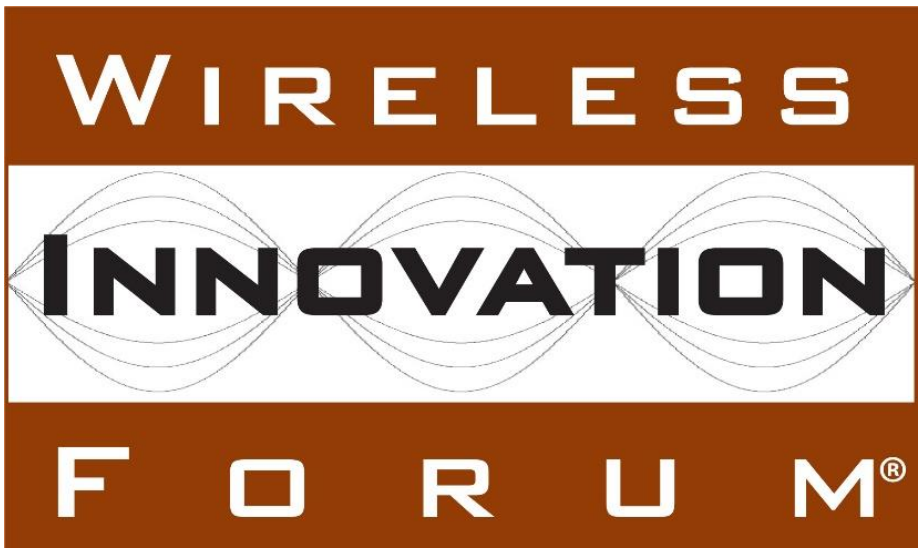

6 GHz Communication Security Technical Report

Document WINNF-TR-2012

Version V1.0.0

29 June 2023

TERMS, CONDITIONS & NOTICES

This document has been prepared by the 6 GHz Committee Functional Specification WG 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 It may be amended or withdrawn at a later time and it is not binding on any member of the Forum or of the 6 GHz Committee Functional Specification WG.

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

Contributors

The following individuals made significant contributions to this document:

Task Group Chair: Richard Bernhardt (WISPA)

Editor: Sho Furuichi (Sony)

Other Member Representatives:

- CommScope: Alexander Medvinsky, Nicol So, Peter Young
- Federated Wireless: Masoud Olfat
- Google: Kate Harrison
- Nokia: Navin Hathiramani (Nokia)

6 GHz Communication Security Technical Report

1 Introduction and Scope

According to 47 CFR 15.407(k)(8)(v) [n.1], Standard Power Devices (SPDs) must incorporate adequate security measures to prevent it from accessing AFC Systems not approved by the FCC. Additionally, the AFC System may establish communications authentication procedures between the AFC System and SPDs. Version V1.2.1 and the beyond of WINNF-TS-1014 [n.2] provides the following requirements to meet 47 CFR 15.407(k)(8)(v):

> *R2-DSQ-05: Standard Power Device shall address R1-DSQ-01-a by verifying the AFC System's Server Certificate.*
>
> *R2-ASQ-05: The AFC System shall identify itself via a Server Certificate issued by a Trusted CA.*
>
> *a. Server Certificates shall be OV (Organization Validated) certificates that include vetted company information.*
> *b. Server Certificates with only domain name shall not be accepted.*

However, the process for implementing these requirements needs more clarification and explanations.

The scope of this technical report is to provide a guideline for implementation of these requirements by AFC Systems and SPDs. The guideline includes the processes for SPDs to authenticate the AFC System, and for the AFC System to authenticate SPDs, separately.

2 References

2.1 Normative References

The following referenced documents are necessary for the application of the present document.

[n.1] Title 47, Code of Federal Regulations, Part 15 Subpart E - Unlicensed National Information Infrastructure Devices, available at: https://ecfr.federalregister.gov/current/title-47/chapter-I/subchapter-A/part-15/subpart-E

[n.2] WINNF-TS-1014, "Functional Requirements for the U.S. 6 GHz Band under the Control of an AFC System", Wireless Innovation Forum

2.2 Informative References

The following referenced documents are not necessary for the application of the present document, but they assist the reader with regard to a particular subject area.

[i.1] RFC 6750, "The OAuth 2.0 Authorization Framework: Bearer Token Usage", October 2012

[i.2] RFC 6749, "The OAuth 2.0 Authorization Framework", October 2012

[i.3] WINNF-TS-0022, "CBRS Certificate Policy Specification", Wireless Innovation Forum

[i.4] WINNF-TS-0065, "CBRS Communication Security Technical Specification", Wireless Innovation Forum

[i.5] WINNF-16-P-0235, "CBRS PKI Root of Trust Operator Requirements", Wireless Innovation Forum

[i.6] WInnForum Approved CBRS Root CA Operators, available at: https://cbrs.wirelessinnovation.org/cbrs-root-ca-operators

[i.7] RFC-3647, "Internet X.509 PKI Certificate Policy and Certification Practices Framework"

[i.8] WINNF-TS-2013, "Amendment to WINNF-TS-0022 for 6 GHz AFC System Authentication", Wireless Innovation Forum

3 Definitions, Abbreviations and Symbols

3.1 Definitions

For the purposes of the present document, the definitions given in [n.2] and the following apply.

Not available for this version of this technical report.

3.2 Abbreviations

For the purposes of the present document, the abbreviations given in [n.2] and the following apply.

CBRS	Citizens Broadband Radio Service
HTTPS	HTTP over TLS
PKI	Public Key Infrastructure

4 AFC System Authentication

4.1 Server Certificate

A digital certificate attests to the ownership of a public key by the subject of the certificate. In the case of an AFC System, the digital certificate is a TLS Server Certificate. To validate a Server Certificate, the ownership of the certificate signing key (i.e., the identity of the certificate authority) needs to be ascertained. In common practice, the ownership of a certificate signing key be a Certificate Authority (CA) is attested to using a CA certificate issued by a root CA, whose public key (often published in the form of a self-signed root CA certificate) is directly trusted. Reliable knowledge of the certificates of trusted root CAs is therefore the basis for trust in Server Certificates. It is critical that the set of root CA certificates an SPD treats as trusted is correct.

"Trusted CA" is defined in WINNF-TS-1014 [n.2] as a CA which has proven to be secure by an external WebTrust audits or equivalent. An example policy against which such audits could be conducted is WINNF-TS-0022 [i.3]. In order to designate "Trusted CA" or "Trusted Root CA", Trusted Root CA Operator Program for AFC System's Server Certificate can be created in a way similar to what is done for Citizens Broadband Radio Service (CBRS) [i.6]. See section 4.2 of this technical report for more details of Trusted Root CA Operator Program.

If the set of Trusted Root CAs is closed, the certificates of Trusted Root CAs can be programmed into SPDs during device manufacture. On the other hand, if the set of Trusted Root CAs is open-ended and could change over time, the certificates of Trusted Root will need to be securely provisioned to SPDs during deployment. For interoperability, there needs to be agreement between AFC System Operators and deployers of SPDs as to what CAs are trusted to issue Server Certificates for AFC Systems. Without a common, agreed-upon set of CAs trusted to issue Server Certificates to AFC Systems, it is possible that an AFC System's Server Certificate is not trusted by some SPDs. If the certificate policy and certification practices of the root and subordinate CAs conform to agreed-upon standards, it is possible to infer that the owner of a Server Certificate is authorized to operate an AFC System based on the identity of the issuing CA. The need for a separate channel for conveying authorization information can be avoided.

The main security requirement for root CA certificates stored in SPDs is integrity protection. Root CA certificates need to be provisioned through a secure process and be protected from unauthorized modification. Any updates need to be verified to be from a trusted source and checked for unauthorized modification.

It is not sufficient for an SPD to be able to authenticate an AFC System using a Server Certificate. The SPD will also need to determine whether the subject of a Server Certificate is authorized to operate an AFC System. If this authorization cannot be inferred from the Server Certificate itself (e.g., the issuing CA is known to issue certificate only to parties authorized to operate AFC Systems), a separate mechanism is needed to provision SPDs with identities of authorized AFC Systems.

4.2 Trusted Root CA Operator Program

SPDs are required by CFR 15.407(k)(8)(v) to incorporate adequate security measures to prevent it from accessing AFC Systems not approved by the FCC. As per WINNF-TS-1014, the AFC System is required to identify itself via a Server Certificate issued by a Trusted CA.

WINNF-TS-0022 "CBRS Certificate Policy" [i.3] is designed to be consistent with RFC-3647 "Internet X.509 PKI Certificate Policy and Certification Practices Framework", governs the certificate PKI operations of components by all individuals and entities within the CBRS PKI (collectively, "PKI Participants"), and provides the minimum requirements that PKI Participants are required to meet when issuing and managing CAs, digital certificates, and private keys related to the CBRS. CBRS PKI Root of Trust operator requirements are specified in WINNF-16-P-0235 [i.5].

Figure 4.2-1 shows the CBRS PKI structure adopted in WINNF-TS-0022 [i.3] and WINNF-TS-0065 [i.4].

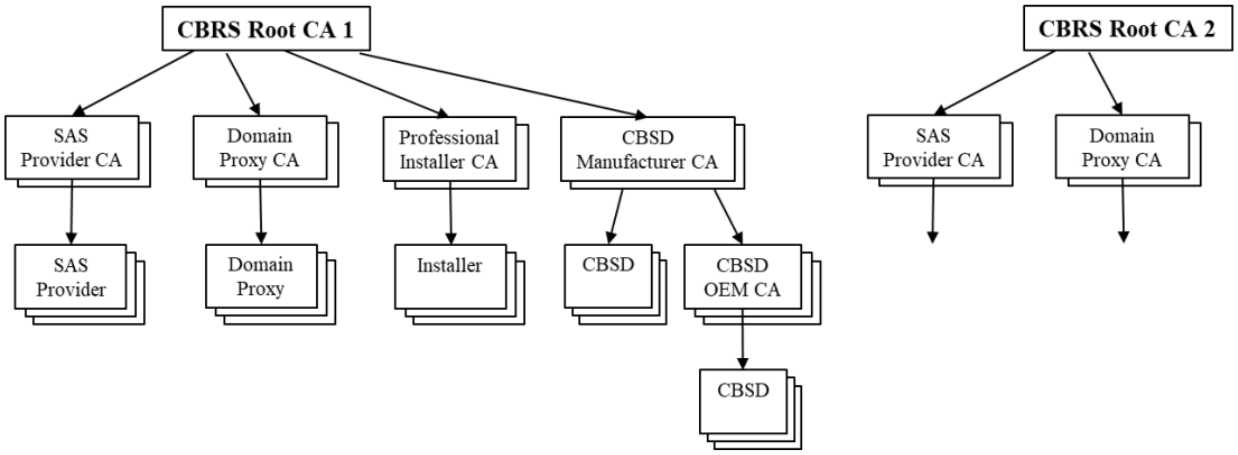

Figure 4.2-1: CBRS PKI Structure ([i.3], [i.4])

In this structure, the operation of CBRS Root CAs must be performed by entities as designated by the WInnForum [i.6], and SAS certificate must be issued by the CBRS Root CA in accordance with the WINNF-TS-0022. In other words, SASs not approved by the FCC cannot use SAS certificate and the FCC-certified CBSDs cannot be used to access to such SASs.

Likewise, the 6 GHz ecosystem will be able to meet the requirements in 47 CFR 15.407(k)(8)(v) by defining a 6 GHz PKI structure (Figure 4.2-2) and relevant requirements for AFC Systems, Standard Power Devices and Proxies. See WINNF-TS-2013 [i.8].

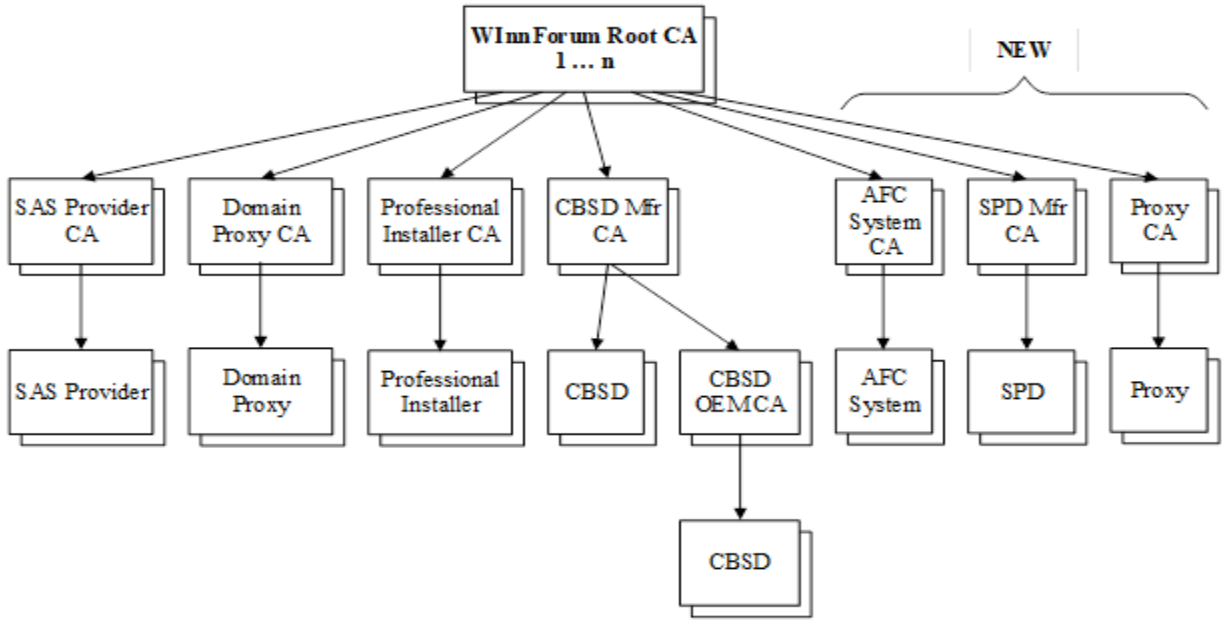

Figure 4.2-2: 6 GHz PKI structure [i.8]

5 Methods for Standard Power Device Authentication

5.1 General

This section introduces methods available to AFC Systems for device authentication. In this version of this technical report, the following methods are introduced.

- Use of client certificates (section 5.2)
- Use of Bearer Tokens (section 5.3)

5.2 Use of Client Certificates

Digital certificates can also be used to authenticate clients to AFC Systems. SPDs are a typical kind of clients in this context, but the same principles apply to Proxies. In setting up a mutually-authenticated TLS session between a client and a server, a client certificate is used to authenticate the client to the server.

Since SPDs have unique identities, each client device must have a unique key pair and a client certificate. The public key in the key pair is included in the client certificate, while the private key is a sensitive secret that must be protected from disclosure (e.g., extraction from the device).

During the setup of a mutually-authenticated TLS session, a “handshake” takes place between the client and the server. The client and server present their certificates to each other, and use their respectively private keys to establish a shared session secret. In the process, each party authenticates the certificate presented by the other. To enable such authentication, each party is equipped with the root CA certificate of the issuer of the other party’s certificate.

Successful handshake during TLS session setup provides assurance to the server that it has set up a secure communication channel with the entity whose identified in the client certificate. A client certificate can also securely convey other information to the server, such as equipment authorization identifiers associated with an SPD.

A CA that issues client certificates must be trustworthy to fulfill the role. It must adhere to good practices as a CA and must agree to issue certificates only according to approved policies. See section 4.2 for more details on how a Trusted Root CA operator program can be used to regulate the issuance of certificates in the ecosystem generally, and more particularly device certificates in this context.

Figure 5.2-1 provides the call flow in the case where an AFC System and an SPD successfully authenticate each other using TLS certificates. To enable the AFC System to verify the FCC ID and serial number of the SPD, the two parameters need to be part of the subject information in the SPD’s client certificate.

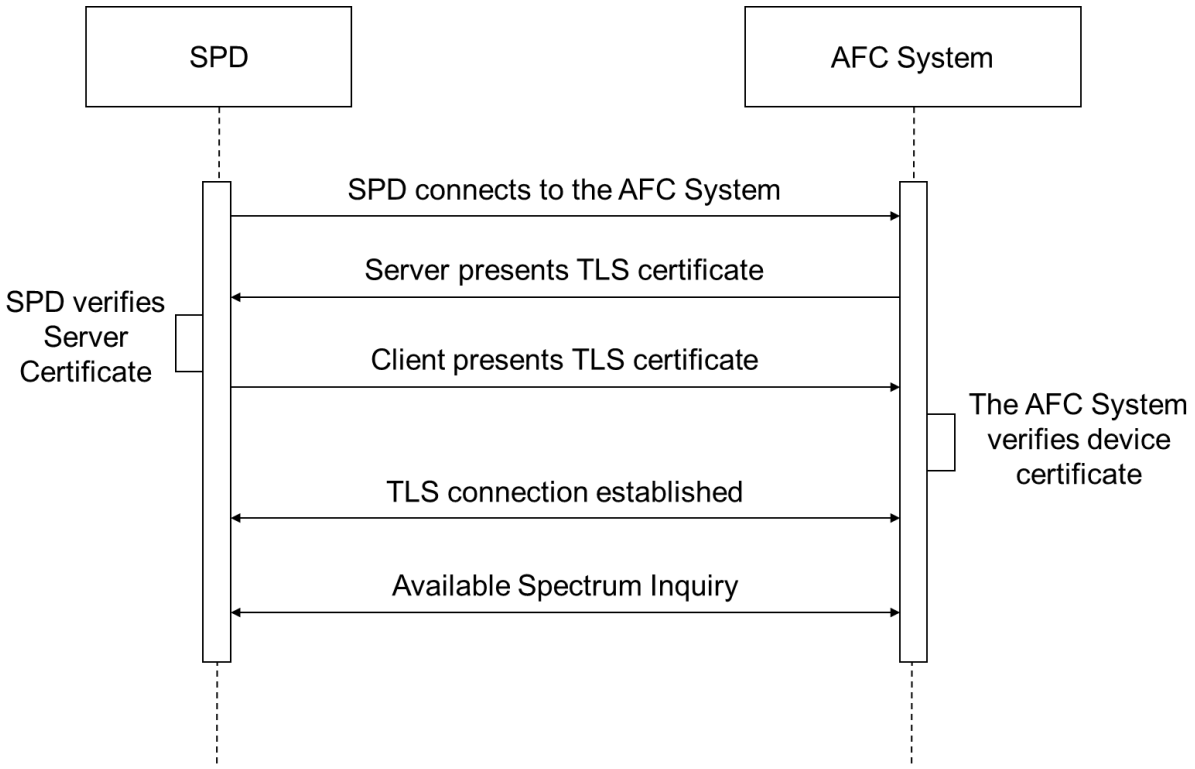

Figure 5.2-1: An AFC System and an SPD successfully authenticate each other using TLS certificates

Figure 5.2-2 provides the call flow in the case where an SPD queries an AFC System through a Proxy. In this case, the Proxy and the AFC System authenticate each other using TLS certificates, where the interface between the SPD and the Proxy is not standardized. The Proxy's certificate contains the FRN of its manufacturer, together with a unique number for the particular Proxy assigned by the owner of the FRN, as part of the certificate's subject information. See WINNF-TS-2013 [i.8] for more details of the specifications for certificates.

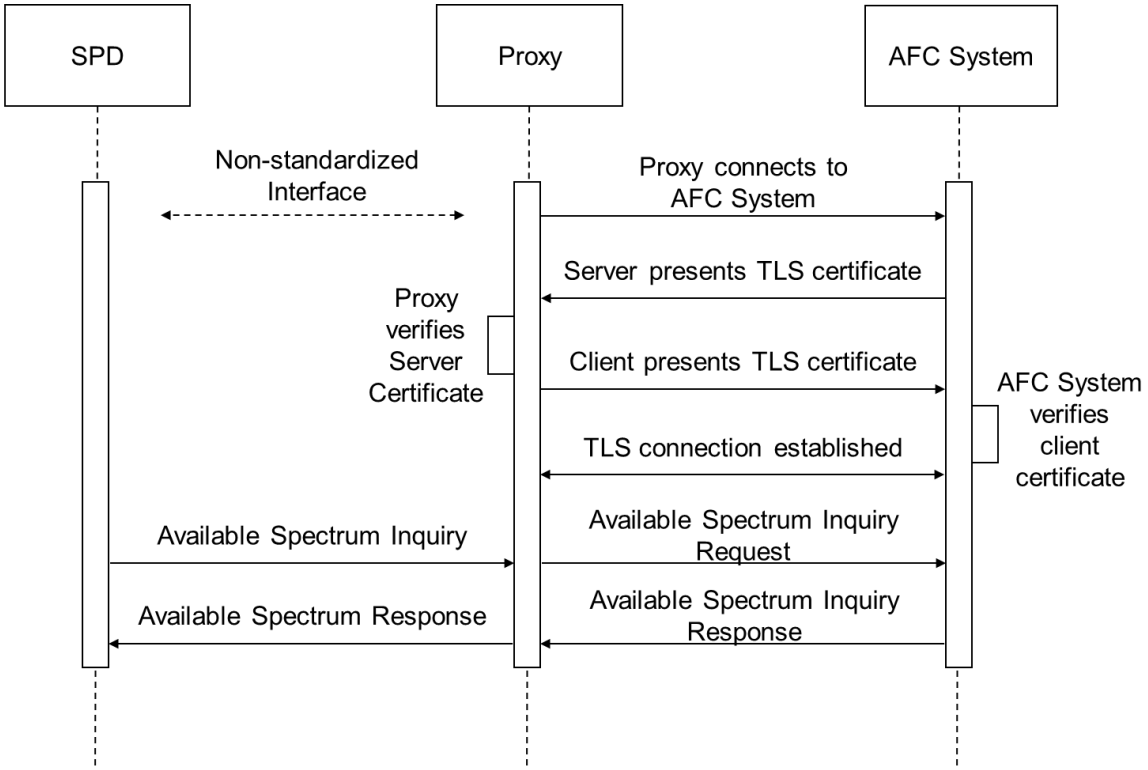

Figure 5.2-2: An AFC System and a Proxy successfully authenticate each other using TLS certificates

5.3 Use of Bearer Tokens

Another approach to satisfy 47 CFR 15.407(k)(8)(v) is to use AFC System generated Bearer Tokens [i.1]. The Bearer Token can authorize the bearer because the AFC System will only generate tokens for trusted entities. The Bearer Token can also authenticate the bearer as a proxy or a specific device. Because the Bearer Token is transmitted as part of the HTTPS request, it is encrypted during communication. Bearer Tokens are part of OAuth 2.0, which is commonly used in industry [i.2]. The AFC System following this method securely distributes Bearer Tokens following a method such as those defined by OAuth 2.0.

Standard TLS provides AFC System authentication to the device and a Bearer Token provides device authentication to the AFC System. Communication between the AFC System and the device will be done through HTTPS. This will be standard TLS, where only the AFC System will present a certificate to the device. As part of the HTTPS request, the client must send a Bearer Token in the Authorization header of the request, i.e., `Authorization: Bearer <TOKEN>`. The token will only be valid for a period of time. Any request without the token will be rejected. The AFC System must validate the token. If the token is not recognized, the request will be rejected. If the token is expired, the request will be rejected.

Figure 5.3-1 provides the call flow in the case where the AFC System successfully verifies the Bearer Token and authentication is successful.

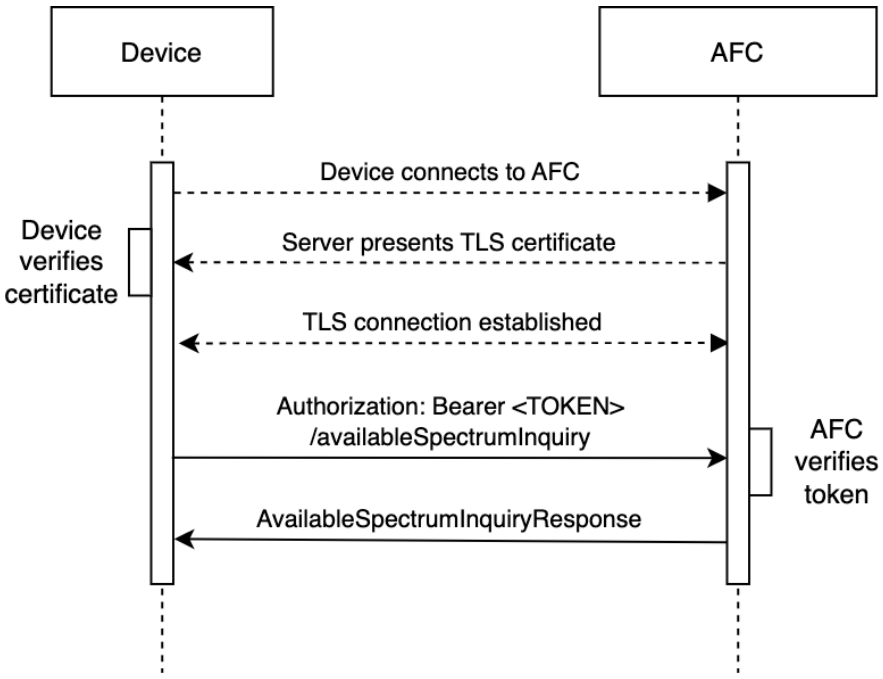

Figure 5.3-1: AFC System verifies token

Figure 5.3-2 and Figure 5.3-3 provide negative call flows for the case where the token is unauthorized/rejected, missing, and mismatched with payload, respectively.

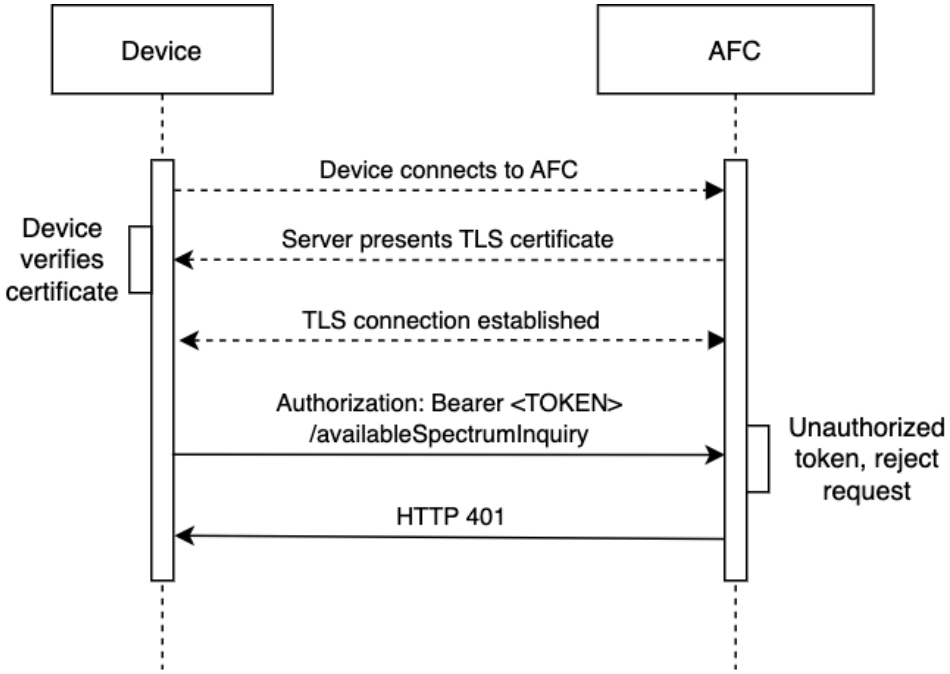

Figure 5.3-2: Unauthorized Token

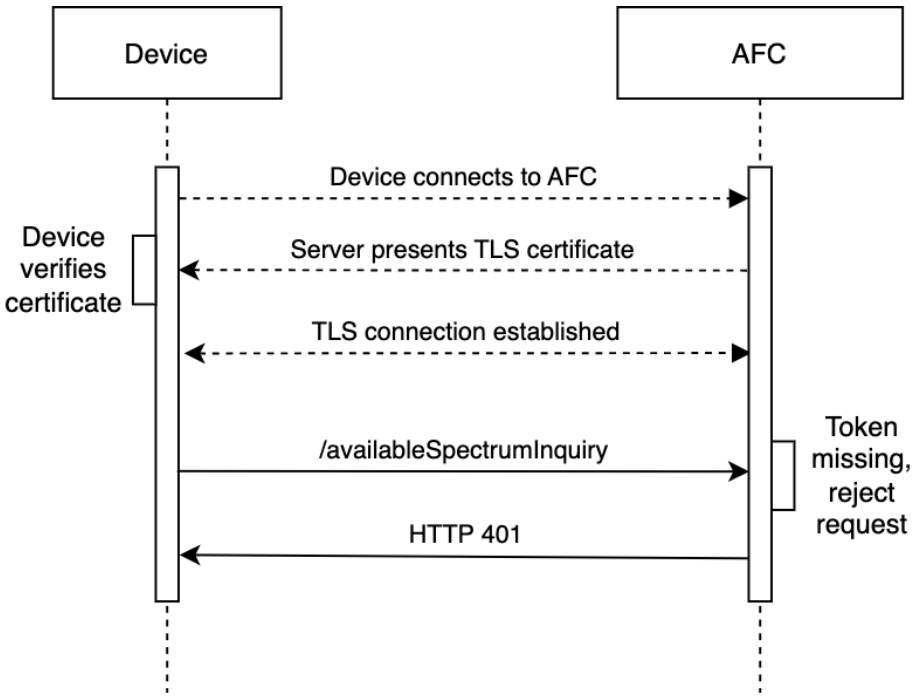

Figure 5.3-3: Missing token

NOTE 1: Before the AFC System issues a Bearer Token to an SPD, the AFC System needs to authenticate and perform authorization check on the requestor. Because Bearer Tokens are short-lived, a programmatic interface is needed for their acquisition. Both the authentication mechanism and the Bearer Token acquisition interface could benefit from standardization, from ease of implementation and interoperability standpoints.

NOTE 2: This solution relies critically on TLS server authentication for protection of Bearer Tokens in transit. The issuer of the TLS Server Certificate used by the AFC System needs to be trusted by the parties responsible for the SPDs' compliance with 47 CFR 15.407(k)(8)(v).

Annex A: Document History

Document History		
V1.0.0-r2.0 (towards V1.0.0)	29 June, 2023	Initial Version