Amendment to WINNF-TS-0022 for 6 GHz AFC System Authentication

Working Document WINNF-TS-2013

Version V1.0.0
July 5, 2023

TERMS, CONDITIONS & NOTICES

This document has been prepared by the 6 GHz Security TG to assist The Software Defined Radio Forum Inc. (or its successors or assigns, hereafter "the Forum"). It may be amended or withdrawn at a later time and it is not binding on any member of the Forum or of the 6 GHz Security TG.

Contributors to this document that have submitted copyrighted materials (the Submission) to the Forum for use in this document retain copyright ownership of their original work, while at the same time granting the Forum a non-exclusive, irrevocable, worldwide, perpetual, royalty-free license under the Submitter's copyrights in the Submission to reproduce, distribute, publish, display, perform, and create derivative works of the Submission based on that original work for the purpose of developing this document under the Forum's own copyright.

Permission is granted to the Forum's participants to copy any portion of this document for legitimate purposes of the Forum. Copying for monetary gain or for other non-Forum related purposes is prohibited.

THIS DOCUMENT IS BEING OFFERED WITHOUT ANY WARRANTY WHATSOEVER, AND IN PARTICULAR, ANY WARRANTY OF NON-INFRINGEMENT IS EXPRESSLY DISCLAIMED. ANY USE OF THIS SPECIFICATION SHALL BE MADE ENTIRELY AT THE IMPLEMENTER'S OWN RISK, AND NEITHER THE FORUM, NOR ANY OF ITS MEMBERS OR SUBMITTERS, SHALL HAVE ANY LIABILITY WHATSOEVER TO ANY IMPLEMENTER OR THIRD PARTY FOR ANY DAMAGES OF ANY NATURE WHATSOEVER, DIRECTLY OR INDIRECTLY, ARISING FROM THE USE OF THIS DOCUMENT.

Recipients of this document are requested to submit, with their comments, notification of any relevant patent claims or other intellectual property rights of which they may be aware that might be infringed by any implementation of the specification set forth in this document, and to provide supporting documentation.

This document was developed following the Forum's policy on restricted or controlled information (Policy 009) to ensure that that the document can be shared openly with other member organizations around the world. Additional Information on this policy can be found here: http://www.wirelessinnovation.org/page/Policies_and_Procedures

Although this document contains no restricted or controlled information, the specific implementation of concepts contain herein may be controlled under the laws of the country of origin for that implementation. Readers are encouraged, therefore, to consult with a cognizant authority prior to any further development.

Wireless Innovation Forum ™ and SDR Forum ™ are trademarks of the Software Defined Radio Forum Inc.

Table of Contents

List of Figures

No table of figures entries found.

List of Tables

Amendment to WINNF-TS-0022 for 6GHz AFC System Authentication

1 Introduction

[WINNF-TS-0022] is the CBRS Certificate Policy Specification which enables WInnForum Roots of Trust to issue certificates for the following CBRS system entities:

- SAS (Spectrum Access System)
- Certified Professional Installer (CPI)
- CBSD (CBRS Device)
- Domain Proxy

This amendment extends WInnForum's Certificate Policy and enables issuance of certificates for these additional entities that participate in the 6 GHz Automated Frequency Coordination (AFC):

- AFC System
- SPD (Standard Power Device)
- Proxy

AFC System may also obtain certificates from CAs that are compliant with and audited against [CABF-BR], but such certificates are out of scope of this document. SPD may have alternative methods of being authenticated by the AFC System that do not require certificates which are also out of scope of this document.

For the most part, certificate policy defined in [WINNF-TS-0022] also applies to the issuance of AFC System, SPD and Proxy certificates. Any additional requirements not already covered in [WINNF-TS-0022] are addressed in this amendment. Sections in this document are numbered in such a manner that they directly correspond to sections with the same number in [WINNF-TS-0022]. If a section number exists in [WINNF-TS-0022] but not in this document, that means there are no changes to the corresponding certificate policy, and it applies exactly as is to the new certificates defined in this document.

1.1.4 Assurance level

Additional digital certificates defined in this document provide assurances that the certificate Subscriber's distinguished name is unique and unambiguous within the CA's domain, and the identity of the Subscriber's organization is based on a comparison of information submitted by the Subscriber against information in business records or databases. These certificates can be used for digital signatures, encryption, and authentication for proof of identity of components that contain

such certificates and are compliant with WInnForum 6 GHz AFC System specifications and this CP.

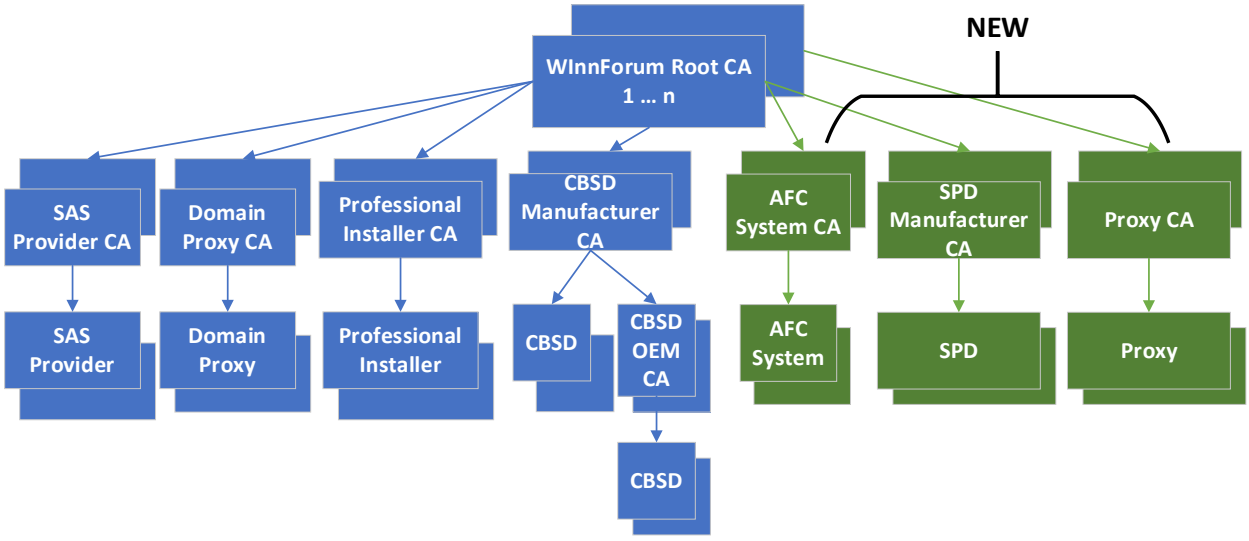
1.2 Document Name and Identification

The following additional WInnForum OID Arcs are utilized within certificates defined in this document:

Table 1 WInnForum OID Arcs

Digitally Signed Object	Object Identifier (OID)
AFC System	1.3.6.1.4.1.46609.1.1.7
SPD	1.3.6.1.4.1.46609.1.1.8
Proxy	1.3.6.1.4.1.46609.1.1.9
SPD device and equipment authorization information	1.3.6.1.4.1.46609.1.8

1.3 PKI Participants



PKI Participants that are defined in [WINNF-TS-0022] are included here in blue color and the new PKI participants are in green. AFC System certificates are issued by an AFC System CA, while SPD certificates are issued by SPD Manufacturer CA and both new CAs chain to a WInnForum Root CA.

WInnForum Root CA and CBRS Root CA (term utilized in [WINNF-TS-0022]) both refer to the same WInnForum Root of Trust. More than one WInnForum Root CA is permitted and currently multiple exist.

1.5 Policy Administration

1.5.5 Validation Procedures

This section enumerates the validation procedures a WInnForum Approved Certificate Authority (CA) must follow before signing certificate requests for AFC Systems, SPDs, and Proxies.

AFC System End Entity Certificate Issuance Guidelines

A CA shall sign an AFC System End Entity certificate request using an AFC System CA certificate if and only if:

1. It validates the AFC System End Entity certificate attributes defined in section 7.

2. It validates the entity presenting the AFC System certificate signing request:

    a) Region-specific full validation: CA validates that AFC system operator has been certified as an AFC System operator by the corresponding regulatory agency, and that certificate attributes reflect this verification method as well as the region of certification.

    b) Region-agnostic validation: CA verifies that the AFC system operator has filed an application with FCC or some other regional authority for certification. AFC system operator alternatively has already obtained certification from FCC or any other valid regional certification authority. Region of certification is not specified in this case, since certification is not guaranteed.

3. It validates that the domain endpoints enumerated in the attributes of the certificate are under the control of the AFC System.

4. It validates that the value of the OrganizationName attribute in the certificate request (i) is or (ii) has a legal link to the entity which entered into an agreement with the CA for the device on which behalf the certificate signing is requested, according to the criteria established by the WInnForum CBRS PKI Certificate Policy guidelines, and that the certificate attributes reflect this identity. OrganizationName attribute may differ slightly from the verified name, such as common variations or abbreviations, provided that the CA documents the difference and any abbreviations used are locally accepted abbreviations, e.g., if the official record shows “Company Name Incorporated”, the CA could use “Company Name Inc.” or “Company Name”.

    In case (ii), the CA shall verify the existence of the legal link by a record in a public database or obtaining a duly signed document stating the legal link from the entity submitting the certificate signing request.

5. It enters into a user agreement with the entity requesting the AFC System certificate to be signed according to the requirements in the WInnForum CBRS PKI Certificate Policy [WINNF-TS-0022] and this amendment.

SPD End Entity Certificate Issuance Guidelines

A CA shall sign an SPD End Entity certificate request using a SPD Manufacturer CA if and only if:

1. It validates the SPD End Entity certificate attributes defined in section 7 including all equipment authorization identifier(s) in the device identifier and in the SubjectAltName extension. If the granting regulatory authority for an equipment authorization is "FCC", the equipment authorization identifier shall be interpreted and validated as FCC ID. The format of the device identifier serial number may optionally be validated.

2. It validates that the entity submitting the SPD End Entity certificate signing request (i) is or (ii) has a legal link to the entity which has been granted the equipment authorizations enumerated in the certificate signing request for the device on whose behalf the certificate signing is requested, according to the criteria established by the WInnForum CBRS PKI Certificate Policy guidelines, and that the certificate attributes reflect this identity. OrganizationName attribute may differ slightly from the verified name, such as common variations or abbreviations, provided that the CA documents the difference and any abbreviations used are locally accepted abbreviations; e.g., if the official record shows "Company Name Incorporated", the CA could use "Company Name Inc." or "Company Name".

   In case (ii), the CA shall verify the existence of the legal link by a record in a public database or obtaining a duly signed document stating the legal link from the entity submitting the certificate signing request.

3. It enters into an agreement with the entity requesting the SPD End Entity certificate to be signed according to the requirements in the WInnForum CBRS PKI Certificate Policy [WINNF-TS-0022] and this amendment.

Proxy End Entity Certificate Issuance Guidelines

An Proxy in a 6 GHz network is a proxy for communications between SPDs and an AFC System.

A CA shall sign an Proxy End Entity certificate request using an SPD Manufacturer CA if and only if:

1. It validates the Proxy End Entity certificate attributes defined in section 7.

2. It validates that the entity submitting the Proxy End Entity certificate signing request (i) is or (ii) has a legal link to the entity which has been granted equipment authorization for at least one Proxy–SPD combination by the regulatory authority referenced in the requested

certificate, according to the criteria established by the WInnForum CBRS PKI Certificate Policy guidelines, and that the certificate attributes reflect this identity. OrganizationName attribute may differ slightly from the verified name, such as common variations or abbreviations, provided that the CA documents the difference and any abbreviations used are locally accepted abbreviations; e.g., if the official record shows "Company Name Incorporated", the CA could use "Company Name Inc." or "Company Name".

In case (ii), the CA shall verify the existence of the legal link by a record in a public database or obtaining a duly signed document stating the legal link from the entity submitting the certificate signing request.

3. It enters into an agreement with the entity requesting the Proxy End Entity certificate to be signed according to the requirements in the WInnForum CBRS PKI Certificate Policy [WINNF-TS-0022] and this amendment.

7 Certificate, CRL, and OCSP Profiles

In the rest of this section, placeholder variables are used. The following are selected placeholders used in the definition of several multi-part identifiers.

Placeholder	Definition
<nra>	An identifier for a regulatory agency. Values defined include: • "FCC" (without quotes), for the FCC of the United States Additional values may be defined in the future.
<equipment authorization ID>	An identifier for an authorization granted by a regulatory agency.
<responsible party ID>	An identifier used by a regulatory authority to identify a party responsible for regulatory compliance.

Where the value of <nra> in a multi-part identifier is "FCC", the following interpretations apply:

Placeholder	Interpretation
<equipment authorization ID>	FCC ID
<responsible party ID>	FRN

7.1 Certificate Profile

In addition to the certificate profiles in [WINNF-TS-0022], this section defines new certificate profiles for additional certificate types (AFC System, SPD and corresponding Sub-CAs).

Table 2: RSA Sub-CA Certificate Profile

Version	v3
Serial number	Unique Positive Integer in the context of the issuing Root CA and not longer than 20 octets.

Issuer DN		c=US o=WInnForum ou=RSA Root CA<ID#> cn=WInnForum RSA Root CA		
Subject DN		c=<Country Code> o=<Organization Name> ou=RSA <Sub-CA Type> <ID#> *or* RSA <Sub-CA Type> <ID#> cn=WInnForum RSA <Sub-CA Type>*or* WInnForum RSA <Sub-CA Type>		
Validity Period		30 yrs		
Signature		Sha384WithRSAEncryption (1.2.840.113549.1.1.12) *or*, Sha512WithRSAEncryption (1.2.840.113549.1.1.13)		
Subject Public Key Info algorithm keysize parameters		 RSA (1.2.840.113549.1.1.1) 4096-bits NULL		
Extensions	OID	Include	Criticality	Value
keyUsage	{id-ce 15}	Mandatory	TRUE	
keyCertSign				Set (1)
cRLSign				Set (1)
digitalSignature		Optional		Set (1)
basicConstraints	{id-ce 19}	Mandatory	TRUE	
cA				Set (TRUE)
pathLenConstraint				0 (zero)
subjectKeyIdentifier	{id-ce 14}	Mandatory	FALSE	
keyIdentifier				<Calculated per Method 1>
authorityKeyIdentifier	{id-ce 35}	Mandatory	FALSE	
keyIdentifier				Calculated per Method 1>
subjectAltName	{id-ce 17}	Optional	FALSE	
certificatePolicies	{id-ce 32}	Mandatory	FALSE	
certPolicyId				1.3.6.1.4.1.46609.2.1
policyQualifiers				Not Present
certPolicyId				See Table 1
policyQualifiers				Not Present
cRLDistributionPoints	{id-ce 31}	Mandatory	FALSE	
distributionPoint				<URI of relevant CRLs>
authorityInfoAccess	{id-pe 1}	Optional	FALSE	
ocsp	{id-ad 1}			<URI of the OCSP responder>, *or* Not Present
caIssuers	{id-ad 2 }			<URI of the Issuer's Certificate location>, *or* Not Present

<Sub-CA Type> is one of the following values (without quotes): “SPD Mfr CA”, “AFC System CA”, “Proxy CA”.

<ID#> indicates the ID number of the CA and is populated when the CA certificate is issued. For Example, “CA0001.”

Table 3: RSA Subscriber Certificate Profile

Version		v3		
Serial number		Unique Positive Integer in the context of the issuing CA and not longer than 20 octets.		
Issuer DN		c=<Country Code> o=<Organization Name> ou=RSA <Sub-CA Type> <ID#> *or* RSA <Sub-CA Type> <ID#> cn=WInnForum RSA <Sub-CA Type> *or* WInnForum RSA <Sub-CA Type>		
Subject DN		c=<Country Code> o=<Organization Name> ou=WInnForum <Device Type> Certificate cn=<Device Identifier>		
Validity Period		5 Years for AFC System and for Proxy 10 years for SPD		
Signature		Sha256WithRSAEncryption (1.2.840.113549.1.1.11) or, Sha384WithRSAEncryption (1.2.840.113549.1.1.12) *or*, Sha512WithRSAEncryption (1.2.840.113549.1.1.13)		
Subject Public Key Info algorithm keysize parameters		 RSA (1.2.840.113549.1.1.1) 2048-bits NULL		
Extensions	OID	Include	Criticality	Value
keyUsage	{id-ce 15}	Mandatory	TRUE	
digitalSignature				Set
keyEncipherment				Set
subjectKeyIdentifier	{id-ce 14}	Mandatory	FALSE	
keyIdentifier				<Calculated per Method 1>
authorityKeyIdentifier	{id-ce 35}	Mandatory	FALSE	
keyIdentifier				<Calculated per Method 1>
subjectAltName	{id-ce 17}	Optional*	FALSE	For SPD device certificates, this is mandatory.
dNSName				<AFC System FQDN> in AFC System certificates or not present

otherName		Optional*		For SPD device certificates, this is mandatory. See notes following this table for this otherName.
certificatePolicies	{id-ce 32}	Mandatory	FALSE	
certPolicyId				1.3.6.1.4.1.46609.2.1
policyQualifiers				Not Present
certPolicyId				See Table 1
policyQualifiers				Not Present
cRLDistributionPoints	{id-ce 31}	Mandatory	FALSE	
distributionPoint				<URI of relevant CRLs>
authorityInfoAccess	{id-pe 1}	Optional	FALSE	
ocsp	{id-ad 1}			<URI of the OCSP responder>, *or* Not Present
caIssuers	{id-ad 2}			<URI of the Issuer's Certificate location>, *or* Not Present

<Sub-CA Type> is one of the following values (without quotes): "SPD Mfr CA", "AFC System CA", "Proxy CA".

<ID#> indicates the ID number of the CA and is populated when the CA certificate is issued. For Example, "CA0001."

<Device Type> is one of the following values (without quotes): "SPD", "AFC System", "Proxy".

<Device Identifier> is one of the following values:

- For SPD device certificates – <nra>:<equipment authorization id>:<device serial number>, e.g. FCC**:**0014720239:234A65760123
- For AFC System certificates – <prefix>:<FQDN>, where:
    - <prefix> is one of the following:
        - <nra> – identifier for a regulatory authority from which the AFC System has authorization to operate.
        - "Relaxed" – a special value indicating that CA performed region-agnostic validation as described in section 1.5.
    - <FQDN> is the fully qualified domain name of an AFC System server

- For Proxy certificates when the Proxy is for FCC-certified SPDs[1]:

  <nra>:<responsible party ID>:<unique identifier assigned by responsible party>

  Note: <responsible party ID> identifies the manufacturer of the SPD; <unique identifier assigned by responsible party> identifies an individual Proxy, not a model/type of Proxy

<AFC System FQDN> is the fully qualified domain name (FQDN) of the AFC System

SPD device certificates must also include, in a SubjectAltName extension, an otherName as specified below[2]:

Component	Type	Value
type-id	Object ID	1.3.6.1.4.1.46609.1.8
value	UTF8String	<device serial number>,<nra>:<equipment authorization id> [,<nra>:<equipment authorization id>] The <nra>:<equipment authorization id> in the CommonName (cn) attribute of the Subject DN shall also be included here. The list of <nra>:<equipment authorization id> pairs here is not required to be exhaustive. An SPD product may have more authorizations from regulatory authorities than enumerated in the device certificate of an individual device.[3] Authorizations not enumerated in an SPD device certificate may affect the ability of the device to interoperate with AFC Systems in some countries or regions.

Table 4: ECC Sub-CA Certificate Profile

Version	v3
Serial number	Unique Positive Integer in the context of the issuing Root CA and not longer than 20 octets.
Issuer DN	c=US o=WinnForum ou=ECC Root CA<ID#> cn=WinnForum ECC Root CA

[1] Device Identifier format of Proxy certificates within other regions of certification is subject for further study.
[2] The value of a subject DN's common name (cn) attribute is limited to 64 characters. The custom otherName defined here allows more equipment authorization information to be included.
[3] A product may gain authorizations from additional regulatory authorities over time. By not requiring the equipment authorization information in a certificate to be exhaustive, already-deployed SPD devices need not have their certificates updated every time the product model gains additional authorizations.

Subject DN		c=<Country Code> o=<Organization Name> ou=ECC <Sub-CA Type> <ID#> *or* ECC <Sub-CA Type> <ID#> cn=WinnForum ECC <Sub-CA Type> *or* WinnForum ECC <Sub-CA Type>		
Validity Period		30 yrs		
Signature		ecdsa-with-Sha384 (1.2.840.10045.4.3.3) or, ecdsa-with-Sha512 (1.2.840.10045.4.3.4)		
Subject Public Key Info algorithm parameters		 EC (1.2.840.10045.2.1) Secp384r1 (1.3.132.0.34) *or* Secp521r1 (1.3.132.0.35)		
Extensions	OID	Include	Criticality	Value
keyUsage	{id-ce 15}	Mandatory	TRUE	
keyCertSign				Set (1)
cRLSign				Set (1)
digitalSignature		Optional		Set (1), *or* Not Set (0)
basicConstraints	{id-ce 19}	Mandatory	TRUE	
cA				Set (TRUE)
pathLenConstraint				0 (zero)
subjectKeyIdentifier	{id-ce 14}	Mandatory	FALSE	
keyIdentifier				<Calculated per Method 1>
authorityKeyIdentifier	{id-ce 35}	Mandatory	FALSE	
keyIdentifier				<Calculated per Method 1>
subjectAltName	{id-ce 17}	Optional	FALSE	
certificatePolicies	{id-ce 32}	Mandatory	FALSE	
certPolicyId				1.3.6.1.4.1.46609.2.1
policyQualifiers				Not Present
certPolicyId				See Table 1
policyQualifiers				Not Present
cRLDistributionPoints	{id-ce 31}	Mandatory	FALSE	
distributionPoint				<URL of relevant CRLs>
authorityInfoAccess	{id-pe 1}	Optional	FALSE	
ocsp	{id-ad 1}			<URI of the OCSP responder>, *or* Not Present
caIssuers	{id-ad 2 }			<URI of the Issuer's certificate location>, *or* Not Present

<Sub-CA Type> is one of the following values (without quotes): "SPD Mfr CA", "AFC System CA", "Proxy CA".

<ID#> indicates the ID number of the CA and is populated when the CA certificate is issued. For Example, "CA0001."

Table 5: ECC Subscriber Certificate Profile

Version		v3		
Serial number		Unique Positive Integer in the context of the issuing CA and not longer than 20 octets.		
Issuer DN		c=<Country Code> o=<Organization Name> ou=ECC <Sub-CA Type> <ID#> *or* ECC <Sub-CA Type> <ID#> cn=WInnForum ECC <Sub-CA Type> *or* WInnForum ECC <Sub-CA Type>		
Subject DN		c=<Country Code> o=<Organization Name> ou=WInnForum <Device Type> Certificate cn=<Device Identifier>		
Validity Period		5 Years for AFC System and Proxy 10 years for SPD		
Signature		ecdsa-with-Sha256 (1.2.840.10045.4.3.2) or, ecdsa-with-Sha384 (1.2.840.10045.4.3.3) or, ecdsa-with-Sha512 (1.2.840.10045.4.3.4)		
Subject Public Key Info algorithm parameters		EC (1.2.840.10045.2.1) Secp256r1 (1.2.840.10045.3.1.7) or Secp384r1 (1.3.132.0.34) *or* Secp521r1 (1.3.132.0.35)		
Extensions	OID	Include	Criticality	Value
keyUsage	{id-ce 15}	Mandatory	TRUE	
digitalSignature				Set (1)
keyAgreement				Set (1)
subjectKeyIdentifier	{id-ce 14}	Mandatory	FALSE	
keyIdentifier				<Calculated per Method 1>
authorityKeyIdentifier	{id-ce 35}	Mandatory	FALSE	
keyIdentifier				<Calculated per Method 1>
subjectAltName	{id-ce 17}	Optional*	FALSE	For SPD device certificates, this is mandatory.
dNSName				<AFC System FQDN> in AFC System certificates or not present
otherName		Optional*		For SPD device certificates, this is mandatory. See notes following this table for this otherName.
certificatePolicies	{id-ce 32}	Mandatory	FALSE	
certPolicyId				1.3.6.1.4.1.46609.2.1

policyQualifiers				Not Present
certPolicyId				See Table 1
policyQualifiers				Not Present
cRLDistributionPoints		Mandatory	FALSE	
distributionPoint				<URI of relevant CRLs>
authorityInfoAccess	{id-pe 1}	Optional	FALSE	
Ocsp	{id-ad 1}			<URI of the OCSP responder>, *or* Not Present
caIssuers	{id-ad 2}			<URI of the Issuer's certificate location>, *or* Not Present

<Sub-CA Type> is one of the following values (without quotes): "SPD Mfr CA", "AFC System CA", "Proxy CA".

<ID#> indicates the ID number of the CA and is populated when the CA certificate is issued. For Example, "CA0001."

<Device Type> is one of the following values (without quotes): "SPD", "AFC System", "Proxy".

<Device Identifier> is one of the following values:

- For SPD device certificates – <nra>:<equipment authorization id>:<device serial number>, e.g. FCC**:**0014720239:234A65760123
- For AFC System certificates – <prefix>:<FQDN>, where:
    - <prefix> is one of the following:
        - <nra> – identifier for a regulatory authority from which the AFC System has authorization to operate.
        - "Relaxed" – a special value indicating that CA performed region-agnostic validation as described in section 1.5.
    - <FQDN> is the fully qualified domain name of an AFC System server
- For Proxy certificates when the Proxy is for FCC-certified SPDs[4]:

  <nra>:<responsible party ID>:<unique identifier assigned by responsible party>

  Note: <responsible party ID> identifies the manufacturer of the SPD; <unique identifier assigned by responsible party> identifies an individual Proxy, not a model/type of Proxy

[4] Device Identifier format of Proxy certificates within other regions of certification is subject for further study.

<AFC System FQDN> is the fully qualified domain name (FQDN) of the AFC System

SPD device certificates must also include, in a SubjectAltName extension, an otherName as specified below[5]:

Component	Type	Value
type-id	Object ID	1.3.6.1.4.1.46609.1.8
value	UTF8String	<device serial number>,<nra>:<equipment authorization id> [,<nra>:<equipment authorization id>] The <nra>:<equipment authorization id> in the CommonName (cn) attribute of the Subject DN shall also be included here. The list of <nra>:<equipment authorization id> pairs here is not required to be exhaustive. An SPD product may have more authorizations from regulatory authorities than enumerated in the device certificate of an individual device.[6] Authorizations not enumerated in an SPD device certificate may affect the ability of the device to interoperate with AFC Systems in some countries or regions.

10 References

RFC 2119	Key Words for use in RFCs to Indicate Requirement Level, IETF (Bradner), March 1997. http://www.ietf.org/rfc/rfc2119.txt
RFC 2560	X.509 Internet Public Key Infrastructure Online Certificate Status Protocol – OCSP, IETF (Myers, Ankney, Malpani, Galperin, Adams), June 1999. http://www.ietf.org/rfc/rfc2560.txt
RFC 3647	Internet X.509 PKI Certificate Policy and Certification Practices Framework, IETF (Chokhani, Ford, Sabett, Merrill, and Wu), November 2003. http://www.ietf.org/rfc/rfc3647.txt
RFC 5019	The Lightweight Online Certificate Status Protocol (OCSP) Profile for High-Volume Environments, IETF (Deacon, Hurst), September 2007. http://www.ietf.org/rfc/rfc5019.txt
RFC 5280	Internet X.509 PKI Certificate and Certification Revocation List (CRL) Profile, IETF (Cooper, Santesson, Farrell, Boeyen, Housley, and Polk), May 2008. http://www.ietf.org/rfc/rfc5280.txt
RFC 6960	X.509 Internet Public Key Infrastructure Online Certificate Status Protocol – OCSP, IETF (Santesson, Myers, Ankney, Malpani, Galperin, Adams), June 2013. https://tools.ietf.org/rfc/rfc6960.txt
FIPS 140-2	Security Requirements for Cryptographic Modules, FIPS 140-2, May 25, 2001. http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf

[5] The value of a subject DN's common name (cn) attribute is limited to 64 characters. The custom otherName defined here allows more equipment authorization information to be included.

[6] A product may gain authorizations from additional regulatory authorities over time. By not requiring the equipment authorization information in a certificate to be exhaustive, already-deployed SPD devices need not have their certificates updated every time the product model gains additional authorizations.

WINNF-TS-0022	WInnForum CBRS Certificate Policy Specification, Version V1.5.0, 17 November 2020.
CABF-BR	Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates, CA/Browser Forum, https://cabforum.org/baseline-requirements-documents/.
WIFI-AFC	AFC System to AFC Device Interface Specification, Version 1.3, Wi-Fi Alliance.