The description of the software must address the following questions in the operational description for the device and clearly demonstrate how the device meets the security requirements.

**Software Security Description**

1. Describe how any software/firmware update will be obtained, downloaded and installed

   Description:

   There are two ways (wireless and wired) to download and install the software/firmware:

   1. One way is from wireless based on WiFi
   2. Another is from wired, there is an 8-pin service port based on Ethernet on the back cover of the product, any new software/firmware can be obtained from the qualified database inside Flying voice.
   3. In both cases (a and b) for firmware upgrade first we have to create ota upgrade file using tools for creating incremental ota upgrade. Then the upgrade file need to upload on server. The Download manager apk will check the server url for upgrade after every boot. If upgrade file is found, it will compare the base version. If base version matches, then it will start upgrading. After upgrade device will reboot
   4. In case of software upgrade, new version of software apk need to be uploaded on server. Scope store apk will check the server url for upgrade. If upgrade found, it will start upgrading if it is force update. If server is configured for manual upgrade, it will ask user for downloading the software update.

2. Describe all the radio frequency parameters that are modified by any software/firmware without any hardware changes. Are these parameters in some way limited, such that, it will not exceed the authorized parameters?

   Description:

   Parameters. The product follows AP setting to adjust the frequency parameters.

3. Are there any authentication protocols in place to ensure that the source of the software/firmware is legitimate? If so, describe in details; if not, explain how the software is secured from modification

   Description:

   1. Firmware are encrypted with integrity check to ensure the validity of its content
   2. Without passing the firmware integrity check, no upgrade will be performed
   3. Incremental upgrade file is created from base (old) version and the new version. This can result in considerably smaller update packages. Files that have not changed don't need to be include. Files that have changed are often very similar to their previous versions, so the package need only contain an encoding of the differences between the two files. To build an incremental update, you need the target_files .zip from the previous build (the one you want to update *from*) as well as the target_files .zip from the new build.
   4. So when download manager find firmware upgrade file on sever, It will ccompare the base version. If base version matches, only then it will start upgrading. Thus it ensure the legitimate firmware upgrade.
   5. Attempting to install the incremental package on a device with some other build results in the recovery error icon. Rebooting the device at this point returns the user to the old system; the package verifies the previous state of all the files it updates before touching them, so the device should not be left in a half upgraded state if this occurs.

4. Are there any verification protocols in place to ensure that the software/firmware is legitimate? If so, describe in details

Description:

Any software/firmware modification will have the verification procedure and verification results and release letter and impact analysis report based on QMS/SDLC process.

Any modification will be highlighted on the release letter, and the impact analysis will also have a review. Verification procedure and verification results will be performed based on the release letter and impact analysis report.

5. Describe, if any, encryption methods used

Description:

No.

6. For a device that can be configured as a master and client (with active or passive scanning), explain how the device ensures compliance for each mode? In particular if the device acts as master in some band of operation and client in another; how is compliance ensured in each band of operation

Description:

1. The device can be operated as master and client, but the software only support a way to operated, if operate as master then client can't to operate and if operated as client then master can't to operate.
2. Responsibility of device acting as client or server depends on the apk which is running. For example if download manager apk, device acts as client and it downloads upgrade file from server.
3. When mobile apk communicates with device, it acts as server.

7. How are unauthorized software/firmware changes prevented?

Description:

1. Firmware are protected by encryption and its checksum for integrity check. Also firmware upgrade check the base version. If base version matches, only then it will upgrade. Without passing the firmware integrity check, no upgrade will be performed.
2. In case of software apk upgrade, app store will check the package name. If apk with same package name is already present in device then only, it will upgrade.

8. Is it possible for third parties to load device drivers that could modify the RF parameters, country of operation or other parameters which impact device compliance? If so, describe procedures to ensure that only approved drivers are loaded.

Description:

It is not possible

9. Explain if any third parties have the capability to operate a US sold device on any other regulatory domain, frequencies, or in any manner that is in violation of the certification.

Description:

It is not possible

10. What prevents third parties from loading non-US versions of the software/firmware on the device?

Description:

It is not possible

11. For modular devices, describe how authentication is achieved when used with different hosts.

Description:

It is not modular device.

In addition to the general security consideration, for devices which have “User Interfaces” (UI) to configure the device in a manner that may impact the operational parameter, the following questions shall be answered by the applicant and the information included in the operational description.

**USER CONFIGURATION GUIDE**

1. To whom is the UI accessible? (Professional installer, end user, other.)

a) What parameters are viewable to the professional installer/end-user?

Description:

Both professional installer and end user can view below parameters:

1. All Settings parameters like time and date, resolution, font, screen aspect ratio, Wifi and hotspot settings, Device information and all other android settings menu which are in settings menu are viewable to professional installer/end user
2. File manager apk, app store apk and other customer apks are viewable to end user/professional installer.

b) What parameters are accessible or modifiable to the professional installer?

Description:

Both professional installer and end user can access/modify below parameters:

1. All Settings parameters like time and date, resolution, font, screen aspect ratio, Wifi and hotspot settings, Device information and all other android settings menu which are in settings menu are accessible to professional installer/end user
2. File manager apk, app store apk and other customer apks are accessible to end user/professional installer.

i) Are the parameters in some way limited, so that the installers will not enter parameters that exceed those authorized?

Description:

All above parameters will run according to android specification in device and user will have access to all the parameters if password and username are correct where it is required.

ii) What controls exist that the user cannot operate the device outside its authorization in the U.S.?

Description:

All parameter are accessible in U.S. There is no location based parameter in the device.

c) What configuration options are available to the end-user?

Description:

time and date, resolution, font, screen aspect ratio, Wifi and hotspot settings, Bluetooth, sound, account information, Device information, system apks and installed apks. All these parameters are part of android settings apk.

i) Are the parameters in some way limited, so that the installers will not enter parameters that exceed those authorized?

Description:

All above parameters works according to android specification. User need authentication to access wifi, bluetooth. So this parameter is limited for end user who don't have authentication.

ii) What controls exist that the user cannot operate the device outside its authorization in the U.S.?

Description:

All parameters behavior is same in boxes in India and U.S.

d) Is the country code factory set? Can it be changed in the UI?

Description:

It is factory set and cannot be changed in the UI

i) If so, what controls exist to ensure that the device can only operate within its authorization in the U.S.?

Description:

This control is handled by customer apk. Android middleware give customer api to access the country name.

e) What are the default parameters when the device is restarted?

Description: Device shows welcome screen with all apks and then after some time customer apk

| |
|---|
| 2. Can the radio be configured in bridge or mesh mode? If yes, an attestation may be required. Further information is available in KDB Publication 905462 D02.<br>Description: No. |
| 3. For a device that can be configured as a master and client (with active or passive scanning),if this is user configurable, describe what controls exist, within the UI, to ensure compliance for each mode. If the device acts as a master in some bands and client in others, how is this configured to ensure compliance?<br>Description:<br>The device can be operated as master and client, but the software only support a way to operated, if operate as master then client can't to operate and if operated as client then master can't to operate. |
| 4. For a device that can be configured as different types of access points, such as point-to-point or point-to-multipoint, and use different types of antennas, describe what controls exist to ensure compliance with applicable limits and the proper antenna is used for each mode of operation. (See Section 15.407(a))<br>Description: Only point-to-point mode, no any other modes for configuration. |

How the product comply 15.407(c)

Description: WIFI chip support automatically discontinue transmission in case of either absence of information to transmit or operational failure, if the chip detect absence of information to transmit or operational failure, it will be automatically shut off.