Hotspot 2.0 (Release 2)
Online Sign-Up
Certificate Policy Specification

Version 1.2

This document is a specification in the
Wi-Fi Alliance Wi-Fi CERTIFIED Passpoint™ (Release 2) program,
a solution for next generation Wi-Fi® hotspots.

Document History

Version	Date	Status	Comments
1.0	2014-08-08	Final	Public release version
1.1	2015-02-03	Final	Editorial fixes to section 2 (References)
1.2	2017-07-26	Final	Table 2 – Changed subject ID# 02 from Verizon to Reserved

Table of Contents

List of Figures

List of Tables

1 Overview

This document provides requirements defining the format and issuing process of public key certificates used for Online Sign-Up (OSU) in the Wi-Fi CERTIFIED Passpoint™ (Release 2) program.

1.1 Scope

The requirements documented herein specifically address the needs of the Hotspot 2.0 (Release 2) specification [12]. The scope of this specification includes:

- A profile of X.509 Certificates used for Online Sign-Up that documents constraints on the allowable certificate fields. The certificate profile includes specification of:
  - Trust Root certificates for OSU
  - Intermediate CA certificates for OSU
  - OSU server certificates
- Requirements on the issuing Certificate Authority for verification of identity information and correspondence between identified entities and the fields in the certificate.
- Requirements for revocation support using the OCSP protocol.

Hotspot 2.0 also uses certificates to authenticate the AAA servers. The requirements for AAA certificates are not in scope of this specification.

1.2 Background

Online sign-up (OSU) is the process by which a mobile device registers with a service provider, enabling a user to select a plan with which to obtain network access, and is then provisioned with the credentials necessary to securely connect to an access network. An example network architecture for online sign-up is shown in Figure 1. Each SP network has an OSU server, an AAA server, and (access to) a CA. These devices can be co-located or separate. If they are separate, the communication between them is outside the scope of this document and is assumed to be secure (the entities are authenticated and communication between them is confidentiality and integrity protected). The hotspot has its own AAA server, and optionally an OSU server. The hotspot's switch is configured to only allow https traffic to OSU servers in home SP networks that are supported by the hotspot.

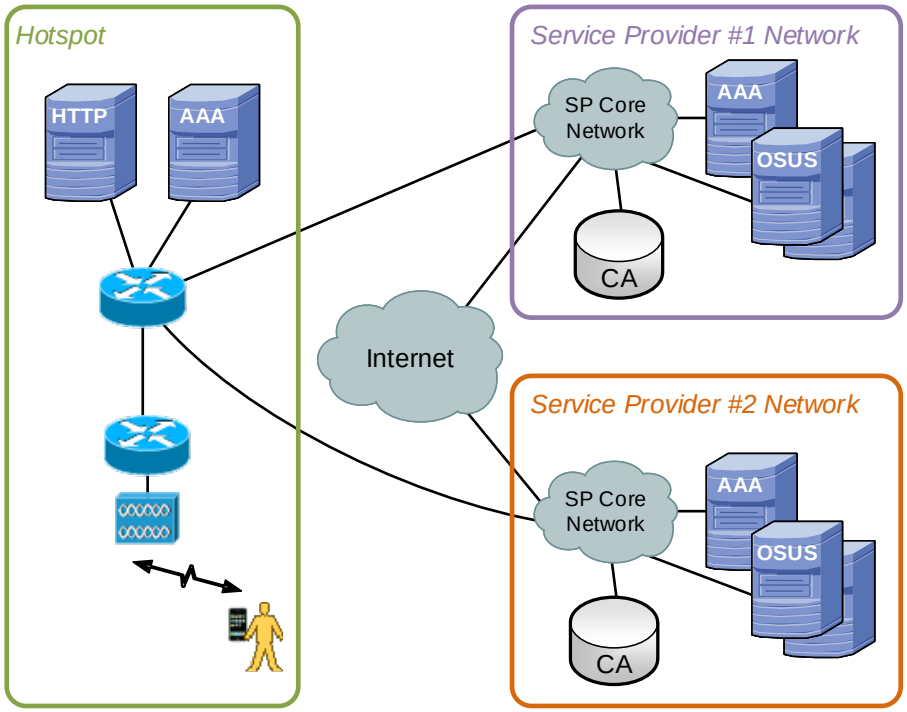

Figure 1: Example Network Architecture for Online Sign-Up

The OSU server is used to register new subscribers and provision the subscriber device with credentials. The SP's AAA server is used to authenticate subscribers using the credentials obtained from the OSU server.

The security architecture for Hotspot 2.0 online sign-up and initial authentication has the following goals:

1. Ensure that the user is communicating with the intended SP network and OSU server.
2. Protect the communication between the mobile device and the network OSU server from eavesdropping and modification.
3. Reduce the risk of a single SP having poor security practices from compromising other SPs.

The user's intent to connect to a selected SP is indicated by the user's selection of a Friendly Name and/or icon displayed on the mobile device's UI. During the OSU procedure, the mobile device verifies the name and icon selected by the user are exactly the same as the ones in the OSU server certificate (which have been certified by the CA/RA issuing that certificate).

2 References

The following are referenced within this document and form a normative part of this specification to the extent specified herein. In the event of a conflict with this specification and the following referenced specifications, the contents of this specification take precedence.

[1] RFC 1035, “Domain Names - Implementation and Specification”, Mockapetris, November 1987

[2] RFC-2560 “X.509 Internet Public Key Infrastructure Online Certificate Status Protocol – OCSP”, Myers, Ankney, Malpani, Galperin, Adams, June 1999

[3] RFC-2585, Internet X.509 Public Key Infrastructure Operational Protocols: FTP and HTTP, Housley, Hoffman, May 1999

[4] RFC-3447, Public-Key Cryptography Standards (PKCS) #1: RSA Cryptography Specifications Version 2.1, Jonsson and Kaliski, February 2003

[5] RFC-3629, UTF-8, A Transformation Format of ISO 10646, Yergeau, November 2003

[6] RFC-3647 “Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework”, Chokhani, Ford, Sabett, Merrill, Wu, November 2003

[7] RFC-3709, Internet X.509 Public Key Infrastructure: Logotypes in X.509 Certificates, Santesson, Housley, Freeman, February 2004

[8] RFC 3986, “Uniform Resource Identifier (URI): Generic Syntax”, Berners-Lee, Fielding and Masinter, January 2005

[9] RFC-4282, “The Network Access Identifier”, Aboba, Beadles, Arkko, and Eronen, December 2005

[10] RFC-4288, Media Type Specifications and Registration Procedures, Freed and Klensin, December 2005

[11] RFC-5280, “Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile”, Cooper, Santesson, Farrell, Boeyen, Housley, Polk, May 2008

[12] Wi-Fi Alliance Hotspot 2.0 (Release 2) Technical Specification, Version 1.1.0, http://www.wi-fi.org/passpoint

[13] ISO 639-2, also see ISO-639 guidance, for further guidance on how to encode language codes.

[14] X.501, http://www.itu.int/rec/T-REC-X.501/e

2.1 Definitions

The following definitions are applicable to this specification:

Certificate Authority: The certificate authority (CA) is 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 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.

Digital Certificate Subscriber Request: The CA vendor specific information certificate request information such as a click-through agreement.

Home SP: An 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.

Hotspot Operator: The entity that is responsible for the operation of the hotspot.

Registration Authority: The registration authority (RA) is 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 to verify certificate contents for the CA.

Registration Data: Registration Data is defined as 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).

Service Provider: An entity offering network services (from the perspective of the Hotspot Operator). SPs are represented in the NAI Realm List and 3GPP Cellular Network Information (in the form of a PLMN List) ANQP messages.

Subscriber: The entity applying for an OSU server certificate or Intermediate CA certificate.

2.2 Abbreviations and Acronyms

The following list describes acronyms and definitions for terms used throughout this document:

Abbreviation	Definition
AAA	Authentication, Authorization and Accounting
AIA	Authority Information Access
ANQP	Access Network Query Protocol
CA	Certificate Authority
CN	Common Name
CRL	Certificate Revocation List
CSR	Certificate Signing Request
DNS	Domain Name System
FQDN	Fully Qualified Domain Name
HTTP	HyperText Transfer Protocol
HTTPS	HyperText Transfer Protocol Secure
n/a	Not Applicable
NAI	Network Access Identifier
OCSP	Online Certificate Status Protocol
OID	Object Identifier
OSU	Online Sign-Up
OU	Organization Unit
PKI	Public Key Infrastructure
PLMN	Public Land Mobile Network
RA	Registration Authority
ROMARIN	Read Only Memory of Madrid Active Registry Information (Database)
SSID	Service Set IDentifier
SP	Service Provider
TLS	Transport Layer Security
UI	User Interface
URI	Uniform Resource Identifier
URL	Uniform Resource Location
WIPO	World Intellectual Property Organization (www.wipo.int)

3 Hotspot 2.0 OSU Certificates

3.1 Overview

Hotspot 2.0 uses three types of public key certificates for the authentication of OSU servers. Figure 2 shows the Hotspot 2.0 OSU certificate hierarchy and depicts the entities where these certificates are installed in a hotspot. These public key certificate types are:

- 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 X.509v3 public key certificates based on RSA key pairs.

Each OSU server has a certificate signed by a Certificate Authority whose root certificate is trusted by the connection manager of the mobile device. In columns 2 and 3 of Table 1, the Intermediate CA is working on behalf of the Trust Root CA; in column 4 of Table 1, the Intermediate CA is working on behalf of the SP.

Table 1: 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

The requirements for the trust hierarchy are specified below:

1. There will be at least two different Hotspot 2.0 Trust Root Certificates authorized by Wi-Fi Alliance.
2. The Hotspot 2.0 OSU server certificates shall be issued by an Intermediate CA with a certificate signed directly by an OSU Trust Root CA. The Intermediate CA and OSU Trust Root CA may be operated by the same company.
3. Trust Root CAs shall only issue Intermediate CA certificates to intermediate CA's that are under the Root CAs direct technical control.
4. Column 4 in Table 1 specifies issuing hierarchy if the Intermediate CA is operated by the same company as the company for whom the OSU server certificate is generated.
    - All the logotype(s) and subjectAltName(s) used in the OSU server certificate shall also be present in the Intermediate CA certificate.
5. Column 2 and 3 of Table 1 specifies issuing hierarchy if the Intermediate CA is operated by the Trust Root CA or a company to whom the Trust Root CA delegates its CA authority.
    - logotype(s) and subjectAltName(s) are not included in the Intermediate CA certificate.
6. The Trust Root CA shall notify Wi-Fi Alliance of the issuance of any Hotspot 2.0 Intermediate CA certificates.

7. The Intermediate CA may issue other end entity certificates defined by the Hotspot 2.0 specification (e.g. remediation, AAA, or policy servers). It shall not issue certificates for non-Hotspot 2.0 applications.
8. OSU server certificates shall only be used for authenticating the OSU server as defined by the Hotspot 2.0 specification.

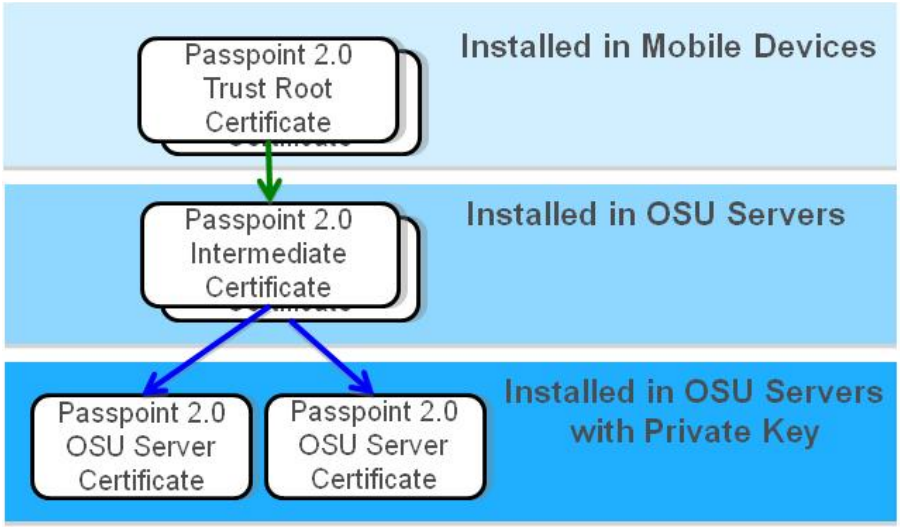

Figure 2: Hotspot 2.0 OSU Certificate Hierarchy

The following subsections define the contents of these certificates and any specific verification rules associated with them.

3.2 Hotspot 2.0 Trust Root Certificates

Table 2 describes the constraints on fields in an OSU Trust Root certificate.

Table 2: Hotspot 2.0 Trust Root Certificate Profile

Selected Certificate Fields	Profile Specific Constraints	M/O[1]	ASN.1 Type & OIDs
version	Shall be "v3" (Integer value 2)	M	Version
serialNumber	Unique positive integer value in an OctetString of ≤20 Octets. Shall be unique per certificate for a given issuer.	M	INTEGER
signature	Shall use only "sha256WithRSAEncryption" (OID 1.2.840.113549.1.1.11). The parameter subelement shall not be included (NULL for RSA)	M	AlgorithmIdentifier
issuer	The “issuer” field shall exactly match the “subject” field.	M	Name
validity	The validity period should be 30 years from the issuing date (about 2043). UTCTime values shall be used.	M	SEQUENCE {notBefore Time, notAfter Time}

Selected Certificate Fields	Profile Specific Constraints	M/O[1]	ASN.1 Type & OIDs
subject	The "subject" field shall only contain the following attributes: C=US O=WFA Hotspot 2.0 CN=Hotspot 2.0 Trust Root CA - <ID#>. Note: ID# identifies the CA hosting the root certificate. For example, for the NetworkFX Trust Root CA, the CN is set to “Hotspot 2.0 Trust Root CA - 01”. ID# = 01 for NetworkFX ID# = 02 Reserved ID# = 03 for DigiCert	M	Name .
subjectPublicKeyInfo	The "algorithm" subfield of "subjectPublicKeyInfo" shall be RSA (OID 1.2.840.113549.1.1.1)	M	SEQUENCE {algorithm AlgorithmIdentifier, subjectPublicKey BIT STRING }
issuerUniqueID	Shall NOT be used.	n/a	n/a
subjectUniqueID	Shall NOT be used.	n/a	n/a
Modulus Length	4096	M	
extensions	Required.	M	Extensions
keyUsage	Mandatory and Critical (Critical set to TRUE)). Shall set "keyCertSign" and "cRLSign". May set “digitalSignature” and “nonRepudiation” for OCSP signing and/or audit log signing.	M	OID 2.5.29.15 BIT STRING{ keyCertSign (5), cRLSign (6), }
subjectKeyIdentifier	Critical shall be set to False.	M	OID 2.5.29.14
basicConstraints	Critical (Critical set to TRUE). The "cA" subfield shall be TRUE. The "pathLenConstraint" subfield shall not be included.	M	OID 2.5.29.19
nameConstraints	Not used on root.	n/a	
CRLDistributionPoints		O	
signatureAlgorithm	Shall use only "sha256WithRSAEncryption" (OID 1.2.840.113549.1.1.11). The parameter subelement shall not be included (NULL for RSA).	M	AlgorithmIdentifier

Notes:

1. M – Mandatory, O – Optional

3.3 Hotspot 2.0 Intermediate Certificates

Table 3 describes the constraints on fields in an OSU Intermediate CA certificate.

Table 3: Hotspot 2.0 OSU Intermediate Certificate

Selected Certificate Fields	Profile Specific Constraints	M/O	ASN.1 Type & OIDs
version	Shall be "v3" (Integer value 2).	M	Version
serialNumber	Unique positive integer value in an OctetString of ≤20 Octets. Shall be unique per certificate for a given issuer.	M	INTEGER
signature	Shall use only "sha256WithRSAEncryption" (OID 1.2.840.113549.1.1.11). The parameter subelement shall not be included (NULL for RSA).	M	AlgorithmIdentifier
issuer	Determined by issuing CA.	M	Name
validity	The validity period should be 10 years from the issuing date. UTCTime values shall be used.	M	SEQUENCE {notBefore Time, notAfter Time }
subject	Any "Name" expressed as a valid Distinguished Name (DN as defined in x.500). Intermediate CA certificates shall use an DN that clearly and uniquely identifies the Intermediate CA. The following attributes shall be used as defined below: C=<country> O=<company> CN=<company> Hotspot 2.0 Intermediate CA	M	Name
subjectPublicKeyInfo	The "algorithm" subfield of "subjectPublicKeyInfo" shall be RSA (OID 1:2:840:113549:1:1:1).	M	SEQUENCE {algorithm AlgorithmIdentifier, subjectPublicKey BIT STRING }
issuerUniqueID	Shall NOT be used.	n/a	n/a
subjectUniqueID	Shall NOT be used.	n/a	n/a
Modulus Length	2048	M	
extensions	Required.	M	Extensions
keyUsage	Mandatory and Critical (Critical set to TRUE)). Shall set "keyCertSign" and "cRLSign". May set “digitalSignature” and “nonRepudiation” for OCSP signing and/or audit log signing.	M	OID 2.5.29.15 BIT STRING{ keyCertSign (5), cRLSign (6), }
subjectKeyIdentifier	Critical shall be set to False.	M	OID 2.5.29.14
authorityKeyIdentifier	Critical shall be set to False.	M	OID 2.5.29.35
basicConstraints	Critical (Critical set to TRUE). The "cA" subfield shall be TRUE. The "pathLenConstraint" shall be 0.	M	OID 2.5.29.19
nameConstraints	Shall not be critical. The field may include one or more "dNSName" values that provide the domain range of certificates issued. Note - the SP Friendly Name and the Icon hash are included in intermediate certs issued to service providers and serve the function of constraining the certificate usage.	O	
id-pe-authorityInfoAccess	The Authority Information Access (AIA) extension is mandatory and not critical. It shall contain a single AccessDescription with an OCSP accessMethod and responder accessLocation HTTP URI.	M	OID 1.3.6.1.5.5.7.1.1

Selected Certificate Fields	Profile Specific Constraints	M/O	ASN.1 Type & OIDs
CRLDistributionPoints		O	
logotype	The "logotype" with critical set to FALSE and contains the "HashAlgAndValue" for a logo that is associated with the service provider.	*O	mediaType IA5String logotypeHash HashAlgAndValue logotypeURI IA5String LogotypeImageInfo
subjectAltName	The "subjectAltName" is not critical and shall contain one or more Friendly Names that identify the service provider. It may also contain the directory name field.	*C	
signatureAlgorithm	Shall use only "sha256WithRSAEncryption" (OID 1.2.840.113549.1.1.11). The parameter subelement shall not be included (NULL for RSA).	M	AlgorithmIdentifier

* Conditional: logotype and Friendly Name subjectAltName extensions shall be included in intermediate CA certificates when they are issued to service providers (see column 4 in Table 1).

3.4 Hotspot 2.0 OSU Server Certificates

OSU server certificates are formatted according to X.509v3 and LogoType (RFC-3709, [6]). They shall contain an RSA public key and they should have the TLS Server Certificate attribute. The OSU server's public key should be at least 2048-bits and the OSU server certificate should be signed using sha256WithRSAEncryption using RSASSA-PKCS1-v1.5 signature method defined in [4]. This assures maximum interoperability. The certificate should allow both signature operations and encryption operations for key transport.

An OSU server certificate:

a. Shall contain the OSU server FQDN as a DNSName type in the subjectAltName field.
b. Shall contain a Friendly Name field and an Icon field.
c. The UTF-8 encoded Friendly Name shall be an otherName sequence to the subjectAltName and shall be encoded with an ASN.1 type of UTF8String. If multiple Friendly Name values are required (same operator, multiple human languages), then multiple otherName fields are present in the certificate. The type-id of the otherName shall be an id-wfa-hotspot-friendlyName:

   id-wfa OBJECT IDENTIFIER ::= { 1.3.6.1.4.1.40808 }

   id-wfa-hotspot OBJECT IDENTIFIER ::= { 1.3.6.1.4.1.40808.1.1 }

   id-wfa-hotspot-friendlyName OBJECT IDENTIFIER ::= { 1.3.6.1.4.1.40808.1.1.1 }

   The id-wfa-hotspot-friendlyName contains exactly 1 language code and Friendly Name for an Operator. In the case where a Friendly Name is to be included in more than one human language, there shall be as many id-wfa-hotspot-Name objects as there are human languages included. The payload of the id-wfa-hotspot-friendlyName is the concatenation of the Language Code and Friendly Name. The Language Code is a 3-octet ISO-14962-1997 encoded string field that defines the language used in the Operator Name field. The Language Code field value is a two or three character language code selected from ISO-639 [13]. A two character language code value has 0

("null" in ISO-14962-1997) appended to make it 3 octets in length. The Friendly Name is a variable length UTF-8 formatted field containing the operator's name. The maximum length of this field is 252 octets. UTF-8 format is defined in [8]. For example, for two human languages the following Friendly Names would be included as two separate otherName objects in the SubjectAltName: "engWi-Fi Alliance" and "fraWi-Fi Alliance".

d. The Icon field shall be a communityLogos type extension of LogotypeExtn [6] and include the imageInfo and language fields. This extension contains the hash of the logo that is displayed in the UI of a device. Multiple icons may be present, carried in the communityLogos extension. The operator shall provide a logotypeURI value where the logo can be obtained. The filename provided in the Icon Metadata subfield of the OSU Providers List shall match the filename portion of the URL. In the OSU server certificate, at least one LogotypeExtn having a language code of "zxx" shall be present. Note: mobile devices use the icon having the language code set to "zxx" as the default icon when an exact match of the mobile device's UI language to the icon's language is not available.

Note: RFC-3709 [6] states that LogotypeExtn shall be non-critical.

Table 4 describes the constraints on fields in an OSU server certificate.

Table 4: Hotspot 2.0 OSU Server Certificate

Selected Certificate Fields	Profile Specific Constraints	M/O	ASN.1 Type & OIDs
version	Shall be "v3" (Integer value 2).	M	Version
serialNumber	Unique positive integer value in an OctetString of ≤20 Octets. Shall be unique per certificate for a given issuer.	M	INTEGER
signature	Shall use only "sha256WithRSAEncryption" (OID 1.2.840.113549.1.1.11). The parameter subelement shall not be included (NULL for RSA).	M	AlgorithmIdentifier
issuer	Determined by issuing CA.	M	Name
validity	The validity period should be 2 years from the issuing date. UTCTime values shall be used.	M	SEQUENCE {notBefore Time, notAfter Time }
subject	The "subject" name shall set the "CN" to the FQDN of the server. The "OU" portion of the name shall be set to "Hotspot 2.0 Online Sign Up Server". If there are multiple FQDNs in the subjectAltName field the certificate requester should choose which one is put in the subject common name.	M	Name
subjectPublicKeyInfo	The "algorithm" subfield of "subjectPublicKeyInfo" shall be RSA (OID 1:2:840:113549:1:1:1).	M	SEQUENCE {algorithm AlgorithmIdentifier, subjectPublicKey BIT STRING }
issuerUniqueID	Shall NOT be used.	n/a	n/a
subjectUniqueID	Shall NOT be used.	n/a	n/a
extensions	Required.	M	Extensions
keyUsageExtension	Mandatory and Critical (Critical set to TRUE). Shall set "keyEncipherment".	M	
extKeyUsage	"extKeyUsage" is critical and shall set "KeyPurposeId" to "Server Authentication".	M	

Selected Certificate Fields	Profile Specific Constraints	M/O	ASN.1 Type & OIDs
logotype	The "logotype" with critical set to FALSE and contains the "HashAlgAndValue" for a logo that is associated with the service provider. Note – RFC 3709 specified inclusion of SHA-1 hash values are not required.	M	mediaType IA5String logotypeHash HashAlgAndValue logotypeURI IA5String LogotypeImageInfo
subjectAltName	The "subjectAltName" is critical and shall contain one or more Friendly Names that identify the service provider. The Friendly Names shall be in UTF-8 format and encoded with an ASN.1 type of UTF8String. The "subjectAltName" field shall include one or more "dNSName" values that provide the FQDN of the server.	M	
subjectKeyIdentifier	Critical shall be set to False.	M	OID 2.5.29.14
authorityKeyIdentifier	Critical shall be set to False.	M	OID 2.5.29.35
basicConstraints	Critical (Critical set to TRUE). The "cA" subfield shall be set to FALSE.	O	OID 2.5.29.19
id-pe-authorityInfoAccess	The Authority Information Access (AIA) extension is mandatory and not critical. It shall contain a single AccessDescription with an OCSP accessMethod and responder accessLocation HTTP URI.	M	OID 1.3.6.1.5.5.7.1.1
signatureAlgorithm	Shall use only "sha256WithRSAEncryption" (OID 1.2.840.113549.1.1.11). The parameter subelement shall not be included (NULL for RSA).	M	AlgorithmIdentifier

OSU servers are web servers that support the HTTP protocol running over TLS (i.e. HTTPS). Hotspot 2.0 OSU server certificates are used by OSU servers to facilitate the TLS connection. The OSU server certificate shall be signed by an Intermediate CA that can be validated using one of the OSU Root CAs.

4 OSU Server Certificate Issuing Process

When issuing a Hotspot 2.0 OSU server certificate, the issuing CA shall follow an approved procedure to validate fields that describe the identity of the OSU server. The validation must provide assurance that the names, DNS address and icons used to identify the server are owned and controlled by the requesting entity. The specific fields requiring validation include:

- subject
- subjectAltName
- logotype

4.1 Naming

4.1.1 Types of Names

For certificates issued under this policy the CA shall assign X.501 distinguished names. The subject field in certificates shall be populated with a non-empty X.500 distinguished name as specified in section 3.

The issuer field of certificates shall be populated with a non-empty X.500 Distinguished Name.

4.1.2 Need for Names to be Meaningful

Subscriber certificates shall contain meaningful names with commonly understood semantics, permitting the determination of the identity of the organization that is the Subject of the certificate.

The subject name in CA certificates shall match the issuer name in certificates issued by the CA, as required by [11].

4.1.3 Anonymity or Pseudonymity of Subscribers

CAs shall not issue anonymous or pseudonymous certificates.

4.1.4 Rules for Interpreting Various Name Forms

Rules for interpreting Distinguished Name forms are specified in X.501 [14].

4.1.5 Uniqueness of Names

Name uniqueness for certificates issued by CAs shall be enforced. Each CA shall enforce name uniqueness within the X.500 name space within its domain. Name uniqueness is not violated when multiple certificates are issued to the same Subscriber. Name uniqueness is enforced for the entire Subject Distinguished Name of the certificate rather than a particular attribute (e.g., the common name). The CA shall identify the method for checking uniqueness of Subject Distinguished Names within its domain.

4.1.6 Recognition, Authentication, and Role of Trademarks

CAs operating under this policy shall not issue a certificate knowing that it infringes the trademark of another. Certificate Applicants shall not use names in their Certificate Applications that infringe upon the Intellectual Property Rights of others. Neither the Wi-Fi Alliance, nor any CA shall be required to determine whether a Certificate Applicant has Intellectual Property Rights in the name appearing in a Certificate Application or to arbitrate, mediate, or otherwise resolve any dispute concerning the ownership of any intellectual property rights, including, without limitation, rights in a domain name, trade name, trademark, or service mark, and Wi-Fi Alliance, and any CA shall be entitled, without liability to any Certificate Applicant, to reject or suspend any Certificate Application because of such dispute.

If the Subscriber generates the certificate key pair, then the CA shall prove that the Subscriber possesses the private key by verifying the Subscriber's digital signature on the PKCS #10 Certificate Signing Request (CSR) with the public key in the CSR.

If key pair is generated by the CA on behalf of a Subscriber, proof of possession of the private key by the Subscriber is not required.

4.1.7 Authentication of Organization Identity

The CA's certificate issuance process shall authenticate the identity of the organization named in the Digital Certificate Subscriber Request by confirming that the organization:

- Exists in a business database (e.g., Dun and Bradstreet) or, alternatively, has organizational documentation issued by or filed with the applicable government (e.g., government issued business credentials) that confirms the existence of the organization, such as articles of incorporation, Certificate of Formation, Charter Documents, or a business license that allows it to conduct business at the address listed in the request. The information on record shall materially match the facts submitted in the request.
- Is not listed on any of the following U.S. Government denied lists:
    - US Department of Commerce's Bureau of Industry and Security Embargoed Countries List, and the US Department of Commerce' Bureau of Industry and Security Denied Entities List

Secondly, the CA's certificate issuance process shall validate the information in the Certificate Application including the Icon and Friendly Name to be inserted into the certificate, including:

- Authentication of the contacts listed in the customer profile
- Verifying the information listed in the certificate application for accuracy and validity for the given organization
- Conducting a trademark search of the logo and Friendly Name in the U.S. Patent and Trademark Office and equivalent international trademark office such as the WIPO ROMARIN.

4.1.8 Authentication of Individual Identity

The CA's certificate issuance process shall authenticate that the:

- Representative submitting the Digital Certificate Subscriber Request is a duly authorized representative of the organization as an employee, partner, member, agent, etc., and is authorized to act on behalf of the organization.
- Requestor listed in the Digital Certificate Subscriber Request and Certificate Application, is a duly authorized representative of the organization as an employee, partner, member, agent, etc. and is authorized to act on behalf of the organization.

4.1.9 Non-verified Subscriber Information

Non-verifiable information MAY be included in PKI certificates provided it does not infringe, dilute or confuse, such as:

- Organization Unit (OU)
- Any other information for which there are no verification rules referenced in this Certificate Policy

4.1.10 Validation of Authority

The CA's certificate issuance process shall confirm that the:

- Contacts listed on the Digital Certificate Subscriber Request are authorized to act on behalf of the Subject organization.

4.1.11 SubjectAltName and Logotype Extension Detail

When SubjectAltName and Logotype extensions are included in SP Intermediate CA certificates (Column 4 in Table 1), trust root CAs shall validate the fields using the same process as defined for OSU server certificates in this section (section 4). Intermediate CAs shall verify these fields in the OSU server certificate are a proper subset of the same fields in the Intermediate CA certificate.

More details regarding the OSU server certificate subjectAltName and logotype extensions can be found in the Hotspot 2.0 specification [12].

4.2 Certificate Revocation Lists

CA vendors shall support OCSP [2] for the distribution of revocation lists.