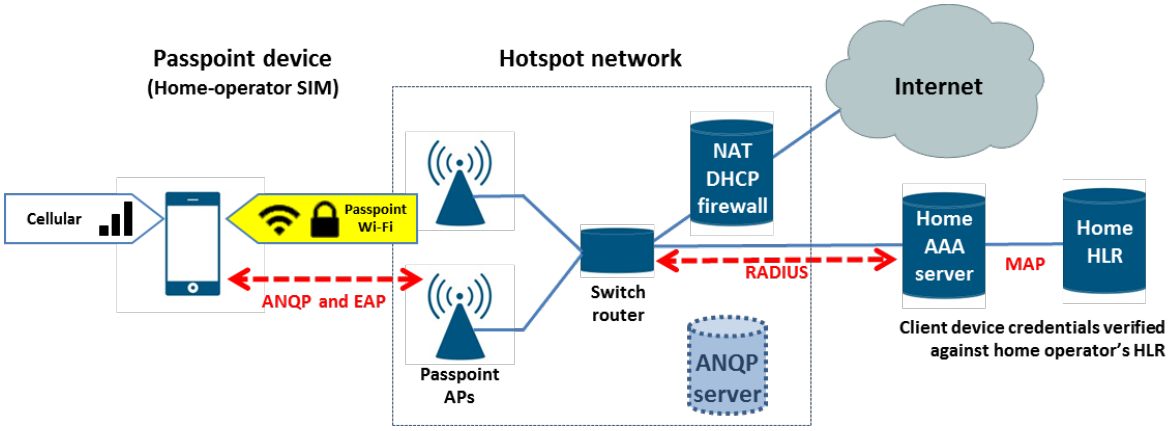

Figure 1: Passpoint hotspot reference architecture: SIM device

© 2019 Wi-Fi Alliance. All Rights Reserved.

2.2 Hotspot 2.0 Network Deployment using Non-cellular Network Credentials for Authentication

Network discovery and authentication includes the following sequence of steps (Figure 2):

1. Device detects Hotspot 2.0 indication in AP beacon frame.
2. Device queries ANQP server for network access identifier (NAI) realms and roaming consortium OIs.
3. Device matches the realms and OIs received against its list of credentials and preferred networks.
4. Device automatically associates with Passpoint AP.
5. Device performs IEEE 802.1X authentication to the Home AAA server using EAP-Transport Layer Security (EAP-TLS) or EAP-Tunneled TLS (EAP-TTLS) with MS-CHAPv2.

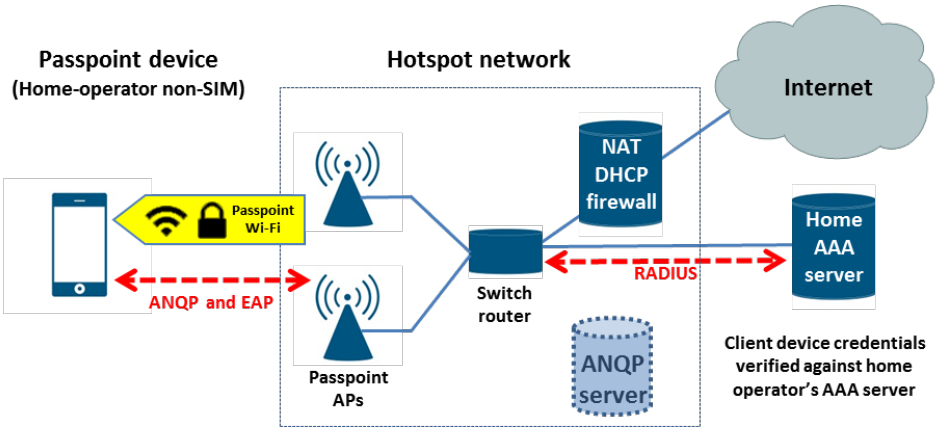

Figure 2: Passpoint hotspot reference architecture: non-SIM device

2.3 Hotspot 2.0 Release 2 Network Deployment When Network Credentials are Needed by the Mobile Device

Network discovery and credential/policy provisioning can be accomplished by the following sequence of steps (Figure 3):

1. Device detects Hotspot 2.0 indication in AP beacon frame.
2. Device queries ANQP server for network access identifier (NAI) realms and roaming consortium OIs.
3. Device attempts to match the realms and OIs received against its list of credentials and preferred networks, however there are no realms or OIs which match any of the device's credentials.
4. Device queries ANQP server for Network Authentication Type to determine if online sign-up is supported; if so, the device queries ANQP server for OSU Providers List.
5. The device, perhaps on request of the user, parses the OSU Providers List and displays the Friendly Name and/or Icon of the available SPs.
6. Upon the user selecting an SP, the mobile device associates to the OSU SSID, connects to that SP's OSU server. Then the user signs up for a subscription and the mobile device is provisioned with the PerProviderSubscription Management Object (PPS MO). If the SP provisions a username and password credential, it's contained within the PPS MO. If the SP provisions a client certificate, the SP's Certificate Authority creates the certificate and provisions it to the device; in this case, the PPS MO contains a reference to the client certificate. The PPS MO also contains device settings for use with the provisioned

© 2019 Wi-Fi Alliance. All Rights Reserved.

credential and optional network-selection policy which governs how the credential can be used.

7. Device automatically dis-associates with OSU SSID and associates to the Passpoint SSID.

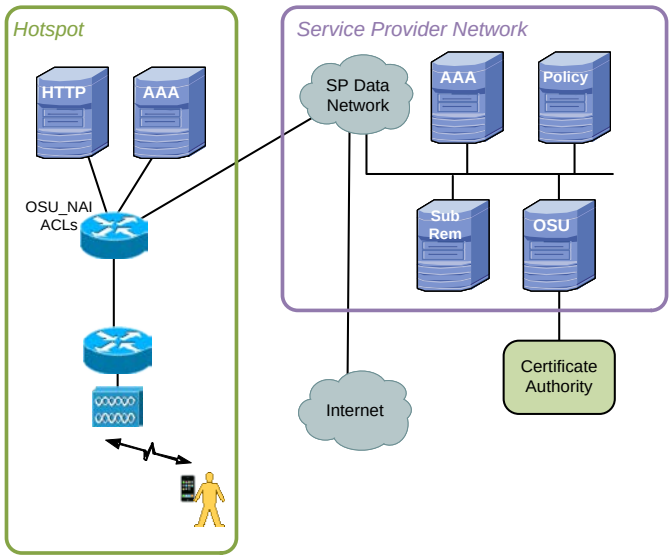

Figure 3: Example Service Provider Network with Subscription Servers

2.4 Hotspot 2.0 Release 2 and Domain Name Resolution

The Hotspot 2.0 Specification defines several URIs/URLs for use by Passpoint mobile devices. Hotspot Operators and Home SPs should take care to add records to their DNS servers, as appropriate, to ensure that server FQDNs (see Figure 3) will be resolvable by mobile devices.

Hotspot 2.0 technology uses the following URIs:

- Online sign-up server URIs, see section 3.4.1.
- Policy server URI, see section 7.1.
- Server trust root URLs, see section 8.8. Server trust root URLs can be defined for Policy servers, Subscription Remediation servers, and AAA servers.
- Subscription Remediation server URI (also used for updating subscription metadata in the PPS MO), see section 10.4.
- PPS MO IconURL (see Figure 59 in [2].)
- OCSP Responder URL (see Table 3 in [8]). Note: this is used by Wi-Fi infrastructure, not mobile devices.

3. Network Discovery and Selection

A mobile device is in one of the following four states: Discovery, Registration, Provisioning or Access, which are described below:

- Discovery: the mobile device is scanning for APs with which to associate and for related information useful for network selection.
- Registration: the mobile device is setting up a new account with an SP or Hotspot Operator. If the mobile device already has valid credentials for the selected hotspot and SP, this state is ephemeral.

© 2019 Wi-Fi Alliance. All Rights Reserved.

- Provisioning: the Wi-Fi infrastructure is establishing credential information and providing policy information to the mobile device. If the mobile device already has valid credentials for the selected hotspot and SP, this state is ephemeral.
- Access: the mobile device has successfully associated and authenticated with the hotspot and can access the services for which the user has subscribed.

These states are summarized in Figure 4:

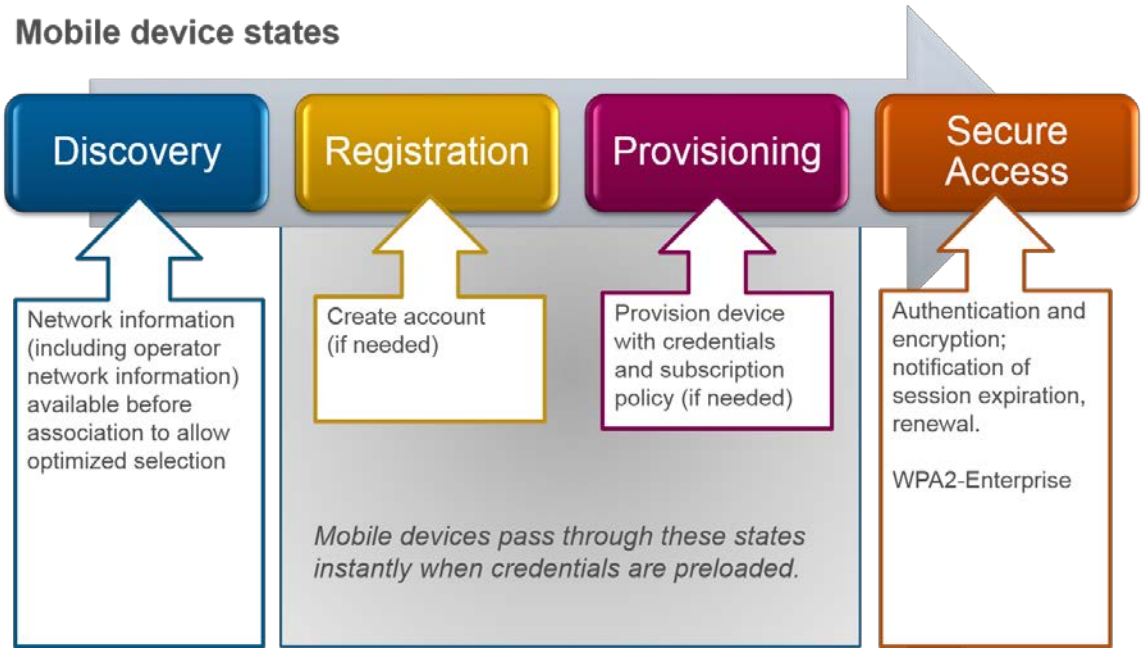

Figure 4: Provisioning Functionality

A mobile device uses ANQP to perform network discovery. The connection manager within the mobile device compares the information obtained from the hotspot via ANQP to the configuration information stored in the device, including Home SP policy and user preferences, to automatically select a hotspot network. The policy information is provisioned using methods that are outside the scope of the Passpoint certification.

A mobile device transmits one or more Generic Advertisement Service (GAS) query frames to determine key SP identification and authentication information. If required, the mobile device can perform further queries to obtain additional information and attempt to make more informed network selection decisions. In response, ANQP-elements are provided to the mobile device by either Passpoint APs or a combination of the AP and the ANQP server, as described above in sections 2.1 and 2.2. The ANQP response is generated using parameters configured by the Hotspot Operator.

Once the mobile device has automatically associated and mutually authenticated with the network, it has network access. The device may be connected through the hotspot to the Internet or the SP's core network; or, using functionality in the device, it can establish a connection through a virtual private network (VPN), to an enterprise or 3GPP network.

3.1 SP Identification and Authentication Methods: ANQP-elements and Beacon Elements

As defined by the Hotspot 2.0 Specification [2], hotspot networks are created by Hotspot Operators and hotspot SPs. A Hotspot Operator is an operator that deploys and operates an access network of publicly accessible Passpoint APs. A Home SP is one that provides network services and operates the AAA infrastructure required to authenticate subscribers. The Hotspot

© 2019 Wi-Fi Alliance. All Rights Reserved.

Operator and Home SP may be the same or different entities. SPs that can be accessed at a hotspot are referred to as the roaming partners for that hotspot. In all cases, the SP performing the authentication can provide its subscribers with AAA connectivity to its network through the hotspot.

SPs are advertised using 3GPP cellular network information, an NAI realm list, or a roaming consortium list.

3.1.1 3GPP Cellular Network ANQP-element

The 3GPP Cellular Network ANQP-element contains the cellular network identity based on public land mobile network (PLMN) information. This is to assist a mobile device with subscriber identity module (SIM) or universal SIM (USIM) credentials issued by a 3GPP home provider to establish whether an AP has a roaming arrangement with 3GPP SPs.

For each 3GPP SP that the Hotspot Operator provides service for, the operator configures the 3GPP cellular network information element as follows:

- The 3GPP cellular network information contains the cellular operator's PLMN ID.
- The PLMN ID is composed of the mobile country code (MCC) and the mobile network code (MNC) elements [7].

A mobile device with SIM or USIM credentials transmits a GAS/ANQP query for 3GPP cellular network information, and compares the response to the PLMD ID stored on its SIM or USIM to determine if the home cellular SP's network can be accessed through the Passpoint AP.

If the 3GPP cellular network ANQP element information matches any PLMN ID stored in the mobile device through either cellular operator pre-provisioning or other means, the mobile device prioritizes that AP for association based on the provisioned policies.

The mobile device knows the EAP method (EAP-SIM, EAP-AKA or EAP-AKA') required to authenticate against its Home SP (for example, the type of Universal Integrated Circuit Card [UICC]), and automatically uses it.

The mobile device's preconfigured user preferences and policy determine whether to associate to a Passpoint AP or to a non-Passpoint AP if both are available.

3.1.2 NAI Realm ANQP-element

The NAI Realm ANQP-element provides a list of NAI realms corresponding to the Home SPs that can authenticate a mobile device with username/password or certificate credentials. The NAI realm list can also be used for devices with SIM or USIM credentials. The NAI realm list also contains the realm of the Hotspot Operator if the operator is also a service provider.

Each NAI realm list entry may optionally include one or more EAP method subfields, which identify the EAP method(s) supported by that NAI realm for authentication. Mobile devices with authentication credentials provisioned by an SP know which EAP methods it supports, because the EAP method used is determined by the credential type(s) that the device stores for authentication: either EAP-TTLS for username/password or EAP-TLS for certificate credentials if using the NAI realm list, as described in Figure 2.

For each SP that the Hotspot Operator provides service for, it configures the NAI realm list as follows:

- Realms that can authenticate a mobile device's username/password or certificate credential are added to this list. This includes the realms of all the roaming partners accessible at the Passpoint AP. The realm of the Hotspot Operator is also included if that operator is also a Home SP.
- A realm corresponding to a PLMN ID may also be included in the NAI realm list (the PLMN ID for that realm also appears in the 3GPP Cellular Network ANQP-element). For example, the PLMN ID has the MCC and MNC fields set to 310 and 410, so the

© 2019 Wi-Fi Alliance. All Rights Reserved.

corresponding realm entry is wlan.mnc410.mcc310.3gppnetwork.org and epc.mnc410.mcc310.3gppnetwork.org [5].
- When a device has been provisioned with credentials by the SP providing the service, the device does not need to use the information in the EAP method list portion of the NAI Realm List.
- The EAP method list may be configured to support devices that do not know what EAP methods are used by a given SP. If configured, the EAP method authentication parameter type is configured as described in [3, section 8.4.4.10, Table 8-188].

A mobile device with username/password or certificate credentials may send a request to get the full list of NAI realms from an AP, or a sub-list of realms of interest using the NAI home realm query. The mobile device compares the received realms against realms contained in stored credentials.

For a mobile device with a SIM or USIM credential, realms can be obtained by the mobile device (as described above) from the Passpoint AP. While 3GPP cellular network information is typically used to quickly determine whether 3GPP credentials can be used to access a hotspot, a targeted NAI home query is an efficient alternative approach.

If the realm information matches what the mobile device has stored, the mobile device selects the Passpoint AP for association based on preconfigured preferences and policy stored in the mobile devices.

The mobile device's preconfigured user preferences and policy are used to decide whether to associate to a Passpoint AP or non-Passpoint AP if both are available.

3.1.3 Roaming Consortium ANQP-element and Beacon Elements

The Roaming Consortium ANQP-element and beacon elements provide a list of identifiers of roaming consortiums and SPs that are roaming partners of the hotspot service provider and that are accessible from the Passpoint AP. OI values assigned by the IEEE[1] identify the roaming consortium (i.e., a group of SPs with an inter-SP roaming agreements) or a single SP.

The Hotspot 2.0 Specification states that registering for an OI is mandatory for large (e.g., national or regional) hotspot SPs and optional for smaller SP (e.g., hotels).

The Hotspot Operator configures the Roaming Consortium ANQP-element as follows:

- If the hotspot allows authentication of mobile devices to the members of a roaming consortium, the operator adds the consortium's IEEE-assigned OI to the roaming consortium list.
- If the hotspot can provide authentication to a particular SP and if that SP has a roaming consortium OI assigned by IEEE, it adds that OI to the roaming consortium list.

The Hotspot Operator selects the OI values to be included in the roaming consortium element. The roaming consortium element is broadcast by the Passpoint AP in the beacon and transmitted in the probe response frames [3, section 8.4.2.98].

A mobile device with any type of credentials can query for the Roaming Consortium ANQP-element. The Passpoint AP assumes that the type of credentials in the mobile device for each OI is that required for the member of the roaming consortium from which the device obtains service. The SP will correlate credentials for a specific realm with an OI in the mobile device using standards-based or proprietary means that are outside the scope of this document. Alternatively, the mobile device may obtain OI information first, and then perform a full NAI GAS/ANQP query to determine the full realm name and required EAP method.

1 See http://standards.ieee.org/regauth/faqs.htm and http://standards.ieee.org/develop/regauth/oui36/index.html.

© 2019 Wi-Fi Alliance. All Rights Reserved.

A mobile device may query for a Roaming Consortium ANQP-element when previous GAS/ANQP queries for either 3GPP or NAI realm information have not provided sufficient information for network selection.

3.2 Hotspot Identification: ANQP-elements

3.2.1 Domain Name ANQP-element

The Domain Name ANQP-element provides a list of one or more domain names of the entity operating the hotspot network. It is possible that a Hotspot Operator might have more than one domain name that it uses to identify itself. For example, the domain names wlan.mnc410.mcc310.3gppnetwork.org, att.com, and attwireless.com all refer to the same SP, AT&T. All three can be contained in the Domain Name ANQP-element.

All Hotspot 2.0 Hotspot Operators possess a domain name and this domain name is configured by the Hotspot Operator in the Domain Name ANQP-element.

At the discretion of the Hotspot Operator, domain names in the domain name list may contain sub-domains.

The mobile device queries the domain name list via ANQP for preliminary screening of APs for association.

When selecting an AP, the mobile device preferentially chooses one operated by its Home SP, except when this selection is overridden by user preferences or policy.

The mobile device compares the fully qualified domain name (FQDN)[2] such as “wi-fi.org” in its credential or a pre-provisioned FQDN[3] against the domain name list retrieved from the AP to determine if it is connecting to a hotspot that is operated by its Home SP. For the purposes of identifying the SP, a match is defined as a suffix match of the domain name with the FQDN. For example, a mobile device whose Home SP is XYZ would consider both coffeshop.xyz.com and eatery.xyz.com to be operated by its Home SP, because they both refer to service provider XYZ (i.e. their suffix matches xyz.com).

The mobile device uses the presence of the domain name of any SP to determine if access to that SP network through this AP is considered home or roaming access. If the SP’s name is not in the domain name list but is in the realm list, then a mobile device that chooses that SP will be considered to be roaming.

3.2.2 Venue Name ANQP-element

The Venue Name ANQP-element provides additional information (i.e., metadata) about the hotspot. For instance, it may include the following information:

XYZ Stadium
Home of Major League Sports
123 Main Street
City, State, Zip Code
Telephone: 123 456 7890

The Hotspot Operator can configure the information in the AP to describe the venue in which the hotspot is located. Typically, when there are multiple Passpoint APs in a given venue, the Hotspot Operator configures all of them with the same venue name. However, different venues (e.g., two

2 Technically, the credential has a realm, not an FQDN; however, in some cases the realm used for authentication matches the SP's FQDN (e.g., user@wi-fi.org; "wi-fi.org" is both the Wi-Fi Alliance’s realm and its FQDN).

3 The FQDN is provisioned using a method that is outside the scope of that specification, see [2].

© 2019 Wi-Fi Alliance. All Rights Reserved.

coffee shops) having Wi-Fi access provided by the same Hotspot Operator may have different venue names even though they may share a service set identifier (SSID) name.

Hotspot Operators can list venue names in multiple languages and can include, for instance, the venue name information in the languages used by their frequent visitors. The mobile device selects the preferred language for the information to be displayed to the user.

The mobile device may obtain venue name information through an ANQP query to assist the user during manual hotspot selection, if this is required. The mobile device implementation determines whether mobile device displays the venue name information.

3.2.3 Venue Info Field

The Venue Info Field in the Venue Name ANQP-element provides additional information about the group and type of hotspot venue. The group and type descriptors are drawn from the International Building Code [6].

The allowable group values are defined in [3, section 8.4.1.34, Table 8-52]. The Hotspot Operator configures the Passpoint AP with one of the venue group description values, such as “assembly” or “business,” from that table.

The allowable type values are defined in [3, section 8.4.1.34, Table 8-53]. The Hotspot Operator configures the AP with one of the venue description values, such as “arena” or “stadium,” from that table.

The mobile device may use the venue info field in the Hotspot 2.0 beacon or Venue Name ANQP-element as defined in [3, section 8.4.4.4] to assist the user during manual hotspot selection, when it is required. Whether the mobile device displays the venue information is determined by the device's implementation.

Following the example in section 3.2.2, the venue group would be set to “1” (assembly) and venue type would be set to “2” (stadium).

3.2.4 Operator's Friendly Name Hotspot 2.0 ANQP-element

The Operator Friendly Name Hotspot 2.0 ANQP-element [2] provides the friendly name of the Hotspot Operator. Operator friendly names can be provided in multiple human languages. The Hotspot Operator configures this information in the Passpoint AP.

The mobile device may obtain the operator friendly name via GAS/ANQP queries to assist the user during manual hotspot selection to provide the operator name of the connected hotspot to the user, or for any other reason. Whether a mobile device displays the operator friendly name is up to the implementation.

3.3 Network Characteristics: ANQP-elements

3.3.1 IP Address Type Availability ANQP-element

The Internet Protocol (IP) Address Type Availability ANQP-element provides information about the IP address version and type that the Hotspot Operator uses and that would be allocated and available to a mobile device after it authenticates to the network.

The Hotspot Operator configures the information in the AP to reflect the IP address configuration of the wireless area network (WAN) router, the Dynamic Host Configuration Protocol (DHCP) server if present[4], and the firewall behind the AP.

4 Note that a DHCP server is not needed when IP addresses are assigned using IPv6 stateless address allocation.

© 2019 Wi-Fi Alliance. All Rights Reserved.

When the SSID provides direct access to a single core network (e.g., the 3GPP Evolved Packet Core [EPC]), IP Address Type ANQP element configuration may take into account the address type supported by the core network.

Available IP Version 4 (IPv4) and IPv6 address parameters are listed in Table 1. See also [3, section 8.4.4.9]:

Table 1: IPv4 and IPv6 Address parameters

Address parameter	Configuration	Condition for use
IPv4		
Public IPv4 address	Allowed	The hotspot allocates a public IPv4 address to the mobile device after association
Port-restricted IPv4 address	Not used[5]	
Single- network address translation (NAT) private IPv4 address	Allowed	The hotspot allocates a private IPv4 address to the mobile device after association[6]
Double-NATed private IPv4 address	Allowed	Access to a single core network is provided and the combination of the hotspot network and the core network allocates a double-NAT IPv4 address to the mobile device after association
Port-restricted public IPv4 address and single-NAT IPv4 address	Not used	
Port-restricted IPv4 address and double-NAT IPv4 address	Not used	
Not available	Allowed	The Hotspot Operator cannot allocate an IPv4 address to the mobile devices
Not known	Allowed	Address allocation is outside the Hotspot Operator's administrative control
IPv6		
IPv6 address	Allowed	The Hotspot Operator is able to natively route IPv6
Not available	Allowed	The Hotspot Operator is not able to natively route IPv6, even if the Hotspot Operator is able to assign

5 As of the date of the Deployment Guide's publication, the Internet Engineering Task Force (IETF) is working on how to port-restrict an IPv4 address.

6 IETF RFC1918, "Address Allocation for Private Internets," http://tools.ietf.org/html/rfc1918.

© 2019 Wi-Fi Alliance. All Rights Reserved.

Address parameter	Configuration	Condition for use
		IPv6 addresses to the mobile devices
Not known	Allowed	Address allocation is outside the Hotspot Operator's administrative control

The mobile device uses the IP address type availability information to make network selection decisions. For example:

- A mobile device that has only an IPv4 stack connects to a hotspot that supports IPv4.
- A mobile device that prefers to use IPv6 connectivity connects to a hotspot that supports IPv6, if one is available.
- If the mobile device sees a port-restricted indication, it can use WAN metrics information to decide if the services it intends to use will traverse the ports in the hotspot network.

3.3.2 WAN Metrics Hotspot 2.0 ANQP-element

The WAN Metrics Hotspot 2.0 ANQP-element provides information about the WAN link that connects the hotspot to the Internet.

The Hotspot Operator configures the parameters shown in Table 2 in the AP to reflect the egress interface from the hotspot to the Internet. If the egress interface is embedded in the AP, the AP may automatically provide some or all of the information [2, section 4.4].

Table 2: Configuration parameters

Parameter	Setting options
Link status	Link up Link down Link in test state
WAN link symmetry (whether link speed is the same in the uplink and downlink)	Symmetric Asymmetric
Downlink speed	Nominal, in kilobits/s
Uplink speed	Nominal, in kilobits/s

The Passpoint AP may also be capable of automatically providing the following additional (implementation-dependent) information [2, section 4.4]:

- Downlink load
- Uplink load
- At capacity: In this condition the AP won't allow additional mobile devices to associate.
- Load measurement duration (LMD): The LMD value, reported to the mobile device in the WAN Metrics Hotspot 2.0 ANQP-element, is the time interval over which the WAN interface device (e.g., edge router or AP) averages its load measurement. A recommended range for LMD is 1 to 15 minutes. The Hotspot Operator may vary the parameter based on its preferences and traffic and deployment characteristics. If Simple Network Management Protocol (SNMP) is used to deliver load information (e.g.,

© 2019 Wi-Fi Alliance. All Rights Reserved.

management information base II [MIB-II]), then the measurement interval will typically be 15 minutes.

The mobile device uses information from the WAN Metrics Hotspot 2.0 ANQP-element to make network selection decisions. For example, if a mobile device application (e.g., video streaming) requires a certain amount of throughput, the mobile device can determine if that throughput level is currently available from the hotspot before connecting. If the mobile device receives a WAN Metrics Hotspot 2.0 ANQP-element indicating the basic service set (BSS) is "at capacity," the mobile device will not associate with that AP.

3.3.3 Connection Capability Hotspot 2.0 ANQP-element

The Connection Capability Hotspot 2.0 ANQP-element provides information on the status of commonly used communication protocols and ports in the hotspot. For example, a firewall upstream of the AP may allow communication on certain IP protocol and port values while blocking communication on others. The permitted IP protocol and destination port number values are listed in [2, Table 5].

The Hotspot Operator should configure the AP with information regarding each of the commonly used protocol and port number values as either closed, open or unknown. Hotspot Operators should make reasonable efforts to ensure the value “unknown” is not used.

The mobile device uses connection capability information to make network selection decisions by determining which services are blocked or supported at the hotspot. For example:

- A TLS VPN application running on a mobile device requires IP protocol value 6 and port number 443. The mobile device will refrain from initiating the TLS VPN connection if traffic through port 443 is not permitted and TLS VPN is required.
- A mobile device using an Internet Protocol Security (IPsec) VPN (with or without User Datagram Protocol [UDP] encapsulation) requires the protocol/port values 17, 500; 17, 4500; and 50, 0 all to be open at the hotspot. If this is not the case, the device will not associate to the AP if availability IPsec VPN is required.

3.3.4 Operating Class Indication Hotspot 2.0 ANQP-element

The Operating Class Indication Hotspot 2.0 ANQP-element provides information on the channels and frequency band(s) used by the AP(s) in the hotspot. Operating classes are defined in [7, Table E-4].

Passpoint APs may be aware of operating class information (without additional configuration) based on the radio frequency (RF) band capabilities of the individual AP.

In a multi-AP hotspot venue, the Hotspot Operator may configure additional information describing the operating classes in use by other APs in the venue having the same SSID.

The mobile device may use operating class information to make network selection decisions. If a mobile device supports more than one frequency band (e.g., 5 GHz as well as 2.4 GHz), it may use this information to select a hotspot operating in the 5 GHz band if this is the preferred band and it is available.

3.3.5 Network Authentication Type ANQP-element

For Release 1 of the Hotspot 2.0 Specification [2], Passpoint APs are configured to not indicate an additional step required for access (ASRA) in the beacon. Correspondingly, the Network Authentication Type ANQP-element is not configured by the Hotspot Operator.

For Passpoint APs with Release 2 features, when at least one OSU provider is supported, the Network Authentication Type ANQP-element will have the Network Authentication Type Indicator having the value of “Online enrollment supported” set.

© 2019 Wi-Fi Alliance. All Rights Reserved.

3.4 Online Sign-up: ANQP-elements

The available Online Sign-up server information is advertised to the device by the OSU Providers List element in the ANQP response. From this list the device should display the friendly name of the available OSU Providers in the language preferred by the device, if available, or in the default language if the preferred language is not found. For mobile devices that support the display of icons, the device will determine from the available Icon(s) the best to display to the user. Once determined, the mobile device sends an Icon file request to the AP using an ANQP query message, The AP will respond to the Icon request with the an ANQP response containing the Icon binary data. If the file was not found or there was some other error the AP will respond to the device with the appropriate Download Status Code.

3.4.1 OSU Providers List ANQP-element

The OSU Providers List ANQP-element contains a list of entities that offer online sign-up service at the hotspot. Each OSU provider entry in the list will contain the OSU SSID, Friendly Name, URI of the OSU server, OSU Methods, and available Icon(s). The entry may also contain the NAI realm to be used for authentication in the case of OSU ESS (OSEN) and the OSU Service Description Duple(s).

The OSU SSID is the SSID that the device will associate and connect to when accessing the OSU server.

The OSU Provider Friendly Name is a list of one or more names in different human languages. This allows the device to display the OSU Friendly Name in alternate languages based on the language selected in the setting of the mobile device.

The URI is the OSU server URI and the OSU Method is the preferred list of encoding methods that the OSU server supports in order of priority.

The Available Icon(s) is a list of available Icon metadata that can be displayed by the mobile device. If the provider does not have an Icon, this list can be blank or zero in length. The Icon list contains the metadata for the available Icon files. The metadata defines the image size, language, image type, and file name. This information allows the mobile device to determine the best Icon to download as well as the file name of the Icon to retrieve from the network.

The NAI realm is used in cases where the OSU ESS (OSEN) SSID is configured. This allows the device to authenticate to the OSU OSEN SSID for access to the OSU server.

The OSU description Duple contains the SP's description of service offering. The content of the service description is left to the discretion of the SP; where appropriate, descriptions are intended to be provided in multiple human languages. An example service description is shown below:

```
Blue Telekom
Enjoy Wi-Fi access during your holiday at our 2,400
locations across Switzerland.  We have the fastest Wi-Fi
connections!  Connect up to 5 devices for 1 week: CHF 15.

Blau Telekom
Genießen Sie Wi-Fi-Zugang in Ihrem Urlaub in unserem 2.400
Standorten in der Schweiz. Wir haben die schnellsten Wi-Fi-
Verbindungen! Anschluss von bis zu 5 Geräte für 1 Woche: 15
CHF.

Bleu Telekom
Profitez de connexion Wi-Fi pendant vos vacances à nos
2.400 sites en Suisse. Nous avons les plus rapides
connexions Wi-Fi! Connecter jusqu'à 5 appareils pour 1
semaine: CHF 15.
```

© 2019 Wi-Fi Alliance. All Rights Reserved.

3.4.2 Icon Request & Response ANQP-elements

There is an ANQP exchange between the device and the AP when the mobile device is capable of displaying the OSU Icon. The mobile device determines which Icon file to download from the AP based on the OSU Icon metadata. The mobile device then sends an ANQP Query to the AP with the Icon request element containing the Icon filename. The AP will respond with an ANQP Response containing the Icon Binary element. The Icon Binary element contains the Download State Code, Icon Type Length, Type, Data Length, and the Icon Binary Data. The Download State Code will indicate to the mobile device if the file was found successfully, file was not found, or if an unspecified file error occurred.

The Icon Type Length and Type indicate the MIME media type of the binary file.

The Icon Data Length defines the size of the binary Icon data followed by the Icon Binary data.

The Icon Binary data will be verified against the corresponding OSU server certificate by comparing the SHA-256 hash of the binary data to the Icon hash in the OSU certificate.

3.5 Capability Query: ANQP-elements

The information in this section is provided for reference. The Hotspot Operator does not configure these parameters; they are obtained from data configured in the previous sections.

3.5.1 HS Query List Hotspot 2.0 ANQP-element

A mobile device sends a hotspot (HS) Query List ANQP-element to the Passpoint AP in a GAS query request to get information about multiple Hotspot 2.0 ANQP-elements simultaneously. In response, the Passpoint AP tells the mobile device how those parameters have been configured by the Hotspot Operator, as described in the previous sections.

3.5.2 HS Capability List Hotspot 2.0 ANQP-element

The HS Capability List ANQP-element is delivered by Passpoint APs in response to a corresponding GAS query, listing parameters configured by the Hotspot Operator, as described in the previous sections. The HS capability list element tells the mobile device what Hotspot 2.0 ANQP-elements are supported by the Passpoint AP, regardless of whether the element is optional or required by the Hotspot 2.0 Specification [2].

3.5.3 NAI Home Realm Query Hotspot 2.0 ANQP-element

A mobile device can use the NAI Home Realm Query Hotspot 2.0 ANQP-element to determine whether the NAI realms for which it has security credentials correspond to SPs or other entities whose networks or services are accessible at the hotspot.

The NAI home realm query includes only the NAI home realm name(s) for which the mobile device has credentials. In response to this query, a responding AP returns an NAI realm list, configured by the Hotspot Operator as described in the previous sections. The NAI realm list with which the AP responds includes only realms that exactly match the names in the query.

3.6 Other Beacon Elements

3.6.1 HESSID Information Element

In typical Wi-Fi deployments, if two APs have different SSIDs, they are considered to be different wireless networks. If two APs have the same SSID, they are considered to be part of the same wireless network. But because SSIDs are not globally administered, it is possible that two APs with the same SSID are, in fact, in different wireless networks. The homogeneous extended service set identifier (HESSID) element allows mobile devices to detect this condition. When two

© 2019 Wi-Fi Alliance. All Rights Reserved.

APs have the same SSID but from different wireless networks, the two networks have different HESSIDs.

The HESSID is included in the IEEE 802.11u interworking element present in beacon and probe response frames in Passpoint APs. The HESSID, a globally unique identifier, is used to give a single identifier for a group of APs connected to the same SP or other destination network(s).

The HESSID is a MAC address. The Hotspot Operator configures the HESSID value with the same value as the basic service set identifier (BSSID) of one of the APs in the network. All APs in the wireless network are configured with the same HESSID value.

In a Passpoint AP, where display of the SSID and the manual selection of the network have been replaced by automated discovery and selection, users do not need to see or use the HESSID and SSID during the network selection process. However, SSIDs are still required for interworking with legacy devices (Section 13).

The SSID is also necessary to enable mobility between APs within a hotspot, because the SSID for all APs in the hotspot needs to be the same to allow handoffs.

3.6.2 Access Network Type Field

The access network type field is automatically included in the IEEE 802.11u interworking element present in beacon and probe response frames in Passpoint APs. Mobile devices can use this information when selecting a hotspot. The access network types are as described in [3, Section 8.4.2.94, Table 8-174].

A Hotspot Operator configures the access network type field according to the type of hotspot being provided. Typically, this will be a "chargeable public network" or a "free public network." However, other access network types, such as "private network" or "private network with guest access," can also be used.

3.6.3 Internet Available Field

The Internet available field in the Interworking information element is included in the IEEE 802.11u interworking element present in beacon and probe response frames in Passpoint APs. The Hotspot Operator configures this field to inform the mobile device whether Internet access is available at a hotspot – which might not be the case in walled-garden environments, where the Hotspot Operator (for example, a museum) may limit Wi-Fi access to locally available content.

3.6.4 BSS Load Information Element

The BSS load information element is provided by Passpoint APs. This element contains information on channel utilization and the current number of associated devices on a given AP. The BSS load element is defined in [3, section 8.4.2.30]. The mobile device uses this information to take into account AP loading when selecting a network.

4. Registration

During registration, a mobile device sets up a new account with an SP or hotspot provider. This is typically followed immediately by provisioning a new credential and optionally network-selection policy[7].

[7] Every SP installing a credential has the option to install network-selection policy. Policy influences the mobile device's connection manager's choice of a Wi-Fi access network. Policy affects these choices only when the associated credential is being used for Wi-Fi access, not when the credential of any other SP is used.

© 2019 Wi-Fi Alliance. All Rights Reserved.

If a user already has an account with an SP and the mobile device for some reason doesn't have the associated credentials, the user just needs to identify their existing account (e.g., by logging in) and then mobile device provisioning can proceed. Mobile device provisioning is described in section 5. This situation can occur when the user just purchased a new device, or an existing device's persistent storage becomes corrupted (e.g., hard disk crash) and subsequently re-imaged. The user could have an existing account with an SP but the device never used the credential for Wi-Fi access (just website access).

4.1 Introduction to Online Sign-up

Mobile devices use online sign-up to accomplish registration. During online sign-up a mobile device registers with an SP, enabling a user to select a plan with which to obtain network access. During registration, an SP would typically collect contact information from the user as well as some form of payment for the subscription. SPs may offer free or paid subscriptions and time-limited or ongoing subscriptions according to their business needs.

A mobile device typically has several subscriptions gathered from multiple sources over time. For Passpoint mobile devices, the user sets the hierarchy of preference for subscriptions, or allows the mobile device to determine the preference of subscriptions. For example, a mobile device may be provisioned for:

- One or more user-provisioned networks (e.g. the user's home network, legacy hotspots from favorite venues)
- A Hotspot Operator-provisioned network (e.g. airport Wi-Fi Access Network, convention center, Wi-Fi aggregator)
- An SP's network (possibly pre-provisioned at activation)
- An enterprise-provisioned network from their employer

The elements comprising data provisioned to a mobile device after a subscription is established are:

- Access credential (e.g. username/password, client certificate, SIM)
- Home SP identifiers (e.g., their domain name and friendly name)
- Home network identifiers (see section 5.4)
- Other associated information, if required

An example network architecture for online sign-up is shown in Figure 3. Each SP network has an OSU Server, a AAA server, and optionally access to a CA. These devices can be co-located or separate. If they are separate, the recommended practice is to secure the communication between them (the servers are mutually authenticated and communication between them is confidentiality and integrity protected). The hotspot's switch is configured to only allow https traffic to OSU Servers in Home SP networks that are supported by the hotspot. The OSU Server is used to register new subscribers.

When a user enters a hotspot and the mobile device is unable to connect, the mobile device may display to the user the option for online sign-up. This can only be done if the hotspot has been configured to provide online sign-up; whether or not to offer online sign-up is left to the discretion of the Hotspot Operator. If a Hotspot Operator wants to provide online sign-up, it can offer online sign-up services for as many SPs as desired, including itself. Each SP has their own OSU server. Each SP can advertise their name, icon (graphical representation of their brand) and a text description of the service plans offered (in multiple human languages, if desired). This information is displayed on the mobile device's UI so the user can select which provider they want to use.

The number and content of webpages served by an OSU server and the information collected from the user during the OSU process are up to the discretion of the SP. The Friendly Name, Icon metadata (e.g., image size), service description and OSU server URL are provided to the mobile device in the OSU Provider List ANQP-element (see section 3.4.1). A mobile device can,

© 2019 Wi-Fi Alliance. All Rights Reserved.

optionally download the binary icon image using the Icon Request and Icon Binary File ANQP-elements (see section 3.4.2).

The user's intent to connect to a selected SP is indicated by the user's selection of a Friendly Name and/or icon on the mobile device's UI. During the OSU procedure, the mobile device verifies the name and/or icon selected by the user are exactly the same as the ones in the OSU server certificate. This ensures the mobile device has connected to the intended OSU server. The Hotspot 2.0 PKI ([2]) ensures the security of the process. Also, all registration exchanges use HTTPS to ensure the user's contact and payment information are not disclosed to eavesdroppers.

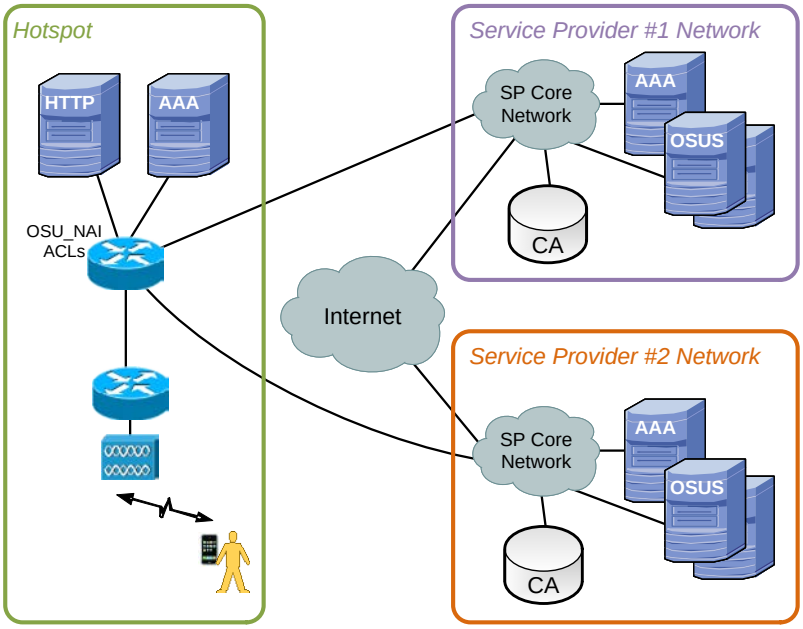

Figure 5: Example Network Architecture for Online Sign-Up

4.2 Hotspot 2.0 PKI

Hotspot 2.0 uses three types of public key certificates for the authentication of OSU servers:

- Hotspot 2.0 Trust Root CA Certificates
- Hotspot 2.0 Intermediate CA Certificates
- Hotspot 2.0 OSU Server Certificates

All Hotspot 2.0 certificates are governed by the *Online Sign-Up Certificate Policy Specification* (see [8]). Table 3 describes the 3 CA/certificate hierarchies than can be used for Release 2 of Passpoint. SPs which employ a small number of OSU servers are expected to use the hierarchy in column 2 of the table; large SPs, which need many OSU server certificates, can use the hierarchy in column 4. In columns 2 and 3, the intermediate CA is working on behalf of the trust root CA; in column 4 the intermediate CA is working on behalf of the SP.

An OSU server certificate may be obtained from any of the CAs authorized by Wi-Fi Alliance. See [7]. OSU server certificates and intermediate CA certificates (if needed) can be obtained by submitting a CSR (certificate signing request) to a CA. The instructions for submitting a CSR can be obtained from your OSU server manufacturer or one of the authorized CAs. An explanation of this process is provided in section 9.

© 2019 Wi-Fi Alliance. All Rights Reserved.

Table 3: Hotspot 2.0 OSU Trust Root Certificate Issuing

1	2	3	4
Trust Root CA	Root CA Vendor	Root CA Vendor	Root CA Vendor
Intermediate CA	Root CA Vendor	Reseller	Service Provider
OSU Server Certificate	Service Provider	Service Provider	Service Provider

Each OSU Server has a certificate signed by a Certificate Authority whose root certificate is trusted by the connection manager of the mobile device. This is depicted in Figure 6. Passpoint Release 2 mobile devices possess the Trust Root certificates from all of the authorized Trust Root CAs. As such, mobile devices can properly validate an OSU server certificate and its metadata (friendly name and icon). This insures the integrity and security of the OSU process.

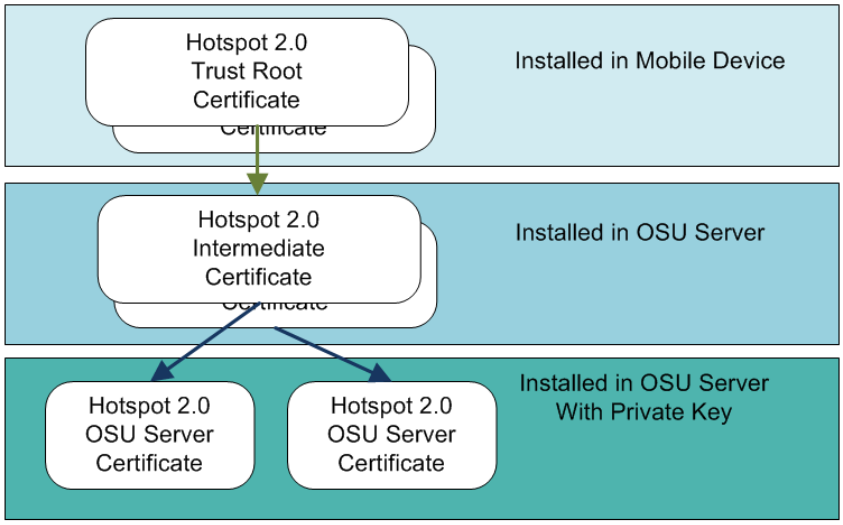

Figure 6: Hotspot 2.0 OSU Certificate Hierarchy

4.2.1 Selection of SP Friendly Name

SPs provide the friendly name they wish to be known by for OSU purposes to the Hotspot Operator for advertisement. SPs provide the exact same friendly name in their CSR when obtaining an OSU server certificate. Friendly names can be provided in any human language (e.g., Arabic, Chinese, French, Korean). Friendly names can and should be provided in several human languages when the hotspot is located in a country having more than one national language (e.g., Switzerland) or, for example, in locations having a lot of international travelers (e.g., airports). The mobile device will choose from the provided human languages the best choice to display to the user.

4.2.2 Usage of SP Icons

SPs provide their icon, which is graphical representation of their brand to the Hotspot Operator for advertisement. SPs provide the exact same icon in their CSR when obtaining an OSU server certificate. For some brands, icons can have human language content and an SP might have several icons having essentially the same image, but different human language content. In these

© 2019 Wi-Fi Alliance. All Rights Reserved.

cases, the SP can and should include multiple icons. The mobile device will choose the icon/human language that's the best choice to display to the user.

SPs should use png encoded icon images (see http://www.w3.org/TR/PNG/) because the Hotspot 2.0 Release 2 specification mandates all mobile devices accept this format; support for no other image format is required by the specification. Image sizes up to a maximum of 65,535 bytes are permitted; SPs are encouraged to use images having a small file size in order to conserve air time when delivering the image to a mobile device. Note that mobile devices will scale the image according to their UI layout.

It's critical that the exact same image file provided in the CSR is also provided to the Hotspot Operator. This is because the CA puts a hash of the icon file in the OSU server certificate and the mobile device computes the hash of the icon delivered by a Hotspot Operator's AP—if the hashes don't exactly match, the mobile device aborts the OSU process.

4.2.3 Revocation of an OSU Server Certificate

If an SP becomes aware that the private key for their OSU server certificate has been lost or compromised, that SP informs the CA which issued the certificate. The CA will then revoke the certificate, putting it on their revocation list. The SP will then need to obtain a replacement certificate. Note that mobile devices certified for Passpoint with Release 2 features check the revocation status of the OSU server certificate before providing any registration data. If the OSU server certificate has been revoked or is invalid (e.g., expired), the OSU process is aborted by the mobile device; this ensures the user's contact and payment information is not stolen or abused by a malicious entity.

4.3 SSIDs for Online Sign-up

Hotspot 2.0 Release 2 requires the use of WPA2-Enterprise for the production WLAN as described in section 8.1. For hotspots offering online sign-up services, a second WLAN is required. A Hotspot Operator has two choices for this second WLAN:

1. The online sign-up WLAN can use the same WLAN/SSID as used for legacy operations (see section 13).
2. The online sign-up WLAN can use an OSEN WLAN/SSID. Hotspot 2.0 defines an OSU Server-Only Authenticated L2 Encryption Network (OSEN). An OSEN is used for OSU access only. In an OSEN, the network is authenticated and any mobile device is allowed to join. Once an OSEN security association is established, the WLAN is encrypted providing confidentiality and integrity protection. Note that the value of the OSEN is to protect mobile device communications not related to OSU (OSU is protected via HTTPS); in many mobile devices, once the device is associated to a WLAN, applications will "wake up" and attempt to communicate with their network peers. It is these communications which OSEN protects as well as protecting the mobile device from potential over-the-air attacks launched by attackers at the hotspot. If the Hotspot Operator chooses OSEN for OSU, there might be three SSIDs used at the hotspot: the production WLAN, the legacy WLAN and the OSEN WLAN.

4.4 Types of Credentials to be issued

The SP decides the type of credentials to provision. Each credential type has their own advantages and disadvantages which need to be considered.

Note: SIM credentials on a mobile device cannot be provisioned using Passpoint Subscription Provisioning.

The SP can choose from the following credential types (assuming they're supported by the OSU server manufacturer):

© 2019 Wi-Fi Alliance. All Rights Reserved.

- User provided username and password. The user may select their own username and password and in addition may re-use other credentials from 3rd party entities (e.g. hotel loyalty program, online web-site credentials)
- SP provided username and password. In this case, password updates are machine-managed. Note that for Hotspot 2.0 Release 2, there is no reason the user needs to be aware of their username and password—the mobile device's connection manager automatically supplies them whenever needed to obtain network access.
- X.509v3 certificates that are supplied by the SP during the OSU process.
- X.509v3 certificates that are supplied by the SP that are pre-provisioned onto the mobile device using an out-of-band method (this method would typically be used only by a mobile network operator having a vendor relationship with the mobile device manufacturer).
- X.509v3 certificates which are supplied by the mobile device manufacturer (e.g., an IEEE 802.1ar-compliant manufacturing certificate). It's up to the mobile device manufacturer whether this option is provided or not. If provided and supported by the OSU server vendor, Hotspot 2.0 protocols provide information on the certificate to the SP so it can be used for Wi-Fi authentication.

5. Provisioning

5.1 Introduction to Mobile Device Provisioning

Once the mobile device has completed registration as described in section 4, it may be provisioned with credentials and the information needed to identify and authorize a network and authenticate for service.

Mobile device provisioning is accomplished using a protocol described in section 5.2. Provisioning data is provided to mobile devices in a data structure referred to as a Management Object (MO); Passpoint with Release 2 features uses an MO entitled the PerProviderSubscription MO (PPS MO) for this purpose. The PPS MO contains the mobile device's Wi-Fi access credential and related metadata (see section 5.3), network identifiers (see section 5.4) and optionally network-selection policy (see section 7).

The SP that provisions the subscription usually provides the policy associated with that subscription. In other words, the entity that provisions the credential controls how it's used.

The PPS MO contains information allowing the mobile device to discover and connect to a Wi-Fi Access Network. This PPS MO can enable a mobile device to select a single Wi-Fi Access Network (e.g. Home network), or multiple Wi-Fi Access Networks (e.g. public Wi-Fi hotspots). If the PPS MO includes Wi-Fi roaming relationships, then this may result in multiple Wi-Fi Access Network connectivity.

Some SPs may have other out-of-band methods of provisioning policy (e.g., re-distribution of SIM cards) which are out of scope of this specification. In this case, the Policy node within the PerProviderSubscription MO is not present.

5.2 Selection of Provisioning Protocol

The Hotspot 2.0 (R2) Specification supports both OMA-DM and SOAP-XML as provisioning protocols between the Online Sign-Up Server and mobile devices. However, mobile devices are only required to support SOAP-XML. It's up to the SP (or the administrator of the OSU Server) to determine which of the two protocols (or both) to deploy within their systems.

© 2019 Wi-Fi Alliance. All Rights Reserved.

Note that when a mobile device requests the OSU Providers List ANQP-element, prior to initial association, the specific provisioning protocol for the target OSU Server is returned within the ANQP response.

Note that SPs having a vendor relationship with a mobile device manufacturer may have an agreement to use OMA-DM as the device provisioning protocol; any such agreement is outside the scope of Hotspot 2.0.

5.3 Subscription Credential

The PPS MO contains subscription parameters and credential metadata, which assist the mobile device with enabling automatic connections to SP networks.

The PPS MO subscription parameters include the creation and expiration dates of the subscription together with what type of subscription is supported, for example “Gold”, “Silver” or Bronze”. Usage limits are also included, so that when a data or time limit is reached or passed, either the subscription or the credential expires.

The PPS MO credential metadata also include creation and expiration dates of the credential, together with information about the types supported as mentioned in section 4.4:

- Username/password
  - In addition to the actual username and password strings, the metadata contains information about the EAP methods that are supported, the ability to share this information, and whether it can be managed by a machine (i.e. without user intervention)
- Certificates
  - The metadata includes the certificate type and an associated fingerprint
- SIM
  - The IMSI and EAP type are provided.

Information about the AAA Server Certificate is also provided. The PPS MO provides information identifying the trust root from which the AAA Server certificate was issued (assuming an EAP method is used which requires such a certificate) as well as whether the mobile device is required to perform a revocation check using OCSP on that certificate.

Finally, the identity of the Realm from which the credential is issued is supplied.

5.4 Network Identifiers

The PPS MO contains network identifiers, which assist the selection of Wi-Fi Access Networks, following the discovery process. A connection manager within a mobile device will use these provisioned network identifiers to match discovered network identifiers from available Wi-Fi Access Networks, which are deemed to be in radio range at the current location of the mobile device.

- NAI Realm(s)
  - A realm advertised by an AP indicates that when a mobile device uses an authentication credential issued from that realm’s SP, authentication will be successful. If the AP has roaming agreements with more than one SP or the SP has more than one realm, then this identifier becomes a list.
- PLMN(s)
  - A PLMN identifier (i.e. an MNC/MCC code) advertised by an AP indicates that when a mobile device uses a (U)SIM credential issued by that PLMN, authentication will be successful. If the AP has roaming agreements with more than one PLMN, then this identifier becomes a list.
- Roaming consortium Object Identifier(s) (OI)
  - A Roaming consortium OI advertised by an AP indicates that when a mobile device uses an OI issued to that SP, authentication will be successful. If the AP

© 2019 Wi-Fi Alliance. All Rights Reserved.

has roaming agreements with more than one SP or the SP has more than one OI, then this identifier becomes a list.

- An SSID or list of SSIDs can identify a Wi-Fi network as a home network.

5.5 Updating Provisioned Subscription Data (PPS MO)

Within the PPS MO there are several items of data which can be updated and re-provisioned within mobile devices. These include the following examples:

- Home SP identification metadata including Wi-Fi home network identifiers, Home OI list, Roaming Consortium OI List, other roaming partners to be deemed as home providers by the mobile device
- Subscription usage limits (e.g., GB/month)
- How often to update this subscription data

6. Access

The Access state is entered when the mobile device has associated to a network for which it has login credentials and WLAN security settings and has successfully authenticated to that network. For Passpoint networks, these settings were previously configured on the mobile device, either in the Provisioning state or via other means.

In the Access state, the mobile device mutually authenticates with the Service Provider's AAA server and if successful, the mobile device receives access to the Wi-Fi hotspot network.

7. Service Provider Use of Network-Selection Policy

7.1 Management of Policy on the Mobile Device

A Service Provider can define policies to control some aspects of the network selection performed by a mobile device. Defining policies is an optional task, and the policies available are all optional, and a SP can choose which, if any, of these policies to define. Note that policy can be provisioned to mobile devices having a any type of credential, including a SIM credential (even though Hotspot 2.0 Release 2 cannot provision a SIM credential to a mobile device).

When defined by a SP, policies are stored in a policy server, and retrieved by the mobile device. There are rules that need to be defined to control the retrieval of the policies by the mobile device:

- The SP can define the update interval for the mobile device to refresh its policies from the policy server. As this policy can incur signaling that can affect the network performance, the refresh period should take this into account.
- The SP can also define the network under which the refresh of policies can occur by configuring the Restriction part of the PolicyUpdate node in the PPS MO. A Service Provider can configure the type of network where policy refresh can occur, as shown in Table 4.
- The URI of the policy server, as well as its trust root server address is also defined to allow the mobile device to validate the policy server identity.
  If desired, a specific policy server credential can be configured, instead of using the subscription credentials.

The table below provides an example of the update policy that can be set by an SP. Note: the subscription remediation mechanism can be used to update the policy in a way that's initiated by the Home SP.

© 2019 Wi-Fi Alliance. All Rights Reserved.

Table 4: PolicyUpdate example

Policy Name	Example Value	Description
UpdateInterval	43200 (minutes)	The mobile device will check for policy updates every 30 days. This value setting is based on the policy update expectations: frequent or infrequent. The SP can set this parameter to a value such that the network doesn't incur unneeded signaling.
UpdateMethod	{SPP-ClientInitiated, OMA-DM-ClientInitiated}	This setting depends on the type of policy server (SOAP or OMA-DM based) deployed by the Service Provider.
Restriction	{RoamingPartner, HomeSP, Unrestricted}	This policy specifies on which type of network the policy update/retrieval can be performed by the mobile device. When choosing HomeSP or RoamingPartner, both of these networks are Hotspot 2.0 compatible networks. Unrestricted, also include non-Hotspot 2.0 networks.
URI	https://policyserver.network.net/policies	This is the URI of the policy server.
Username/Password	Residential-user, mypassword	These credentials are to be used only to authenticate toward the policy server of the Home SP, instead of using the mobile device subscription credentials.
TrustRoot	https://certs.network.net/certstore/SP-Policy-cert.pem 0xFA3DD…	The trustroot URL provide access to the root CA certificate that signed the policy server certificate. This allows the device to trust the policy server certificate presented by the policy server during the TLS authentication phase.
Other	Vendor specific policies	The SP can define additional specific policies related to the update of policies. If any vendor specific polices are defined, it's up to the SP to determine whether they are supported by the particular mobile device being provisioned.

7.2 Configuration of Home and Roaming Partner Identities

A Service Provider can control the selection priority associated with its roaming partners when these roaming partners are available in the same coverage area.

When a mobile device makes use of this policy, the roaming partner with the highest priority ranking is selected when the environmental conditions[8] allow.

[8] Environmental conditions include, but are not limited to the minimum RSSI needed to join a Wi-Fi network, the mobile device's battery level (state of charge), whether other interfaces are currently in use (e.g., Bluetooth, Cellular, USB) on the mobile device, etc. Determination of

© 2019 Wi-Fi Alliance. All Rights Reserved.

Care should be taken when a SP defines this policy, as it may lead to suboptimal service in some situations, i.e.: a Wi-Fi network is selected, yet the perceived RSSI from the nearest AP (nearest in an RF sense) is lower than a neighboring Wi-Fi network, or an AP is selected, yet its perceived RSSI is lower than a neighboring AP.

Once defined by the SP, this list should be maintained to adapt to changes in roaming partner priority, based on commercial agreements, or commercial presence in some countries, as well as in changes of characteristics of the roaming partners.

It's not required for the SP to update the PreferredRoamingPartnerList every time a new roaming partner is introduced, unless there is a requirement to change the default priority ranking.

- The PreferredRoamingPartnerList defines the priority assigned to a roaming partner whose FQDN is defined in FQDN_Match. In addition to the FQDN, one or more countries may be defined. For example, a roaming partner may have different priorities based on the country where it operates, as shown in the table below.

Table 5: PreferredRoamingPartnerList Policy example.

PreferredRoamingPartner List Policy	Wi-Fi Network 1	Wi-Fi Network 2	Mobile device behavior
FQDN_Match = fastNetwork.com,includeSubdomains Priority = 1 Country = US FQDN_Match = fastNetwork.com,includeSubdomains Priority = 200 Country = *	Domain Name (from Domain Name ANQP-element) = play.fastNetwork.com AP is located in the US	Domain Name (from Domain Name ANQP-element) = boingo.com AP is located in the US	Mobile device home network is home.net. fastNetwork.com and boingo.com are roaming partners of home.net. Mobile device is roaming in the US. Mobile device will select FastNetwork based on the PreferredRoamingPartnerList policy.

The following example showcases how the mobile device will select a roaming partner not explicitly defined in the PreferredRoamingPartnerList policy. When not explicitly defined in the PreferredRoamingPartnerList, the priority assigned is 128.

- The HomeOIList is used by the Service Provider to indicate to the mobile device whether it can successfully authenticate to a hotspot belonging to a specific Home Organizational Identifier as advertised in the Roaming Consortium OI. Another case where the organizational Identifier can be used, is when the user's Home SP has hotspots that should only be accessed by specific categories of subscribers: e.g., business subscribers vs. residential subscribers. In this case, the contents of the PPS MO for business subscribers would be different than for residential subscribers; specifically, business subscriber's PPS MO would have a designated OI in the HomeOIList and HomeOIRequired would be set to "true". The mobile device would only select a hotspot network that advertises the designated OI. When defined, this policy will override the default selection behavior of the mobile device, therefore Service Providers need to evaluate their requirements for enabling this policy.
- The RoamingConsortiumOI, when included in the PPS MO, is used by the mobile device to select hotspots networks that advertise one of the Roaming Consortium OIs. When using RoamingConsortiumOI, HomeOIRequired is set to false.

---

whether environmental conditions are suitable to join a Wi-Fi network are left to the discretion/implementation of the mobile device manufacturer.

© 2019 Wi-Fi Alliance. All Rights Reserved.

- The OtherHomePartners allow the Service Provider to define a list of FQDNs that are to be considered as home networks by the mobile device, instead of being considered roaming partners. A hotspot advertises its domain name (or FQDN) in the Domain Name ANQP-element -- when the domain name matches one of the FQDNs in OtherHomePartners, that hotspot will be deemed by the mobile device as a home network. This can be used in the case where a service provider is associated with another service provider. For example, a service provider acquired another service provider, but doesn't want to change the advertised domain of the acquired SP, yet the mobile device should not consider the acquired SP as a roaming partner anymore in its selection process.

The following is an example of how this policy can be used by a SP:

- Service provider BlueNetwork acquires service provider GrayNetwork.
- The subscribers of BlueNetwork will have their policy updated by the SP in the policy server, so it indicates an entry into the FQDN leaf of the OtherHomePartners internal node, indicating the GrayNetwork domain name.
- When in the presence of a GrayNetwork hotspot, a mobile device belonging to the BlueNetwork, won't consider it a roaming network, and would select it as a home network. The selection of GrayNetwork would take precedence over the roaming partners that may be defined in the PreferredRoamingPartnersLists internal node. If both BlueNetwork and GrayNetwork were present, the mobile device would select its home network, in this case: BlueNetwork.
- An update of the policy of the GrayNetwork mobile device will also be performed, where the OtherHomePartners internal node will contain the BlueNetwork domain name, to allow the GrayNetwork mobile device to consider the BlueNetwork hotspots as a home network, and select it in priority over roaming partners, that are present in the coverage area.
- The NetworkID policy, in conjunction with the FQDN leaf, defines the Access Points that will be selected in priority by the mobile device. The mobile device would consider that an access point is part of its home network, and therefore would select it in priority, only if it is advertising the SSID defined in the Network ID, in addition to the network domain name. This can be used when subscribers belonging to the same network, but having different subscription types (i.e.: business vs consumer subscription) and the service provider want to ensure that the business subscriber's mobile devices select specific Access Points (see Table 7).

Table 6: NetworkID Policy example

NetworkId Policy	Wi-Fi Network 1 Configuration	Wi-Fi Network 2 Configuration	Mobile device behavior
SSID = Business FQDN = fastLane.net HESSID not defined	SSID = Business FQDN = fastLane.net	SSID = Internet FQDN = fastLane.net	A mobile device with this policy setting belongs to a business subscription. AP 1 will be selected.

7.3 Configuration of Exclusion List

The exclusion list is a policy that can be used to restrict the automatic selection by the mobile device of specific SSIDs being broadcasted by service providers. The SPExclusionList policy can contain up to 128 SSIDs that an operator can define. The user can override the defined exclusion list policy by manually selecting a broadcasted SSID.

© 2019 Wi-Fi Alliance. All Rights Reserved.

An example of when a SP may choose to define this policy is when it's deploying new access points and would like to ensure that only these new Access Points are selected in priority by the devices. The new Access Points would be assigned a new SSID, and the SPExclusionList policy would be set with the SSID assigned to the old Access Points. When the mobile device makes use of this policy, it will only select the Access Points whose SSID is not defined in the SPExclusionList policy. If the only available SSIDs are the one defined in the SPExclusionList policy, the mobile device won't associate to any access points. A user is able to override this behavior by manually selecting a SSID even if it's defined in the SPExclusionListPolicy.

The table below showcases an example of how the mobile device perform the AP selection when the Exclusion List policy is in effect:

Table 7: SPExclusionList Policy example

SPExclusionList Policy	Wi-Fi Network 1	Wi-Fi Network 2	Mobile Device Behavior
SSID = "oldSSID"	SSID = "oldSSID"	SSID = "newAP"	The mobile device will select Wi-Fi Network 2.

A Service Provider should ensure that this policy does not lead to sub-optimal service offering.

7.4 Configuration of Traffic-Load Thresholds

Policies are available to allow the selection of networks based on their traffic loading.
A mobile device can be provisioned with both or either one of these policies:

- A selection policy based on the access point's maximum acceptable BSS load, defined in the MaximumBSSLoadValue. This policy has an Access Point scope.
- A selection policy based on the hotspot's available backhaul bandwidth, defined in the MinBackhaulThreshold. This policy has a hotspot scope.

When the mobile device makes use of these policies, network selection will primarily be based on their evaluation, provided environmental conditions are suitable.

7.4.1 Minimum Available backhaul bandwidth policy

The mobile device when in a presence of one or more networks advertising their currently available backhaul bandwidth using the WAN Metrics ANQP-element, can perform a prioritization of these networks, and select the one which complies with its defined policy.

The following are the network selection rules, when the Home SP defines the minimum available backhaul bandwidth policy:

- The Service Provider can define a Home network policy and a Roaming network policy.
- The operator can choose to define uplink policy, or downlink policy, or define both.
- Network selection by the mobile device will take place, even if none of the available networks advertises its available backhaul bandwidth, the selection policy may then be based on a different policy, if defined, or based on radio characteristics.
- The mobile device may select the network with the best available backhaul bandwidth, relative to the other available networks when none comply with the policy defined on the mobile device's PPS MO.
- When some networks advertise their available backhaul bandwidth, and others don't advertise it, the mobile device will give priority to those that advertise their characteristics. The network selected will be the one with the relative best characteristic.
- The defined policy is only evaluated upon initial network selection. Once associated with a network, the policy is not evaluated again. This policy won't trigger the mobile device to

© 2019 Wi-Fi Alliance. All Rights Reserved.

change networks because of a change in network WAN Metric values.

An example of the minimum available backhaul bandwidth policy, and the mobile device behavior is defined in Table 8:

Table 8: Minimum Backhaul Threshold Policy example

MinimumBackhaul Threshold Policy	Wi-Fi Network A	Wi-Fi Network B	Mobile Device Behavior
DLBandwidth = 2000kbps ULBandwidth = 1000kbps	DL speed = 8.5Mbit/s UL speed= 512kit/s DL Load = 0 UL Load = 0	DL speed = 5Mbit/s UL speed = 2Mbit/s UL Load = 127 DL Load = 127	The mobile device selects the network B, as it has a more complete WAN Metrics data, which is compliant with its policy. Hotspot Network B has 2510 kbit/s of *available* DL speed (50% of 5Mbit/s) and 1003 kbit/s (50% of 2Mbit/s) of *available* UL speed inline with the defined policy.
DLBandwidth = 3000kbps ULBandwidth = 500kbps	DL speed = 7Mbit/s UL speed = 0 DL load = 30 UL Load = 0 This is an example of the uplink Load and speed not being available.	DL speed = 2Mbit/s UL speed = 2Mbit/s UL Load = 50 DL Load = 50	The mobile device selects Hotspot Network A as it has a compliant policy (albeit, incomplete) vs. hotspot Network B that is not compliant with the defined policy.

7.4.2 Maximum BSS Load policy

The Maximum BSS Load value policy is linked to the BSSLoad value being broadcasted by the access point. This value fluctuates over time, and depends on the channel utilization and interference. The Channel Utilization parameter within the beacon frame BSSLoad element contains the BSSLoad value.

The following are the network selection rules that apply when the Home SP defines this policy:

- When the mobile device is evaluating the APs from its home network it, selects an AP that broadcasts a BSSLoad value that's lower than BSSLoad value of this policy, provided environmental conditions are acceptable. This policy can be ignored by mobile devices if APs are not broadcasting their BSS Load.
- The mobile device will select an access point based on other criteria's such as signal strength, when the BSSLoad value is not advertised by non-Passpoint APs[9].
- If none of the APs advertise a BSSLoad value acceptable by the defined policy, a mobile device selects the access point with the best signal strength or other mobile device determined criteria.
- When the SP defines this policy in the PPS MO, the policy is only evaluated upon initial network selection. The policy won't trigger a change of access point (AP reselection), if the BSSLoad value changes.

[9] Passpoint certified APs are required to support BSSLoad and Hotspot Operators are required to enable it.

© 2019 Wi-Fi Alliance. All Rights Reserved.

Table 9: Example BSS Load Policy

BSSLoad Policy	AP 1	AP 2	AP 3	Mobile Device behavior
BSSLoad = 55	Broadcasted BSSLoad = 20	Broadcasted BSSLoad = 100	Broadcasted BSSLoad = 203	The mobile device selects AP 1.

Note: in the above table, all APs are in the mobile device's home network.

7.5 Configuration of Open Firewall Ports

The mobile device may have application(s) installed or made available by the service provider, that require specific firewall ports to be open so they can function properly. The RequiredProtoPortTuple is a policy defined by the Home SP to ensure that a mobile device joining a visited network can use applications provided by the Home SP. This policy doesn't apply to the home network, as it's assumed that the Home SP network will have the required port tuples defined to suit its application.

This policy doesn't cover applications installed by the end-user.

The mobile device rules for network selection when the RequiredProtoPortTuple policy is defined are:

- When no hotspots fully comply with this policy, based on the ProtoPortTuple(s) advertised in the Connection Capability ANQP-element, the mobile device will select a hotspot that partially complies with this policy, if possible.
- The mobile device will select a hotspot, based on other policy criteria, when none of the available hotspots comply with the open firewall ports policy.

Table 10: Required Proto Port Tuple policy example

RequiredProtoPortTuple Policy	AP 1	AP 2	Mobile Device behavior
IPProtocol = 6 (tcp) PortNumber = 80, 443 (http, https) IPProtocol = 17 (udp)	Connection Capability ANQP-element: TCP/HTTP TCP/HTTPS UDP with Port 500	Connection Capability ANQP-element: TCP/HTTP TCP/HTTPS	The defined policy is for web traffic and any UDP traffic. The mobile device will select AP 1, as it complies with the defined policy.
IPProtocol = 50 (ipsec) IPProtocol = 17 (udp) PortNumber = 500 (IKE)	Connection Capability ANQP-element: TCP/HTTP	Connection Capability ANQP-element: TCP/HTTP TCP/HTTPS	The defined policy is for IPSec traffic and UDP traffic. The mobile device not finding any compliant AP, will select the AP using a different criteria, such as RSSI for example.

© 2019 Wi-Fi Alliance. All Rights Reserved.

8. Security Features and Hotspot Network Security

This section describes the security features of networks using Passpoint equipment and the security threats that they mitigate. It also provides guidelines on Passpoint AP deployment to help create a secure Hotspot 2.0 network.

Wi-Fi Alliance is committed to creating the strongest possible security while promoting interoperability. Wi-Fi security depends on supplicants being correctly configured to validate server certificates.

8.1 WPA2™-Enterprise Security

8.1.1 Mutual Authentication

Authentication of a mobile device is based on the IEEE 802.1X mutual authentication framework with EAP support. Mutual authentication is used to prevent a mobile device from connecting to a rogue network controlled by an attacker.

Mobile devices are provided with unique credentials (according to the EAP method supported) in order to authenticate to the IEEE 802.1X authentication server. Before a mobile device submits its credentials to the server for validation, the device first authenticates the server (for example, based on the server's certificate).

As defined in [2], a Passpoint AP can be configured to prevent peer-to-peer (P2P) operation, direct link setup (DLS) and tunnelled DLS (TDLS); a Passpoint AP is not permitted to use WPA2-Personal, Temporal Key Integrity Protocol (TKIP) or Wired Equivalent Privacy (WEP).

Credentials and related EAP methods supported by the Passpoint certification program are described in Table 11 and [2]. Passpoint APs support all EAP methods and credential types listed in Table 11. Mobile devices with SIMs or USIMs are required to support all the EAP methods listed in Table 11 and their associated credential types. Mobile devices without a SIM or USIM do not support EAP-SIM, EAP-AKA or EAP-AKA'.

The Hotspot 2.0 Specification mandates an SP support either a certificate or username/password credential type, or both, plus its associated EAP method(s) listed in Table 11.

Table 11: Credential Types and EAP Methods

Credential Type	EAP Method(s)
Certificate	EAP-TLS
SIM	EAP-SIM
USIM	EAP-AKA, EAP-AKA'
Username/password (with server-side certificates)	EAP-TTLS with MS-CHAPv2

If an SP has a SIM/USIM infrastructure, the Hotspot 2.0 Specification additionally mandates support SIM/USIM credentials and their associated EAP methods. These requirements ensure that a mobile device will always have at least one valid credential type to authenticate against an SP's network.

© 2019 Wi-Fi Alliance. All Rights Reserved.

8.1.2 Strong Encryption

Advanced Encryption Standard (AES) encryption is used over the wireless interface between a mobile device and the Passpoint AP. AES is one of the most advanced standards-based encryption algorithms available in the industry. The AES encryption keys (the Pairwise Transient Key [PTK] and the Group Temporal Key [GTK]) are derived from the unique Pairwise Master Keys (PMKs) generated as part of the IEEE 802.1X authentication process.

The strong encryption used between a mobile device and the Passpoint AP makes it extremely difficult for an attacker to compute the keys needed to eavesdrop on the traffic exchanged between the devices. The integrity protection afforded by the AES encryption mechanism makes it computationally impractical for an attacker to perform a man-in-the-middle attack.

Passpoint APs and mobile devices that are certified for WPA2 with Protected Management Frames (PMF) [5] mitigate eavesdropping and DoS vulnerabilities. PMF does not protect pre-association ANQP-elements.

8.2 L2 Traffic Inspection and Filtering

A Passpoint AP operating as a “free public network” or “chargeable public network” support inspection and filtering of data frames exchanged between mobile devices in the same BSS or extended service set (ESS), [2]. The inspection is aimed at verifying that MAC service data units (MSDUs) match a specific set of traffic filters in the entity (AP or firewall) performing the filtering. The aim of the filtering is to protect a mobile device from attacks by other mobile devices. The only MSDUs delivered to a mobile device are those that are addressed to it from another mobile device and that successfully pass through the enabled filters.

All Hotspot Operators deploy a firewall function in their hotspot network. The firewall function can reside either in a Passpoint AP or in an external entity to which the AP is connected. The firewall protects the AP and the associated mobile devices from Internet-based attacks, and it protects a mobile device from attacks by other mobile devices.

The proxy Address Resolution Protocol (ARP) service, as defined in [3], is enabled to prevent ARP spoofing attacks upon a mobile device by another mobile device belonging to the same BSS or ESS.

8.3 Deactivation of Broadcast/Multicast Functionality

It is recommended that hotspots using Passpoint APs disable the multicast/broadcast capability unless those services are needed for functions such as providing IP TV services or high-definition (HD) streaming services. When the multicast/broadcast functionality is disabled, no GTKs are used; hence it is not possible for an attacker that has successfully authenticated to the AP to send the AP spoofed packets encrypted with the GTK. (This type of attack is known as a hole-196 attack.)

When multicast/broadcast capability is disabled, the Passpoint AP uses proxy-ARP service [3], to provide ARP functionality. It is recommended that proxy-ARP service also be used when multicast/broadcast functionality is enabled.

8.4 AAA RADIUS Parameters Supported by Passpoint Certified APs

Passpoint APs exchange authentication, authorization and accounting parameters with the AAA server using the Remote Authentication Dial-in User Service (RADIUS) protocol. The Wi-Fi Alliance has developed a recommended set of RADIUS parameters, see [9]. Verification of these parameters is not part of Passpoint certification testing.

The set of RADIUS attributes to be used between proxy AAA servers and home AAA servers is outside the scope of this deployment guide.

© 2019 Wi-Fi Alliance. All Rights Reserved.

8.5 EAP Method Negotiation

Hotspot 2.0 requires mobile devices and AAA servers to support a minimum set of EAP authentication methods (see section 2 in [2]). EAP method negotiation occurs during the initial message exchange. The AAA server requests the mobile device to authenticate using an authentication method. If the mobile device supports the authentication method, it will use it to authenticate with the AAA server. If the mobile device does not support the authentication method, it will reject the request. To maximize interoperability, the SP should configure the AAA server to request authentication methods that are required to be supported by [2].

8.6 Certificate Management

Server Certificates

Certificates are used to authenticate Subscription servers (see Figure 3). They are used in HTTPS connections with OSU, Remediation, and Policy servers. They are also used in EAP-TTLS or EAP-TLS authentication messaging with the AAA server. A typical certificate validation chain consists of a root CA certificate, intermediate CA certificate(s), and a server certificate. SPs install the server certificate, its associated private key, and any intermediate CA certificates on each Subscription server they are using. Root CA certificates are installed in the mobile device during manufacture or during the provisioning process (including OSU).

OSU server certificates are issued by Wi-Fi Alliance authorized commercial CA vendors holding OSU server root CA and/or intermediate CA certificates [7]. SPs acquire OSU server certificates from one of these vendors. The OSU certificate chain consists of a root CA certificate, an intermediate CA certificate, and a server certificate. SPs install the server certificate, its associated private key, and the intermediate CA certificate, on the OSU server. Mobile device vendors will install all OSU root CA certificates from the authorized commercial CA vendors on the mobile device during manufacturing to be used as a trust anchor for validating certificates received from the OSU server during the authentication process.

Certificates for the other Subscription servers (AAA without OSEN, Remediation, Policy) can be issued from any CA the SP prefers including the authorized CA vendors. Root CA certificates for these servers are installed on the mobile device during the manufacturing or provisioning process. OSU supports secure provisioning of these root CA certificates to the mobile device using the PPS-MO (see section 5.7).

Client Certificate

Passpoint supports user mobile device authentication using a client certificate (EAP-TLS). The client certificate can be issued from any CA the SP prefers and is installed on the mobile device during the manufacturing process or provisioning process. OSU supports provisioning client certificates to mobile devices. The OSU server acts as a proxy between the mobile device and the CA and forwards certificate enrollment requests and responses. The CA certificate used to issue the client certificate is installed on the AAA server to be used as a trust anchor for validating client certificates received from the mobile device during the authentication process.

If the CA used for issuing client certificates is the same as the CA used for issuing the AAA server certificate, the AAA trust anchor CA certificate can be downloaded to the mobile device using the client certificate enrollment process instead of using the PPS-MO. Just leave the AAAServerTrustRoot node out of the PPS-MO.

Certificate Renewal and Revocation

SPs should renew their server certificates before they expire. An expired server certificate will cause the mobile device to fail server authentication and not connect to the network.

Mobile devices are required to check the revocation status of OSU server certificates. This is done using TLS messaging extensions when establishing an HTTPS connection to the OSU server. The SP configures the OSU server to acquire revocation status using OCSP from the

© 2019 Wi-Fi Alliance. All Rights Reserved.

commercial CA that issued the OSU server certificate. The commercial CA's OCSP responder URL is included in the OSU server certificate's AIA extension.

OSU Provider List Configuration

The OSU provider list contains Friendly Name and Icon Metadata subfields. The mobile device checks these subfield values against values in the OSU server certificate when a user selects an SP for OSU. If they do not match the mobile device will shut down the connection with the OSU server.

When the Hotspot Operator configures the OSU Providers List in the AP it should make sure that the OSU Friendly Name subfield language code [9] and text string match the corresponding fields in the Friendly Name extension of the OSU certificate for a given SP. It should also make sure that Icon Metadata (pixel width, pixel height, language code, type, and filename) match the corresponding values in the Icon field extension of the OSU certificate. The Hotspot Operator typically obtains the OSU certificate field information from the SP.

8.7 Online Sign-up SSID Configuration

The online sign-up SSID can be configured to be open or encrypted using OSEN (see section 4.3). When the SSID is open, the mobile device establishes a secure HTTPS connection with the OSU server over an open Wi-Fi Access Network. Server authentication is performed using the OSU server certificates and the authorized trust anchor root CA certificates.

When the SSID uses OSEN the mobile device first connects to the AAA server and establishes keys with the AP for encrypting the Wi-Fi link before connecting to the OSU server. The AAA server connection uses Anonymous EAP-TLS messaging where only server authentication is performed. The AAA server sends authentication status and keying material to the AP so that the necessary link layer encryption keys can be setup between the AP and mobile device. Since the mobile device has not yet been provisioned it uses the authorized trust anchor root CA certificates (installed during manufacturing) to validate the AAA server certificate. Therefore, AAA server certificates used for OSEN SSIDs are issued by one of the Wi-Fi Alliance authorized commercial CAs.

8.8 Management Object Security Parameters

Hotspot 2.0 uses two management objects for sending parameters between servers and mobile devices which are the PerProviderSubscription management object (PPS MO) and the Hotspot 2.0 vendor-specific extensions to the DevDetail management object. This section provides deployment guidelines for the security parameters in these management objects.

Server Trust Anchor Certificates

The PPS-MO contains parameters for communicating trust anchor certificate information to the mobile device. CA certificate trust anchors are used to validate certificates received from Subscription servers (see Figure 3) during authentication. The same CA certificate may be used as a trust anchor for more than one server. There are TrustRoot nodes for each server, except OSU, that provides the necessary information for the CA certificate trust anchors. OSU server trust anchor root CA certificates have already been selected and installed in the mobile device (see section 8.6) and therefore, there is not a PPS-MO TrustRoot node for the OSU server.

The TrustRoot node contains an HTTPS URL and certificate fingerprint. The URL is used by the mobile device to retrieve the trust anchor certificate. The fingerprint is a SHA-256 hash digest value of the trust anchor certificate in DER format. The mobile device can use this fingerprint value to determine if it already has the trust anchor certificate installed or if it needs to download it using the URL.

The SP is required to include a TrustRoot node in the PPS-MO for the Remediation Server. If a Policy server is used the SP includes a TrustRoot node in the PPS-MO for it. Including a TrustRoot node for the AAA server depends upon what kind of credential the mobile device is

© 2019 Wi-Fi Alliance. All Rights Reserved.

using for authentication. If a password credential is used the SP includes a TrustRoot node in the PPS-MO for the AAA server. If a certificate credential is used the SP includes a TrustRoot node in the PPS-MO for the AAA server if they want the mobile device to ignore any trust anchor CA certificates downloaded during the client certificate provisioning process using EST. If a certificate credential is used the SP does not include a TrustRoot node in the PPS-MO for the AAA server if they want the mobile device to use the CA certificate downloaded during the EST client certificate provisioning process as the trust anchor for the AAA server.

Mobile Device Credentials

The PPS-MO supports three types of mobile device credentials that can be used for the subscription; UsernamePassword, DigitalCertificate, and SIM. The SP is required to include at least one or more of the three credential types in the PPS-MO. If a UsernamePassword credential is used the SP should make sure that the provisioning system updates the subscriber database with this information so the AAA server can access it during the authentication process. There are other UsernamePassword parameters that are also required to be set. The MachineManaged parameter indicates if the password was provided by the SP or not. The EAPType node is indicates what type of EAP authentication protocol is being used. To be interoperable with all Passpoint mobile devices the SP should set the EAPType node to 21 (EAP-TTLS) and the InnerMethod node to 'MS-CHAP-V2'.

If a DigitalCertificate credential is used the SP includes the CertificateType and the CertSHA256Fingerprint nodes. The fingerprint is used by the mobile to locate an installed certificate that has the same fingerprint value. Once located the certificate is used as a credential when the mobile device authenticates to the AAA server. An SP that is using the PPS-MO for provisioning mobile devices should keep track of certificate fingerprints for certificates that are issued as a credential for mobile device authentication so that the fingerprint value can be included in the CertSHA256Fingerprint node. This includes when certificates are issued during the OSU certificate enrollment process. The fingerprint is created by calculating a SHA-256 digest over the DER encoded certificate.

If a SIM credential is used the SP includes the IMSI and EAPType nodes. The IMSI helps the mobile device select the correct SIM card when there is more than one and helps with AP discovery. The EAPType node indicates what EAP authentication method the mobile device should use for authentication. Hotspot 2.0 supports EAP-SIM, EAP-AKA, and EAP-AKA'.

For any of the credential types the SP includes a Realm node that is used by the mobile device for AP selection.

To enable mobile device revocation checking of the AAA server certificate during the EAP-TTLS or EAP-TLS authentication protocol exchange, the SP can include the CheckAAAServerCertStatus node set to True. The SP should enable OCSP stapling using TLS on the AAA server and setup the necessary OCSP responder interface with the issuing CA before including this node in the PPS-MO.

The CredentialPriority node is used to indicate credential priority when more than one credential is used in a PPS-MO. The SP includes the CredentialPriority node in the PPS-MO. The lower the value, the higher the priority.

When the mobile device establishes an HTTPS connection to the Policy and Remediation servers, it is required to provide a credential for authentication. The SP can provide a username/password credential by including the Policy/PolicyUpdate/UsenamePassword node and/or the SubscriptionUpdate/UsernamePassword node in the PPS-MO. If these nodes are not included the mobile device uses the credential configured by the Credential node.

Mobile Device Capabilities

The mobile device communicates security capability information to the OSU server with the Hotspot 2.0 vendor-specific extensions to the DevDetail–MO. Capabilities include supported EAP methods, SP provisioned certificate credentials, manufacturing provisioned certificate credential, and SIM card possession. The OSU server can use this information to determine how to

© 2019 Wi-Fi Alliance. All Rights Reserved.

provision the mobile device with the PPS MO. SPs should configure their OSU server to provision mobile devices with credentials based on capability settings in the Hotspot 2.0 vendor-specific extensions to the DevDetail-MO.

8.9 Protected Management Frames

All Passpoint Release 2 AP and mobile devices support Protected Management Frames (PMF). Robust[10] unicast management action frames are protected from both eavesdropping and forgery, and robust broadcast/multicast management action frames are protected from forgery (see clause 4.5.4.9 in [3]). Passpoint protected management frames include WNM-Notification Request Frames that are sent by the AP to the mobile device to notify it of needed subscription remediation or if deauthentication is about to occur.

9. Hotspot Server Certificate Lifecycle

9.1 Certificate Signing Request (CSR)

9.1.1 What is a Certificate Signing Request (CSR)?

A Certificate Signing Request or CSR is an encoded file that provides a standardized way to send a Certificate Authority (CA) the public key portion of the public/private key pair along with information that identifies the company and the domain name; this information is included in the OSU Server Certificate. Before an OSU Server Certificate can be ordered and purchased, a key pair and a CSR is generated by the applicant.

Note: The CA confirms that the applicant owns the key pair by verifying the applicant's digital signature on the CSR with the public key in the CSR.

```
-----BEGIN CERTIFICATE REQUEST-----
MIICvDCCAaQCAQAwdzELMAkGA1UEBhMCVVMxDTALBgNVBAgMBFV0YWgxDzANBgNV
BAcMBkxpbmRvbjEWMBQGA1UECgwNRGlnaUNlcnQgSW5jLjERMA8GA1UECwwIRGln
aUNlcnQxHTAbBgNVBAMMFGV4YW1wbGUuZGlnaWNlcnQuY29tMIIBIjANBgkqhkiG
9w0BAQEFAAOCAQ8AMIIBCgKCAQEA8+To7d+2kPWeBv/orU3LVbJwDrSQbeKamCmo
wp5bqDxIwV20zqRb7APUOKYoVEFFOEQs6T6gImnIolhbiH6m4zgZ/CPvWBOkZc+c
1Po2EmvBz+AD5sBdT5kzGQA6NbWyZGldxRthNLOs1efOhdnWFuhI162qmcflgpiI
WDuwq4C9f+YkeJhNn9dF5+owm8cOQmDrV8NNdiTqin8q3qYAHHJRW28glJUCZkTZ
wIaSR6crBQ8TbYNE0dc+Caa3DOIkz1EOsHWzTx+n0zKfqcbgXi4DJx+C1bjptYPR
BPZL8DAeWuA8ebudVT44yEp82G96/Ggcf7F33xMxe0yc+Xa6owIDAQABoAAwDQYJ
KoZIhvcNAQEFBQADggEBAB0kcrFccSmFDmxox0Ne01UIqSsDqHgL+XmHTXJwre6D
hJSZwbvEtOK0G3+dr4Fs11WuUNt5qcLsx5a8uk4G6AKHMzuhLsJ7XZjgmQXGECpY
Q4mC3yT3ZoCGpIXbw+iP3lmEEXgaQL0Tx5LFl/okKbKYwIqNiyKWOMj7ZR/wxWg/
ZDGRs55xuoeLDJ/ZRFf9bI+IaCUd1YrfYcHIl3G87Av+r49YVwqRDT0VDV7uLgqn
29XI1PpVUNCPQGn9p/eX6Qo7vpDaPybRtA2R7XLKjQaF9oXWeCUqy1hvJac9QFO2
97Ob1alpHPoZ7mWiEuJwjBPii6a9M9G30nUo39lBi1w=
-----END CERTIFICATE REQUEST-----
```

Figure 7: Sample CSR

[10] Note: "Robust" is the term given in [2] for PMF-protected management frames.

© 2019 Wi-Fi Alliance. All Rights Reserved.

9.1.2 How to Get a Certificate Signing Request (CSR)

9.1.2.1 Applicant Generated Key Pair

From the server on which the certificate is to be installed, the applicant generates a key pair (public key and private key). The server public key is used to encrypt sensitive data that is sent to the server. The server private key is used to decrypt that sensitive data. The private key always remains on the server. If the private key is lost (removed or deleted from the server), the OSU Server Certificate becomes useless because the sensitive data can no longer be decrypted. Note that when the OSU Server Certificate is installed on the server, the certificate is paired with the private key that corresponds with the public key that was included in the CSR.

9.1.2.2 Applicant Generated CSR

From the same server used to generate the key pair, the applicant generates a CSR. When the CSR is generated, most server software requests the following information: Common name, organization, organization location (city/locality, state/province, and country/region), key type, and bit size.

The common name is the name through which the OSU Server Certificate is to be accessed; this is usually the fully-qualified domain name (e.g. *www.example.com* or *mail.example.com*). The organization is the legally registered name of your organization/company. The key type is RSA *(Ron Rivest, Adi Shamir, and Leonard Adleman).* Bit size for RSA key types is 2048 bit (or higher).

9.1.2.3 Process for Generating the Key Pair and CSR

The process for generating the key pair and the CSR are dependent upon the operating system (i.e. Windows, Linux, etc.) and webserver software (e.g. IIS, Apache, etc.). For example, when generating a CSR on a Windows server using IIS 8, the key pair and CSR are created at the same time. When generating a CSR on an Apache server with OpenSSL, the key pair and CSR can be generated separately or together depending on which commands are run.

After the key pair and CSR are created, the CSR will contain the matching public key and other information like your organization's name, location, and domain name. The applicant can now order the Hotspot 2.0 OSU Server Certificate.

Sample CSR Creation Instruction

How to Create a CSR on Windows Server 2012 R2 - IIS 8.5

I. Open Internet Information Services (IIS) Manager.
II. In **Internet Information Services (IIS) Manager**, under **Connections**, click your server's Hostname.
III. In the center menu, in the **IIS** section, double-click the **Server Certificates** icon.
IV. In the **Actions** menu, click **Create Certificate Request** to open the **Request Certificate** wizard.
V. On the **Distinguished Name Properties** page, enter the following information:

- **Common name** — Enter the name that will be used to access the certificate. This name is usually the fully-qualified domain name. For example, *www.example.com* or *mail.example.com*.
- **Organization** — Enter the legally registered name of your organization/company.
- **Organizational Unit** — Enter the name of your department within the organization. For example, you can enter IT or Web Security. You can also leave the text box blank.

© 2019 Wi-Fi Alliance. All Rights Reserved.

- **City/locality** Enter the city in which your organization/company is located.
- **State/province** Enter the state/province in which your organization/company is located.
- **Country/region** Type or select your two-digit country code from the drop-down list.

VI. On the **Cryptographic Service Provider Properties** page, enter the following information:

- **Cryptographic service provider** In the drop-down list, select **Microsoft RSA SChannel...**, unless you have a specific cryptographic provider.
- **Bit length** In the drop-down list, select **2048**.

VII. On the **File Name** page, click the **…** box to browse to a location where you want to save the CSR file, enter the filename, and then click **Open**.

- If you only enter the filename without selecting a location, your CSR file is saved to the following location: C:\Windows\System32.
- Make sure to note the filename and the location where you saved your CSR file. You need to open this file as a text file, copy the entire body of the text file (including the **Begin New Certificate Request** and **End New Certificate Request** tags), and paste it into the online order process when you are prompted.

VIII. Click **Finish**.

For detailed instructions about creating a CSR, refer to the OS and software companies' instructions. These instructions may be provided with the product, or they may be available on the company's website.

CAs often provide basic instructions for creating a CSR. In addition, CAs may also provide tools to help simplify the CSR creation process (and OSU Server Certificate management). These instructions and tools may be available on the CAs' website.

For information about Wi-Fi Alliance -authorized CAs, refer to [7]

9.2 Ordering the Hotspot 2.0 OSU Server Certificate

9.2.1 Select a Certificate Authority (CA)

Before a Server Certificate can be ordered (and purchased), it is important to select a "Wi-Fi Alliance authorized" CA.

OSU Server Certificates can only be ordered (and purchased) from "Wi-Fi Alliance-authorized" CAs. Wi-Fi Alliance-authorized CAs are required to adhere to certain standards, meet audit requirements, and ensure their root certificate is trusted by the connection manager of the mobile device. Hotspot 2.0 OSU Server Certificates are issued by Wi-Fi Alliance-authorized CAs.

Wi-Fi compatible devices will come with a pre-installed list of authorized CAs. These CAs have a root certificate in the mobile device's trusted root store. An OSU Server Certificate issued by a CA to an organization and its domain/Wi-Fi hotspot verifies that a trusted third party (the CA) has authenticated the certificate issued to that organization. Since the mobile device's connection manager trusts the CA, the device now trusts that organization's identity too. Passpoint mobile devices will only connect to OSU servers having a certificate issued by one of the Wi-Fi Alliance-authorized CAs.

There is a select number of Wi-Fi Alliance-authorized CAs from which a Hotspot 2.0 OSU Server Certificate may be purchased. For information about authorized CAs, refer to [7]

© 2019 Wi-Fi Alliance. All Rights Reserved.

9.2.2 Order a Hotspot 2.0 OSU Server Certificate

After the key pair and CSR are generated and a CA has been selected from which to purchase the OSU Server Certificate, the applicant should visit the CAs website and follow the directions for ordering a Hotspot 2.0 OSU Server Certificate.

Example of an OSU Server Certificate Order Process:

1. **Product**

   Participating CAs should make Hotspot 2.0 OSU Server Certificates one of the products that can be easily accessible for purchase.

2. **Validity Period**

   A Hotspot 2.0 OSU Server Certificate lifespan ranges from 1 to 2 years.

3. **Name to Secure**

   Common name that is to be secured; this name is usually the fully-qualified domain name. For example, *www.example.com* or *mail.example.com*

4. **Service Provider Icon/Logo(s)**

   Enter the logo(s) URL to be used for the Hotspot 2.0 OSU Server Certificate.

   A variety of logos can be included to accommodate the different languages. A Wi-Fi compatible mobile device will select the appropriate language based on the client's settings. If the logo for the client's language is not available, the client will use the specified default language. Hotspot 2.0 OSU Server Certificates and devices support non-Roman character sets.

5. **Service Provider Friendly Name(s)**

   Enter the friendly name(s) to be used for the Hotspot 2.0 OSU Server Certificate.

   Like logos, friendly names can be provided in multiple languages. A Wi-Fi compatible mobile device will select the appropriate language based on the client's settings. Friendly names can be provided in non-Roman character sets.

9.2.3 Hotspot 2.0 OSU Server Certificate Validation

CAs verify information about the organizations applying for a certificate. OSU Server Certificates not only create secure and encrypted OSU server connections, but they also indicate the legitimacy of the Hotspot and the company behind it. As ecommerce expands, customer trust is essential to financial success, customer conversion, and business growth. When issuing a Hotspot 2.0 OSU server certificate, the issuing CA follows an approved procedure to validate fields that describe the identity of the OSU server. This validation provides assurance that the names, DNS address and icons used to identify the server are owned and controlled by the requesting entity.

The process used to verify each applicant is specified in the applicable CA's Certification Practice Statement, which is available on each CA's website. For more details, refer to [7]

© 2019 Wi-Fi Alliance. All Rights Reserved.

9.3 Installing the Hotspot 2.0 OSU Server Certificate

After the CSR is created, the certificate is purchased, and the validation process is completed, the CA provides the applicant with their Hotspot 2.0 OSU Server Certificate, typically through email or via a download in the account. The applicant is responsible for installing the certificate on the OSU server, but some CAs may provide assistance with this process or tools that automate the process.

This process requires installing intermediate certificates that are part of the certificate chain. These intermediate certificates help establish a chain of trust between the OSU Server Certificate and the CA's OSU Server Root Certificate.

© 2019 Wi-Fi Alliance. All Rights Reserved.

Figure 8: Certificate Examples

9.3.1 Hotspot 2.0 OSU Server Certificate Installation

The process for installing the certificate and related chain is dependent upon the operating system (i.e. Windows, Linux, etc.) and webserver software (e.g. IIS, Apache, etc.).

Sample Server Certificate Installation Instruction

Lync 2010: Installing your SSL Certificate

1. On the Windows **Start** menu, click All **Programs > Microsoft Lync Server 2010 > Lync Server Deployment Wizard**.
2. In the **Lync Server 2010 – Deployment Wizard**, click **Install or Update Lync Server System**.

© 2019 Wi-Fi Alliance. All Rights Reserved.

3. Under **Step 3: Request, Install, or Assign Certificates**, click **Run**.
4. In the **Certificate Wizard**, select **External Edge certificate (public internet)** and then click **Import Certificate**.
5. On the **Import Certificate** page, enter or browse for the location of the certificate file.
   If you used the Lync interface to create the CSR, the certificate file is a .cer file (i.e. *yourdomain_com.cer*).
   If you are using a .pfx file, check **Certificate file contains certificate's private key**.
   If you are using a .cer file, do not check this box.
6. Click **Next**.
7. On the **Import Certificate Summary** page, verify that the information is correct, and then click **Next**.
8. On the **Executing Commands** page, verify that the **Task status** is **Completed**, and then click **Finish**.
9. In the **Certificate Wizard**, select **External Edge certificate (public internet)** and then click **Assign**.
10. On the **Certificate Assignment** page, click **Next**.
11. On the **Certificate Store** page, click **View Certificate Details** to verify that you installed the correct certificate.
12. In the **Certificate** window, review the certificate information, and then click **OK**
13. On the **Certificate Store** page, click **Next**
14. On the **Executing Commands** page, verify that the **Task status** is **Completed**, and then click **Finish**.
15. On the **Certificate Store** page, click **Next**.
16. To verify that your certificate was properly installed, in the Certificate Wizard, make sure that the status of the **External Edge certificate (public internet)** is **Assigned**.
17. Your SSL certificate has been successfully installed and assigned.

For detailed instructions about installing an OSU Server Certificate, refer to the OS and software companies' instructions. These instructions may be provided with the product, or they may be available on the company's website.

CAs often provide basic instructions for installing an OSU Server Certificate. In addition, CAs may also provide tools to help simplify the certificate installation process (and OSU Server Certificate management). These instructions and tools may be available on the CAs' website.

For information about Wi-Fi Alliance-authorized CAs, refer to [7]

9.3.2 Check OSU Server Certificate Installation

Once the OSU Server Certificate is installed, the applicant should check that everything is working correctly. Contact your CA for assistance in checking the certificate installation.

9.3.3 OSU Server Certificate Back Up

Applicants should also back up the certificate. The process for backing up the OSU Server Certificate is dependent upon the operating system (i.e. Windows, Linux, etc.) and webserver software (e.g. IIS, Apache, etc.).

Sample OSU Server Certificate Back Up Instruction

Exporting/Backing Up to a .pfx File

Before the OSU Server Certificate can be exported as a .pfx file, it's first installed on the server from which the CSR was generated.

1. From the **Start** screen, type and then click **Run**.
2. In the **Run** window, in the **Open** box, type *mmc* and then, click **OK**.

© 2019 Wi-Fi Alliance. All Rights Reserved.

3. In the **User Account Control** window, click **Yes** to allow the Microsoft Management Console to make changes to the computer.
4. In the **Console** window, in the menu at the top, click **File > Add/Remove Snap-in**.
5. In the **Add or Remove Snap-ins** window, under **Available snap-ins** (left side), click **Certificates** and then, click **Add**.
6. In the **Certificates snap-in** window, select **Computer account** and then, click **Next**.
7. In the **Select Computer** window, select **Local computer: (computer this console is running on)**, and then, click **Finish**.
8. In the **Add or Remove Snap-ins** window, click **OK**.
9. In the **Console** window, in the **Console Root** section, expand **Certificates (Local Computer)**, expand the folder that contains the certificate that you want to export/back up, and then, click the associated **Certificates** folder.
   Note: Your certificate will be in either the **Personal** or the **Web Hosting** folder.
10. In the center section, right-click on the certificate that you want to export/back up and then, click **All Tasks > Export** to open the **Certificate Export Wizard**.
11. On the **Welcome to the Certificate Export Wizard** page, click **Next**.
12. On the **Export Private Key** page, select **Yes, export the private key**, and then, click **Next**.
13. On the **Export File Format** page, select **Personal Information Exchange**, check **Include all certificates in the certification path if possible**, and then, click **Next**.
    Warning: Do not select **Delete the private key if the export is successful**.
14. On the **Security** page, check **Password**, enter and confirm your password, and then, click **Next**.
15. On the **File to Export** page, browse to and select the file that you want to export/back up and then, click **Next**.
    Make sure to note the filename and the location where you saved your file.
    If you only enter the filename without selecting a location, your file is saved to the following location: **C:\Windows\System32**.
16. On the **Completing the Certificate Export Wizard** page, verify that the settings are correct and then, click **Finish**.
17. You should receive *"The export was successful"* message.
    The .pfx file is now saved to the location that you selected.

For detailed instructions about backing up an OSU Server Certificate, refer to the OS and software companies' instructions. These instructions may be provided with the product, or they may be available on the company's website.

For information about Wi-Fi Alliance-authorized CAs, refer to [7]

9.4 Hotspot 2.0 OSU Certificate Revocation

9.4.1 Circumstances for Revocation

Revocation of a certificate permanently ends the operational period of the certificate prior to the certificate reaching the end of its stated validity period. Prior to revoking a certificate, the CA may first require the requester to confirm their authorization over the certificate.

9.4.2 Who Can Request Revocation

CAs typically accepts revocation requests from authenticated and authorized parties, such as the certificate holder or an affiliated organization. Other entities may request certificate revocation for fraud or misuse by contacting the CA.

9.4.3 Explanation of OCSP and Revoked Certificates

CAs revoke OSU Server Certificates using OCSP. A revoked certificate will have its status pushed out to the CA's OCSP Server. OSU servers can obtain Hotspot 2.0 OSU Server Certificate status information by querying the issuing CA's OCSP server using the certificate's

© 2019 Wi-Fi Alliance. All Rights Reserved.

serial number and relay this information to mobile devices during TLS setup (aka OCSP stapling). OCSP locations are specified in the certificate's Authority Information Access field.

10. Subscription Remediation

During the lifetime of a user's subscription some elements of the subscription may change requiring remediation of the subscription. Subscription remediation is the process that Home Service Providers use to correct, update, and resolve subscription issues. There are two methods at the disposal of Home SPs. Mobile device initiated update based on the device SubscriptionUpdate settings and Home Service Provider initiated remediation that is initiated for updates or resolution of subscription issues.

10.1 Mobile Device Initiated Subscription Update

The mobile device initiated subscription update is used by the Home Service Provider to allow for periodic update of the mobile device subscriber's configuration. The details of this method are defined in section 5.3 Subscription Update initiated by the mobile device will only update the device subscription configuration and not network-selection policy.

10.2 Service Provider Initiated Remediation

The Service Provider initiated remediation process allows the Service Provider to trigger the resolution or implementation of items in the subscription at the time of the user's authentication by the Service Provider's AAA. The remediation process may or may not require user interaction to complete the remediation. There are two classes of remediation; machine remediation and user remediation.

- Machine remediation is the remediation process that does not require user intervention, example of machine remediation is updating the mobile device subscription configuration.
- User remediation is the process where user interaction is required; examples of user remediation is updating service agreement or billing information.

While both the machine and user classes of remediation are trigged immediately after AAA authentication neither the machine nor the user classes directly initiate the remediation.

The Service Provider should not use the User remediation class unless the remediation action fully requires user interaction; this is to ensure automatic and seamless remediation from the point of view of the user. Examples where user class remediation would be used are when the user has to accept a change in the service agreement or entering of billing information such as a credit card number.

Subscription remediation should not be confused with mobile device initiated remediation or update; Mobile device subscription update is intended to only update the mobile device's subscription configuration and is set to happen at a predetermined interval as indicated in the mobile device subscription configuration.

10.3 Remediation Actions

The Service Provider determines the condition when user subscription remediation is needed and if the remediation needs to be done at the time of the next user's AAA authentication or at the subscription update time as defined in the mobile device subscription configuration. The remediation actions include items such as an update to a service/privacy agreement, modifications to the mobile device subscription configuration, accounting or billing resolution. Accounting resolution can include renewing of the subscription based on time or data usage. Billing resolution includes renewing of billing information, billing resolution, or general user information update. Note that during mobile device initiated remediation, only the mobile device

© 2019 Wi-Fi Alliance. All Rights Reserved.

subscription configuration can be updated, all other subscription remediation is done using Service Provider initiated remediation.

During remediation the mobile device should be restricted to only having access to the remediation server to prevent the user from bypassing the act of remediation once the user authentication is completed. This can be accomplished by the Hotspot Operator imposing network access restrictions using access control lists in its networking equipment. The need for network access restrictions (during remediation) can be indicated in the RADIUS Access-Accept attributes.

When the Service Provider has determined subscription remediation is needed, the Service Provider needs to ensure that the remediation server is configured to handle the remediation before triggering remediation. This is to ensure that when remediation is triggered, remediation can be completed successfully. If the update is for the mobile device subscription configuration, then updating subscription database should trigger the AAA to signal the device that remediation is needed. For other types of remediation, the remediation server should be used to trigger the AAA to request remediation.

10.4 Network Access or Reauthentication Remediation Flow

During user access to the network, remediation can be triggered at the end of the EAP authentication by the AAA server including the Hotspot 2.0 subscription remediation needed tuple as part of the RADIUS Access-Accept message. If remediation is not possible as determined by the Home SP then the AAA should not authenticate the subscription and return an access-reject. Once the device receives the remediation needed message, the device will then start the remediation process by contacting the remediation server using the server method and URI as defined in the mobile device subscription's SubscriptionUpdate section.

Examples of reasons that remediation may not be possible include the home service provider wishes to have remediation to only happen over select networks or partners. Home service provider will have to determine the policies and conditions in which remediation is allowed or not allowed.

10.5 Remediation Server Authentication

The device is authenticated to the remediation server by one of the three following options:

- HTTP Digest using the username and password that was used to authenticate to the access network
- HTTP Digest using the username and password that is held in the mobile device subscription configuration as the SubscriptionUpdate/UsernamePassword section in the PPS MO. This option is recommended for devices connecting using SIM cards.
- TLS using the device certificate that was used to authenticate to the access network.

The method used is determined by the server method in the mobile device subscription configuration. If the operator plans on using the HTTP Digest option as described in the second bullet above, the operator first configures the SubscriptionUpdate/UsernamePassword elements in the mobile device's PPS MO.

11. Traffic Management

Disassociation Imminent and Deauthentication Imminent are traffic management features provided to operators by Hotspot 2.0 compatible networks. Disassociation Imminent functionality, can be used to notify users that their session is about to expire and as a result of which they will be disassociated from the network. Deauthentication Imminent can be used to deauthenticate users and prevent them from retrying authentication for a certain amount of time dictated by the network.

© 2019 Wi-Fi Alliance. All Rights Reserved.

11.1 Disassociation Imminent

The Disassociation Imminent feature provides the operator with the capability to effectively terminate the association between the AP and the mobile device Furthermore, hotspot certified AP enables the operator to notify the user before their session is terminated and also provide them with additional information possibly regarding the cause of the termination and, if feasible, ways to avoid it. There are numerous reasons why the operator might want to terminate a user's session and some of those include:

- The user's subscription is approaching its limits (either in terms of consumed amount of data, if the subscription is traffic-based, or in terms of used service time, if the subscription is duration-based)
- The user is generating significant amount of traffic, which causes the performance of other users connected to the network to degrade
- The user is browsing illegal content or routing traffic that is not allowed by the operator
- User subscription profile prioritization (e.g., if a bronze user is connected to an AP, but at a certain point several new gold users request connection and there is not enough capacity to support both the gold and the bronze users, the bronze might be disassociated by the operator and given a possibility to upgrade their subscription type)

Depending on the reason for the disassociation, the operator can configure a Session Warning Time to an appropriate value in order to give the user the opportunity to react. For example, if the user's prepaid data subscription is about to expire, the operator can provide the user with the opportunity to extend their subscription well before the subscription cap is reached (e.g., 10 minutes) so that the user can have time to purchase the session extension. However, if the user is routing traffic that is not allowed by the operator, the operator can provide a shorter amount of time for the user to terminate the disallowed traffic (e.g., 1 minute) before terminating their association.

The operator provides the additional information regarding the reason for the disassociation via a Session Information URL pointing to a webpage (the content of the webpage is defined solely by the operator). Once the Disassociation Imminent is sent to the mobile device, the mobile device could launch a browser to the received URL and notify the user. If the operator would like to make use of the Session Information URL features, a HTTP server is deployed in the operator's network, reachable from all the APs where the Disassociation Imminent feature will be used.

11.2 Deauthentication Imminent

In certain situations, a Hotspot Operator might want to deauthenticate some users from the network and notify them that they are not authorized to use the network services at this location at this particular time. Furthermore, the operator might want to keep the users deauthenticated for certain duration. In such situation, the operator can make use of the Deauthentication Imminent feature, which provides the capability to deauthenticate certain mobile device and instruct it on the amount of time to wait before the a subsequent authentication will be allowed by the network. There could be many reasons why the operator would like to use this feature and some of them include:

- Temporary degradation in the network conditions that require some of the users to be removed from the network for a certain amount of time even though they have valid subscriptions and have carried a successful authentication. Such conditions might include congestion in the Wi-Fi access network or congestion on a node in the mobile device's core network (e.g., the home subscriber server, HSS)
- The user is no longer authorized to use the Passpoint network at the time and/or location where the Deauthentication Imminent Notice was received

When deauthenticating a mobile device the operator can optionally provide a reason informing the user on the reason for the deauthentication. In this case the operator provides a Reason URL pointing to a webpage, containing additional information (the content of the webpage is defined

© 2019 Wi-Fi Alliance. All Rights Reserved.

solely by the operator). Upon reception of the URL, the mobile device might either launch a browser to the URL or provide information on its user interface. In order to make use of the Reason URL, the operator deploys an HTTP server that is reachable from all the APs where the Deauthentication Imminent feature will be used.

If the operator chooses to provide an authentication retry period, the mobile device will obey that period and will not try to reauthenticate with the network.

12. Free Public Hotspot 2.0-Based Hotspots

Hotspot Operators may provide Hotspot 2.0-based free, public, hotspot service. In this particular service, Hotspot Operators have the need to ensure hotspot users have accepted the terms and conditions governing their hotspot's use, but are not interested in knowing (or do not wish to know/track) any particular user's identity. This functionality is provided by Hotspot 2.0 Release 2 infrastructure. The Hotspot Operator configures their infrastructure as follows:

1. The user in a Free Public Hotspot initiates the online sign-up registration process with the Free Public Hotspot's OSU server.
2. During the registration exchange, the OSU server presents the terms and conditions to the user.
3. If the user accepts the terms and conditions, the OSU server issues a credential; if the user refuses, no credential is provisioned. Note that the same credential is issued to all users which have accepted the terms and conditions; therefore, the Hotspot Operator cannot track the identity of an individual user during the Hotspot 2.0 Access state (see section 6).
4. When the user/mobile device returns to the same Free Public Hotspot, the previously provisioned credentials are used to provide secure, automatic access. The mobile device authenticates using EAP-TTLS, which provides for the generation of unique cryptographic keying material even though users share a common password.

If the terms and conditions change, then the user is taken through a subscription remediation process during which the new terms and conditions are presented. If the user accepts the changed terms and conditions, then a new credential is provisioned.

13. Backwards Compatibility of Passpoint Hotspots

Many Hotspot Operators have existing hotspot deployments that employ open SSIDs and captive portals for authentication. Some Hotspot Operators have existing hotspots that employ WPA2-Enterprise security. These legacy Hotspot Operators may want to add Passpoint APs to their base of installed networks to provide secure and automatic network discovery and selection for their customers while at the same time continuing to operate legacy deployments to provide a service for their existing customers. This section of the deployment guide discusses the interaction of Passpoint deployments with legacy deployments that use non-Passpoint APs.

13.1 Operation of Passpoint Mobile Devices and Legacy Hotspots

Hotspot Operators with legacy hotspots – employing, for instance, an open SSID with captive portal authentication – may have the ability to add a second SSID that supports Passpoint functionality and keeps Passpoint traffic separate, as shown in Figure 9. This can be done by

© 2019 Wi-Fi Alliance. All Rights Reserved.

using the multiple-BSSID feature available in many commercial-grade APs. APs having this capability can transmit the second Passpoint SSID using the same radio hardware used for transmitting the existing SSID. If APs do not support multiple BSSIDs, a second set of APs is needed to provide Passpoint functionality. The legacy and Passpoint SSIDs are configured with different values (i.e., different names) to preserve network security and also keep the networks and the broadcast domains separate.

Legacy Hotspot Operators with APs that support WPA2-Enterprise can upgrade their hotspots to use Passpoint APs without causing backward compatibility issues. The SSID used for the network configured for WPA2-Enterprise can remain in use for the Passpoint network. There is no need to have separate SSIDs for Passpoint hotspots and legacy hotspots that support WPA2-Enterprise.

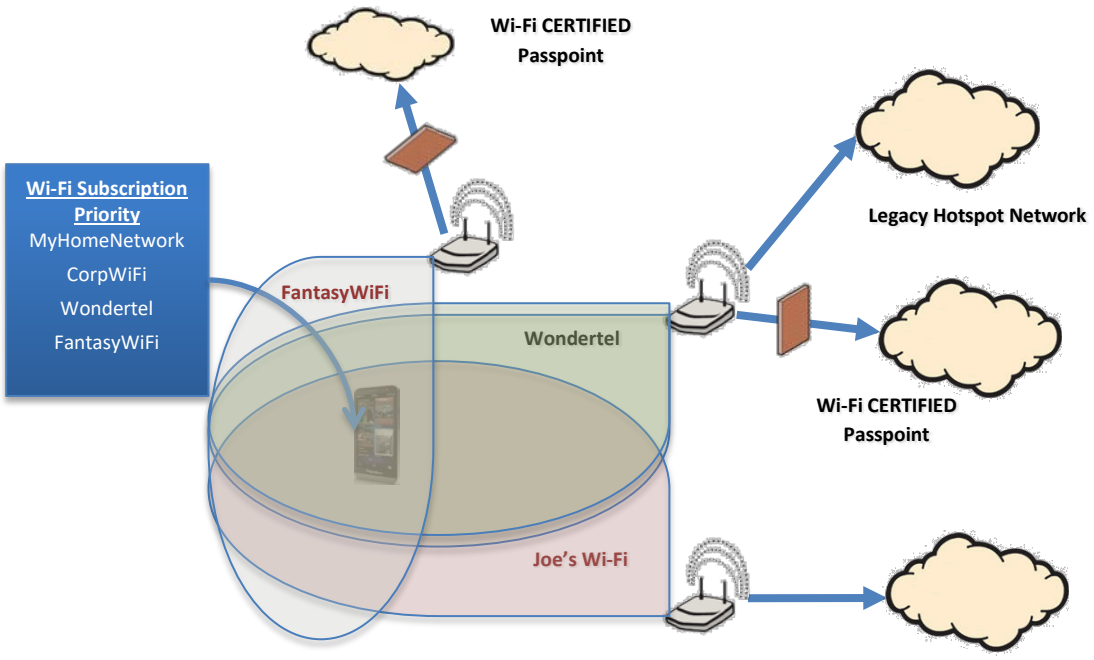

Figure 9: Multiple Passpoint Hotspots with Legacy Hotspots

13.2 Passpoint Mobile Device Operation in a Legacy Hotspot

A Passpoint mobile device is capable of connecting to legacy networks. Passpoint (Release 1 or Release 2) mobile devices negotiate Hotspot 2.0 Release 1 or Release 2 features when they connect with a Passpoint AP. Therefore, mobile devices connecting with APs that do not advertise Hotspot 2.0 capability (aka legacy APs) will not employ any Hotspot 2.0-specific features and are therefore backwards compatible with legacy hotspots.

A Passpoint device will automatically connect to a legacy network if legacy networks are preferred by the user. The ability of the device to automatically connect to non-user preferred legacy networks is dependent on the device implementation.

Legacy mobile device behavior is dependent on the device's capabilities for authenticating with legacy networks and is not part of the Passpoint certification testing.

Mobile devices, upon entering a hotspot with one Passpoint SSIDs and one legacy SSID, will have the following behavior:

- Passpoint mobile devices will automatically select and join the Passpoint network, unless the legacy network is preferred by the user.

© 2019 Wi-Fi Alliance. All Rights Reserved.

- Legacy mobile devices will continue to join the open SSID network and authenticate to the captive portal. If the mobile device has a third-party connection manager or native captive portal capability, the authentication step may be automatic. Typically, the authentication is automatic if the legacy hotspot is operated by the mobile device's Home SP or if the user has previously authenticated to that hotspot. Otherwise, user intervention is likely to be required. Additionally, user intervention is typically required in a roaming environment where the hotspot is not operated by the Home SP and additional steps are required to identify and authenticate with the Home SP (drop-down windows in the captive portal interface, etc.).
- If the legacy mobile device is WPA2-Enterprise certified and WPA2-Enterprise is activated, when the device detects an SSID from a Passpoint network, it will announce the presence of that SSID to the user. The user can then manually enter the Home SP username/password credentials to join the Passpoint network. In this scenario, the user enjoys stronger security than in the legacy authentication. A mobile device with WPA2- Enterprise credentials already configured for a particular SSID will automatically attempt to connect to a Passpoint AP using the same SSID. This enables existing devices already using EAP-SIM to continue to connect to APs that have been upgraded to Passpoint without the need for additional SSIDs.

Upon entering a hotspot composed exclusively of Passpoint APs, mobile devices have the following behavior:

- Passpoint mobile devices automatically select and join the Passpoint network.
- Legacy mobile devices that do not support WPA2- Enterprise are not able to connect to Passpoint hotspot networks.
- On first-time connection, legacy WPA2-Enterprise mobile devices are able to join the Passpoint network manually; thereafter, they can join automatically, as described above.

13.3 Passpoint SSID Configuration for Release 2

The online sign-up (aka credential provisioning) feature in Release 2 of Passpoint requires the use of an additional SSID (i.e., beyond the WPA2-Enterprise SSID for authenticated mobile devices); this SSID is referred to, for the purposes of this document, as the OSU SSID. It's up to the discretion of the Hotspot Operator whether to support online sign-up. When supported, the Hotspot Operator has several choices for configuring the OSU SSID:

- An OSEN SSID as described in section 8.7; this choice adds a new SSID to the hotspot. The OSEN SSID provides a secure connection which better protects mobile devices from attackers. Note that communications between the mobile device and OSU server use HTTPS and are thus protected from eavesdropping and other attacks. However, once the Wi-Fi link is up, mobile devices typically enable their IP networking function, allowing embedded applications the opportunity to communicate with servers on the Internet. OSEN provides link-layer security for these communications.
- If the hotspot already has an open SSID for public Wi-Fi access, that SSID can be shared between legacy and online sign-up operations.
- A dedicated, open SSID; this choice adds a new SSID to the hotspot.

13.4 Passpoint (Release 2) Mobile Device Operation with Passpoint (Release 1) Hotspot

Passpoint (Release 1 or Release 2) mobile devices negotiate Hotspot 2.0 Release 1 or Release 2 features when they connect with a Passpoint AP. Therefore, mobile devices connecting with a Passpoint (Release 1) capable AP will only be able to negotiate Release 1 features[11]. Passpoint

[11] This does not apply to any features which are not part of Hotspot 2.0.

© 2019 Wi-Fi Alliance. All Rights Reserved.

(Release 1) mobile devices will only be able to perform the discovery and access states as described in sections Figure 4 and 6 respectively.

Many Hotspot Operators will have existing hotspot deployments that utilize Passpoint (Release 1) equipment. Passpoint (Release 1) assumes that a mobile device is provisioned with a security credential by some other means

13.5 Passpoint (Release 1) Mobile Device Operation with Passpoint (Release 2) Hotspot

Passpoint (Release 1 or Release 2) mobile devices negotiate Hotspot 2.0 Release 1 or Release 2 features when they connect with a Passpoint AP. Therefore, Passpoint (Release 2) capable APs accepting connections with Passpoint (Release 1) mobile devices will restrict themselves to use only Release 1 features[12] with those mobile devices. Passpoint (Release 2) capable APs can concurrently provide Release 1 and Release 2 features to associated Release 1 and Release 2 mobile devices respectively.

Note: Release 2 infrastructure (that supports WPA2-Enterprise and Passpoint (Release 1) mobile devices) should be configured in a manner that supports non-PMF mobile device connectivity.

14. Appendix A: Hotspot Operator's Network Security

The Passpoint program contains security features focused on improving the security between the mobile device and the Passpoint AP. However, when Passpoint APs are deployed as part of a Hotspot Operator's network, there are additional security considerations to keep in mind to improve overall network security.

The purpose of this section is to raise awareness of various hotspot network security issues so Hotspot Operators can address them as needed for their particular deployment situations. Hotspot Operators should also refer to their AP manufacturer's deployment and configuration guides and to relevant technical publications to address specific security issues.

14.1.1 Physical Security

A Passpoint AP can be deployed at both secure and insecure premises. Secure premises are locations where the AP is not physically accessible to an attacker and hence the equipment cannot be tampered with. At insecure premises, the AP is physically accessible to an attacker, which is often the case in an outdoor deployment.

For a public hotspot deployment, it is important to prevent physical access to APs by unauthorized persons. Access to APs by unauthorized persons could lead to security breaches. Examples of such breaches are:

- Theft. APs can contain shared secrets used, for example, to authenticate to external servers such as the AAA server via RADIUS. A stolen shared secret could enable an attacker to eavesdrop on trusted communications or to add a rogue device.
- AP resetting. Resetting an AP typically reverts the AP configuration to the out-of-the-box configuration. This can leave WPA2-Enterprise security, as well as other features necessary for secure and reliable hotspot operation, disabled.
- Attachment of a device to an unused wired port on the AP. If there is an open console port or Ethernet port, an attacker could use it to reconfigure the AP or steal Internet access.

[12] This does not apply to any features which are not part of Hotspot 2.0.

© 2019 Wi-Fi Alliance. All Rights Reserved.

For deployments at insecure premises, the overall security of a Hotspot Operator network using APs can be enhanced by hardening the AP against physical attacks. This typically means that the number of access ports on the device has to be minimized and all processing relating to authentication, encryption and booting processes has to occur in a secure environment within the AP. A secure environment can be created by, for example, invoking password-protected configurations of the AP.

14.1.2 AP Management

Passpoint AP management can be done remotely or locally. This deployment guide assumes that the Hotspot Operator security provisions are such that the AP software and configuration parameters of a Passpoint AP can be changed only by trusted parties and that only known management hosts can establish a connection to the management interface. Moreover, any communication related to the AP management is expected to be secure.

14.1.3 Network Security beyond the AP

A variety of hotspot network architectures and backhaul connection possibilities exist. User data can be securely transmitted between a mobile device and a Passpoint AP using WPA2-Enterprise security. However, beyond the AP, transfer of data to other components such as a firewall or edge router also needs to be performed securely. Secure transfer can be facilitated by restricting physical access to these devices or by using secure transport protocols (e.g., IPsec).

14.1.4 Backhaul Security for Hotspot Networks

In some hotspot networks, the Hotspot Operator may route all the user traffic to the Internet upon egress from its firewall. This provides a level of security that is roughly equivalent to that in a typical residential network or in many enterprise networks.

A Hotpot 2.0 operator may also establish a secure link from a Passpoint AP to a Home SP core network or a roaming partner’s core network. For such a deployment, a secure connection extends from the Passpoint AP or edge router to a security gateway in the SP’s core network via a secure backhaul connection that can provide integrity, confidentiality and replay protection of the transmitted data.

14.1.5 AP Authentication

It is recommended that the Hotspot Operator require authentication of any AP connecting to the network. This is important to identifying malicious devices trying to connect to the network and perform a man-in-the-middle attack.

© 2019 Wi-Fi Alliance. All Rights Reserved.