

January 19, 2018

Marlene H. Dortch, Secretary  
Federal Communications Commission  
445 12th Street, S.W.  
Washington, D.C. 20554

Re: Promoting Spectrum Access for Wireless Microphone Operations (GN Docket No. 14-166); Expanding the Economic and Innovation Opportunities of Spectrum through Incentive Auctions (GN Docket No. 12-268).

Dear Ms. Dortch:

Shure Incorporated (“Shure”), together with the Aerospace and Flight Test Radio Coordination Council, Inc. (“AFTRCC”), by their undersigned counsels, hereby submit this *ex parte* communication to update the Commission on the material progress in ongoing discussions between representatives of AFTRCC and major wireless microphone manufacturers to implement the Commission’s August 2015 Report and Order in the above-captioned proceedings.<sup>1</sup>

In the 2015 Report and Order, the Commission determined that the 1435-1525 MHz band would be made available, on a secondary basis, for licensed professional wireless microphone operations at specified locations and under particular conditions to ensure adequate protection of primary aeronautical mobile telemetry (“AMT”) and flight test operations.<sup>2</sup> Specifically, the Commission required that “[w]ireless microphone users in the band must be coordinated with the non-governmental coordinator for assignment of flight test frequencies in the band (i.e., AFTRCC), and authentication and location

---

<sup>1</sup> *Promoting Spectrum Access for Wireless Microphone Operations; Expanding the Economic and Innovation Opportunities of Spectrum Through Incentive Auctions*, GN Docket Nos. 14-166, 12-268, Report and Order, 30 FCC Red 8739, 8749 (2015) (“2015 Report and Order”).

<sup>2</sup> Primary Federal government users of this spectrum, often with the support of aerospace government contractors, are the Department of Defense (“DOD”), the National Aeronautics and Space Administration (“NASA”), and the Department of Energy (“DOE”). The commercial aviation industry uses the band for flight testing of new and modified commercial, corporate, and general aviation aircraft at various facilities across the United States.

verification will be required before a coordinated wireless microphone begins operations.<sup>3</sup> Further, Section 74.803(d) of the Commission's Rules was added by the Report and Order to require that Part 74 Low Power Auxiliary Station ("LPAS") devices, i.e., wireless microphones, "must . . . employ software-based controls or similar functionality to prevent devices in the band from operating except in the specific channels, locations, and time periods that have been coordinated [with AFTRCC], and be capable of being tuned to any frequency in the band."<sup>4</sup> In rendering its decision, the Commission declined to impose specific operational procedures and technical requirements and instead decided to "leave the details of these matters for resolution at a future time, to be informed by further negotiation between manufacturers and the flight test community."<sup>5</sup>

In the spirit of that flexible approach, representatives of AFTRCC and wireless microphone manufacturers have worked cooperatively and constructively to address the priority concerns of AFTRCC's membership and operational needs of the licensed wireless microphone users likely to seek coordination to operate in the 1.4 GHz band. Shure, with input from others in the wireless microphone manufacturing community, has been working on an approach to implement the Commission's decision for products designed to operate in this band.

On November 15, 2017, representatives of two major wireless microphone manufacturers (Shure and Sennheiser Electronics Corporation) participated in discussions with AFTRCC coincident with the semi-annual AFTRCC meeting held in San Antonio, Texas, and presented a progress report to the participating AFTRCC members on the current certificate-based approach that has been developed with consultation among manufacturers to enable wireless microphone equipment to operate on a secondary, shared basis in the 1.4 GHz band. The certificate-based spectrum sharing approach under discussion is being designed to ensure that wireless microphones would transmit only at authorized locations, on allowed frequency ranges, and at specified time frames as reflected in the AFTRCC coordination for the particular operation. As envisioned by the Commission's 2015 Report and Order, software-based and equipment controls will prevent devices from operating in the band except when and where coordination was successful. Equipment authentication under this approach would be done through an automated mechanism and repeated

---

<sup>3</sup> The Commission required that wireless microphone "equipment authentication be done through an automated mechanism and repeated regularly, that the equipment be designed to automatically cease operation in the absence of such registration and authentication, and that the equipment incorporate a geolocation capability more sophisticated than the manual entry of coordinates." Report and Order at Para 119.

<sup>4</sup> 47 C.F.R. §74.803(d).

<sup>5</sup> Report and Order at Para 120.

regularly, at least once per 24 hours, as contemplated in the manufacturers' plan presented to AFTRCC. A public key infrastructure and digital signature would assure authenticity and data integrity.

In practice, the automated coordination system under discussion would work as follows:

- A licensed wireless system operator will submit a request to AFTRCC, seeking permission to use a specific amount of spectrum, at a specific location, on a particular date(s), and for a specified duration of time.
- AFTRCC officials will evaluate the request, and if granted, issue a digitally signed certificate in the form of a file, which can be sent to the requester. Digital certificates will not only formally grant a user permission to operate in the requested band, but will enable enforcement of that permission at the device level.
- The wireless microphone operator will download the certificate file to the wireless microphone system, deploy the wireless microphone at the designated location, and enable its geo-awareness device function. Provided that the certificate is authentic and not corrupt and the hardware is situated within the specified geo-perimeter (confirmed through integrated or adequately tethered geolocation capability) and seeks operation within the authorized time-frame, the wireless microphone system would be allowed to operate within the permitted frequency range.

At the November 15 AFTRCC meeting, Shure circulated the attached White Paper "AFTRCC 1435 – 1525 MHz Certificate Based Spectrum Sharing" which discusses in further detail all aspects of the sharing scheme it has developed for consideration including software and hardware features required to implement this approach. In view of the significant progress in developing a detailed framework for the sharing scheme represented in the White Paper, representatives of AFTRCC and wireless microphone manufacturers informally agreed at the meeting to form a working group to begin solidifying the inbound request system requirements in early 2018.

The Commission should also be aware that the attached White Paper has been circulated by Shure within the global professional audio community and has generated interest within working groups studying permissions-based spectrum access concepts, particularly within the European Telecommunications Standards Institute ("ETSI"), where similar proposals for spectrum sharing between wireless microphones and incumbent operations are being explored. The approach in the White Paper under discussion holds promise for a successful implementation of the operational controls for wireless microphones required

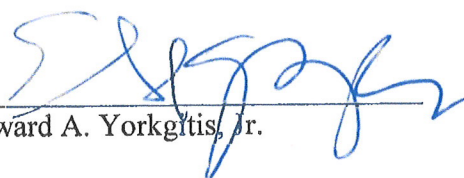
Marlene H. Dortch, Secretary  
January 19, 2018  
Page 4

by the Commission and could pave the way for a wider adoption of the concept in other regions of the world.

As Shure, other manufacturers, and AFTRCC continue their discussions, they intend to update the Commission on further progress in developing a joint approach to the matters discussed herein,

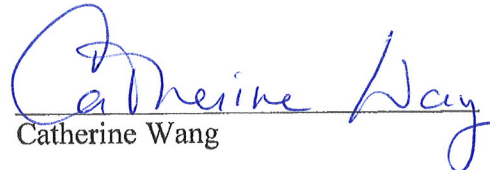
Please address any questions regarding this *ex parte* submission to the undersigned individuals.

Very truly yours,

  
\_\_\_\_\_  
Edward A. Yorkgitis, Jr.

Kelly Drye & Warren, LLP  
3050 K Street, N.W.  
Washington, DC 20007  
Bus.: 202.342.8400  
Fax.: 202.342.8451

Counsel to Aerospace and Flight Test  
Radio Coordination Council, Inc.  
("AFTRCC")

  
\_\_\_\_\_  
Catherine Wang

Morgan, Lewis & Bockius LLP  
1111 Pennsylvania Avenue, N.W.  
Washington, DC 20004  
Bus.: 202.739.3000  
Fax.: 202.739.3001

Counsel to Shure Incorporated

Attachment

# AFTRCC 1435 – 1525 MHz

## Certificate Based Spectrum Sharing

### 1.1 Background Information

#### 1.1.1 AFTRCC

Aerospace & Flight Test Radio Coordinating Council (AFTRCC) is a professional non-profit organization of Radio Frequency Management Representatives from major aerospace manufacturing companies. AFTRCC is the only organization dedicated to protecting radio frequencies used for flight evaluation. One of its main objectives is efficient allocation and utilization of the electromagnetic spectrum, in connection with the flight testing of aircraft, missiles and major components thereof. The RF band 1435 – 1525 MHz is allocated specifically for use in collecting telemetry data from a test subject during flight.

Flight testing is conducted in limited areas around the country, mostly around military bases and commercial airports where private aerospace companies are located. Receive sites track the planes over a 200 mile distance with very high gain parabolic antennas, typically oriented with a 0-degree grazing angle and mounted on top of buildings or antenna towers.

Since the receive antennas look out over the horizon, AFTRCC must ensure any wireless microphone operating in the 1425-1525MHz range is not located anywhere near the path to the aircraft.

Currently AFTRCC performs all frequency coordination manually. All their communications rely primarily on email, conventional mail, fax, and phone.

#### 1.1.2 Sharing AFTRCC frequencies with Wireless Microphones

With the spectrum available to wireless microphones shrinking year after year, the possibility of sharing spectrum with other users has become an important option. The 1435 -1525 MHz band -- coordinated by AFTRCC -- offers sharing potential due to the limited number of test sites and their highly coordinated use. With no other operators in this frequency range, the band offers 90MHz of virtually interference-free spectrum that can be used by wireless microphones in many areas of the US.

AFTRCC already shares flight telemetry spectrum at 2360MHz with Medical Body Area Networks (MBAN). This sharing was enabled through AFTRCC partnering with GE Healthcare on a promise that MBAN devices could be restricted to indoor use only. GE created a demonstration that showed MBAN devices turning off once they left the room. This demonstration paved the way for a joint proposal to the FCC by GE and AFTRCC that resulted in a sharing agreement in 2360MHz

In the case of wireless microphone systems, AFTRCC required that they transmit only **at the authorized location and within allowed frequency range and time frame.**

The following technologies used together with wireless microphone systems can assure compliance with AFTRCC requirements:

- Geo location and time awareness via
  - Ethernet connected GPS receiver
  - Mobile phone/tablet geo coordinate server operating over WIFI
- Certificate based configuration of wireless receiver and transmitter
  - Certificate specified configuration

- Digital signatures for certificate authentication

While this section discusses technologies specifically designed to meet AFTRCC requirements, they could also be used in similar spectrum sharing scenarios.

### 1.1.3 Proposed Scenario for Reserving and Using AFTRCC Spectrum

Currently, AFTRCC's method of interacting with wireless operators is very manual and based on forms users need to fill out and submit, typically via email. AFTRCC officials handling the forms perform necessary coordination and verification of the location and time requested, and then determine whether the request can be approved.

The general scenario of an authorized use of shared spectrum would typically consist of the following steps. (Notice that the financial aspect of the spectrum reservation or specific mechanisms by which a user makes a request and receives a response are ubiquitous and not specifically discussed here.)

- A **licensed** wireless system operator submits a request to AFTRCC, asking for use of a specific frequency range, at a specific location, and for a specified duration of time.
- AFTRCC officials process the request, and if granted, issue a **digitally signed certificate** in form of a file, which can be sent to the requester. Digital certificates not only formally grant a user permission to operate in the requested band, but enable **enforcement of that permission at the device level**.
- The user downloads the certificate file to the wireless microphone system, deploys the wireless microphone at the designated location, and enables its geo-awareness function. Provided the certificate is authentic and not corrupt and the hardware is situated within the specified geo perimeter and time frame, the system would be allowed to operate within the permitted frequency range.

## 1.2 AFTRCC Certificates

Operation of wireless microphone systems in the 1435 – 1525 MHz band is strictly regulated and coordinated by AFTRCC. The certificate AFTRCC issues in response to a user's request would contain all aforementioned restrictions plus any metadata (e.g. wireless operator's name, address, location address, etc.). AFTRCC's firm expectation is that wireless systems operating in the band respect restrictions and **never transmit** outside specified restrictions.

The enforcement of the certificate-specified restrictions is two-pronged:

- Certificates cannot be forged or altered
- Wireless system HW would not transmit unless it has an authentic certificate and all the restrictions specified in the certificate are observed

This section is dedicated to cryptographic techniques assuring AFTRCC certificate's authenticity and data integrity.

An AFTRCC certificate file would contain plain human readable data (the main content of the certificate) **digitally signed** by AFTRCC. The certificate could be compared to a driver's license or a passport, where all information is clearly readable, yet the authenticity of the document is manifested via holographic seals, or other components that only an authorized authority (the issuer of the document) can make.

### 1.2.1 Digital Signatures

Digital signatures, just like conventional signatures, serve a singular purpose – they authenticate the document. The recipient of a signed document is expected to have a means of tying the signature to the signer. Unlike a conventional signature, a digital signature can be authenticated only by specialized software.

The rest of this subsection describes how AFTRCC could create a unique signature, sign its certificates, and how devices operating based on such certificates would authenticate

#### 1.2.1.1 Public Key Infrastructure (PKI). Very Brief Overview

In brief, PKI is what makes all modern e-commerce possible. Every time a user logs into an online account (bank, online retailer, or even social media site), he/she would like to be assured that the site is what it claims to be, and not an imposter. All this site authentication work is performed by modern browsers or other client software in the background, with users hardly noticing anything.

While public-key cryptography theory has been purportedly developed by British Intelligence in late 1960s – early 1970s, due to secrecy of the work, the research has never been revealed or published. It is Diffie, Hellman (Stanford), and Merkle (Georgia Tech), who have become world famous as the cryptographers who invented the concept of public-key cryptography, while Rivest, Shamir, and Adleman have been credited with developing RSA, the most elegant implementation of public-key cryptography.

Unlike the symmetric key cryptography where the same key is used to encrypt and decrypt data, in public-key cryptography there are two keys. Data can be encrypted with one key and decrypted with the other key. This solved the most difficult problem of securing secret key distribution. With public-key cryptography, the owner of the resource (i.e. website) keeps the private key secret and never distributes it. The public key is readily available to anyone in the world. What is encrypted with the public key can be only decrypted with the matching private key and vice versa.

At the heart of the PKI framework is Certificate Authority (CA), an entity that issues digital certificates. A digital certificate certifies the ownership of a public key by the named subject of the certificate. CA is a trusted third party -- trusted both by the subject (owner) of the certificate and by the party relying on the certificate. The owner of the certificate is also issued a private key to be kept secret at all times, while the matching public key is published in a publically available certificate.

The most common practical realization of a digital certificate today is an SSL certificate. When installed on a web server, it activates the padlock and the https protocol and allows secure connections from a web server to a browser. It also allows the certificate holders to use their private key to sign any file.

#### 1.2.1.2 AFTRCC's Digital Signature

AFTRCC is already in possession of a valid SSL certificate, and therefore has a private key it could use to sign the certificates it issues. DigiCert Inc is the certificate authority that has issued www.afrcc.org, its current SSL certificate. AFTRCC could obtain a separate digital certificate for the specific purpose of signing its certificates.

The following two-step operation of signing certificates is depicted in Fig. 1 and Fig. 2

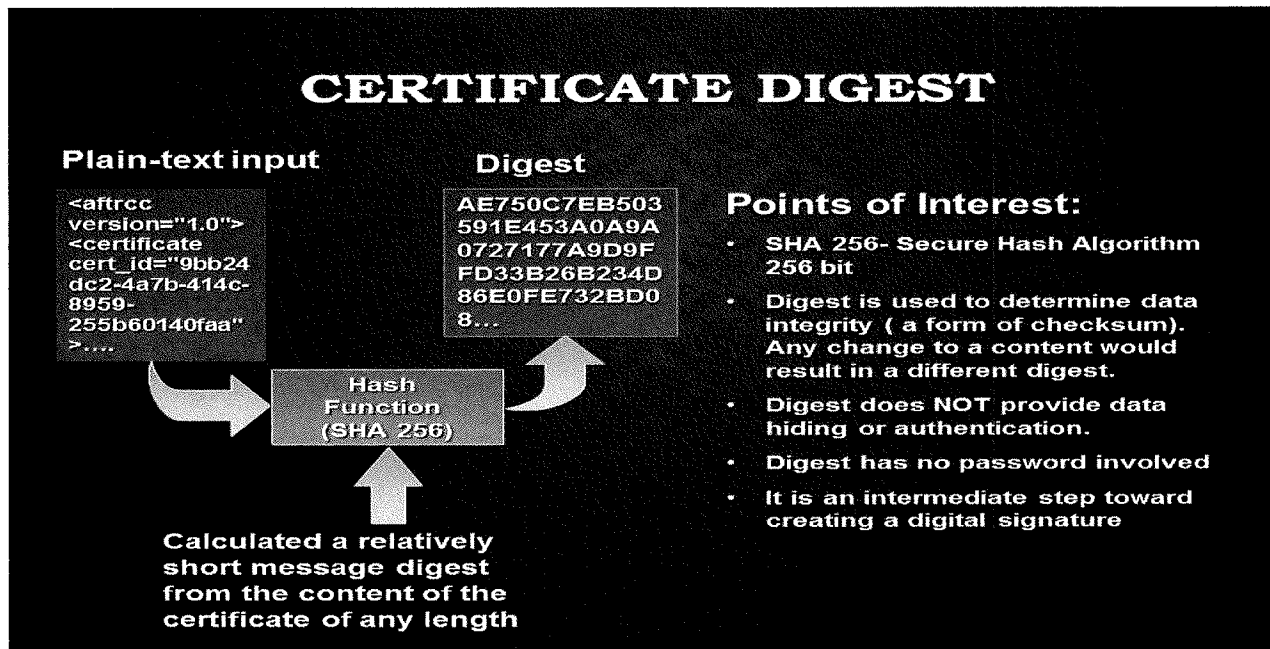


Fig. 1 Creation of certificate digest

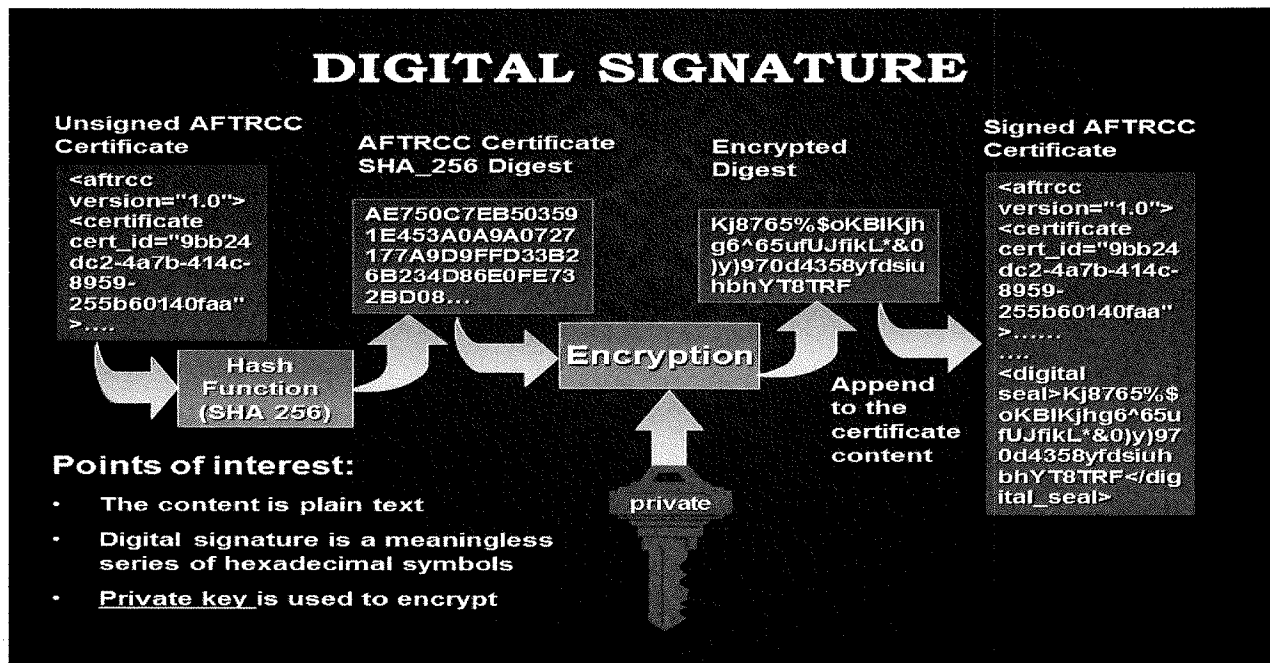


Fig. 2 Generation of digital signature and signing of the certificate

The signing of the certificate would happen automatically or semi-automatically (user triggered) upon an AFTRCC official approving a request. The exact content of AFTRCC certificate is irrelevant, however the geo perimeter, time, and frequency restrictions must be specified in order to be set in the wireless microphone systems.

Once the certificate in a form of a file is delivered to the requester, it needs to be downloaded to wireless systems intended to be used at the specified location, within specified time frame, and within allowed frequency range. The exact mechanism used in delivering the certificate file or its content to devices is up to hardware designers.



Before a device can operate based on the certificate data, it must establish its authenticity and data integrity. The following diagram depicts the process.

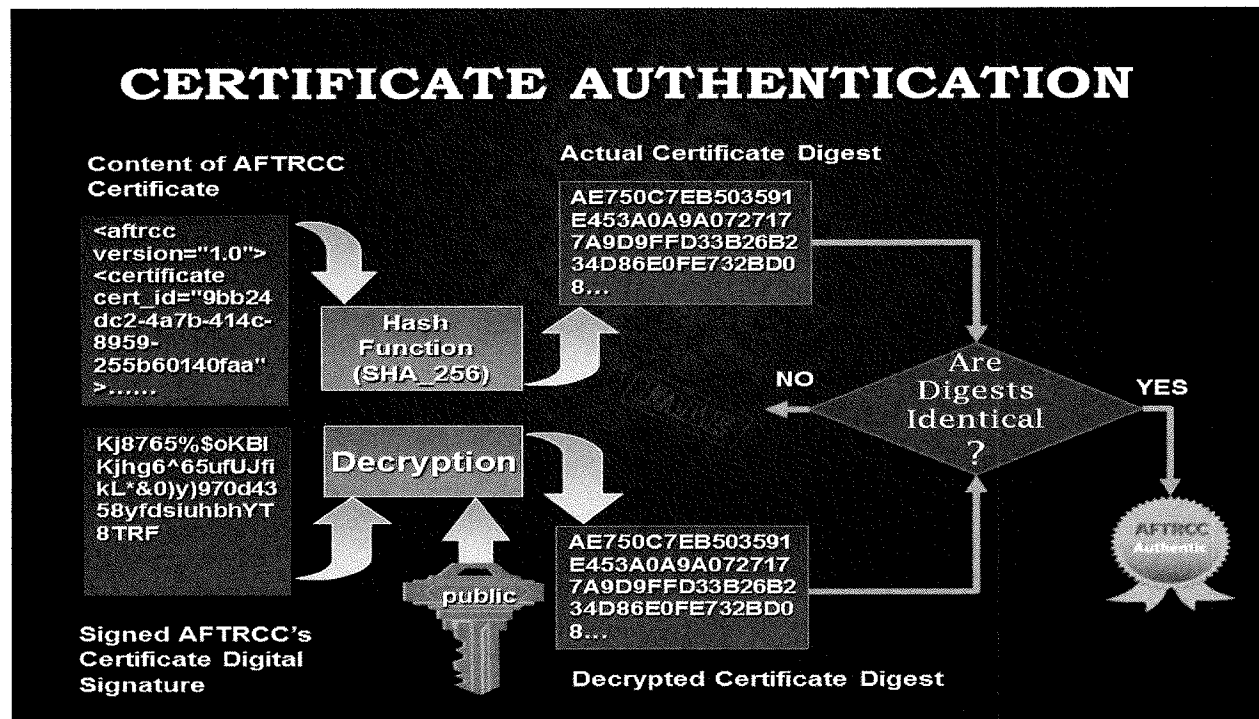


Fig. 3 Authenticating AFTRCC certificate.

The practical realization of the process depicted in Fig.3 is accomplished all in the device firmware or device management software. Once again, it is up to system designers how to implement it. Cryptographic tools capable of all necessary functions are widely available for any software platform.

### 1.3 Geo location awareness

Wireless microphone systems must be able to operate exclusively within a geo perimeter designated by AFTRCC's certificate. Such geo perimeter is typically designated as a GPS coordinate and a radius. Both parameters are provided by wireless system operators during their request and recorded in the certificate issued by AFTRCC upon approval.

#### 1.3.1 Acquiring Geo Coordinates and Current Time

While a variety of methods can be used to serve GPS and time data to the wireless systems, the following approach is practical and reasonable.

There are multiple industrial and consumer HW devices as well as such ubiquitous items as cell phones that can provide accurate geo coordinates in real time. Three particularly suitable ways of providing geo coordinates to HW devices are listed below (in an order of decreasing accuracy).

- **GPS receivers.** An Ethernet connected GPS receiver is best suited for the task. Veracity VTN-TN-PRO Master NTP Server is one of many industrial type GPS receivers and time servers capable of serving GPS data and real time in UTC (Coordinated Universal Time) to Ethernet connected devices. Just one such device can serve hundreds of clients (networked wireless receivers or transmitters).
  - **The GPS receiver in smart phones and tablets** with an accompanying application can serve networked devices via WIFI.

- **Mobile network geolocation** can be accomplished by any network connected cell phone. With a specialized phone application, GPS coordinates can be served to wireless systems via a WIFI network. The challenge of this approach lies in availability of cell service. Indoor operation could be problematic in some cases. IEEE article [Geolocation and assisted GPS](#) provides more in-depth information.
- **Wi-Fi positioning system (WPS)** can be used by most WIFI capable devices (phones, tablets, etc.) when GPS and cell networks are unavailable. The device does not require connection to WIFI in order to acquire its geo location.

Modern smart phones use all three methods at the same time and pick the most accurate available method.

All three methods of serving geo coordinates to wireless systems can also include Coordinated Universal Time and time zone information or local time. Current time is a requirement for wireless systems to stay compliant with the allowed time frame granted via a certificate.

## 1.4 AFTRCC 1435-1525 MHz Band Compliant Wireless Systems

The AFTRCC certificate is a time limited mandate within which a wireless system is permitted to operate. When sharing spectrum with wireless microphones, AFTRCC's primary concern is the microphone transmitter.

It is assumed at the present moment that portable devices do not have capability to receive geo coordinates and time directly from GPS/Timer server and need to be configured to observe the restrictions of AFTRCC certificates by some other means. This configuration can be achieved by various technologies.

In wireless systems with portable transmitters the main challenge lies in their configuration.

**Default out-of-the-box behavior of AFTRCC compliant transmitters must be RF OFF when powering on.** This assures that there could be no accidental transmission by a device regardless of the user's actions.

A wireless transmitter can be set up to transmit within specified frequency ranges and for a certain duration immediately after being synched with a receiver. In this scenario, a wireless receiver is presumed to have a valid AFTRCC certificate, as well as being able to receive GPS coordinates and UTC data. Once the receiver validates its current location and time per certificate data, it can configure a transmitter to operate accordingly. Upon synchronization, the transmitter would receive a frequency range within which it can tune and the duration of time (a.k.a. the **time lease**) within which it can transmit. The transmitter begins countdown from the given duration, and when the countdown reaches 0, it ceases to transmit.

Preliminarily, the maximum duration of the lease is set to 24 hours, meaning a wireless transmitter can transmit for 24 hours before it needs to get another lease. Since current battery technology would not allow a wireless microphone to operate for this long without battery change, AFTRCC compliant wireless transmitters could have a built-in real time clock, allowing the countdown to continue even when the main battery is removed. A real time clock powered by the additional power source also allows for any number of power off/on cycles without losing a lease and consequently, the ability to transmit. This means that the whole wireless microphone system can operate for up to 24 hours without needing to verify its geo location or real time. The 24 hour window greatly reduces dependability on the constant presence of GPS signals or Internet connectivity. After the lease expires, the transmitter **must** be synched with the receiver again if it needs to continue transmitting. Provided the allowed time frame has not expired and the receiver could validate its geo location, IR Sync would enable transmitter operation for another maximum of 24 hours or the time remaining to certificate expiration, whichever is shorter.

The following diagram puts all components together.

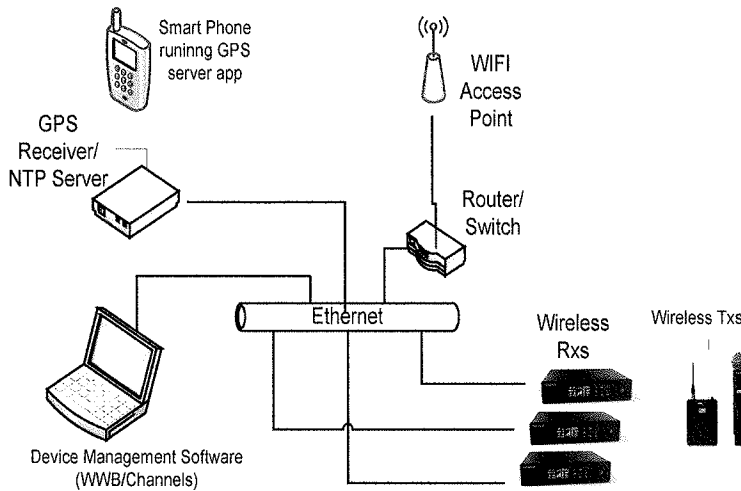


Fig. 4 Typical wireless system setup for operation in AFTRCC 1435 -1525 MHz band

The setup in Fig. 4 contains the components a wireless system operator would typically need to configure after obtaining a certificate from AFTRCC. For the sake of completeness, it shows two different ways GPS and UTC data can be provided: Ethernet wired GPS receiver/NTP server and a mobile device connected to the network via Wi-Fi.

These are typical operations a wireless microphone operator would need to perform to make the system fully operational

1. Request, obtain, and download AFTRCC certificates to all devices intended to operate in the 1435 – 1525 MHz frequency range (this could be a planning step done prior to the event).
2. Bring all devices to the venue.
3. Create a local network or use an existing network to which network capable devices are connected. This may or may not include setup and configuration of a Wi-Fi access point or a router. If the venue already provides a hookup to a local network, the wireless microphone operator would need to assure that all wireless receivers are discoverable and the connection to GPS server (wireless or wired) can be established.
4. Configure wireless receivers to connect to the GPS/NTP server.
5. Use Device Management Software or receiver front panel controls to verify that all wireless receivers have a valid authentic AFTRCC certificate and can receive current time and GPS coordinates. If not, download certificates to devices that do not have them yet or fix GPS server configuration in wireless receivers.
6. With all previous steps completed successfully, sync all wireless microphones to the receivers, which enables the microphones to transmit.

After completion of these steps, the system would become fully operational and should remain operational for the duration of the lease received by the wireless transmitters.