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 one way (wireless) to download and install the software/firmware: a. One way is from wireless based on WiFi
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
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: 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.
7. How are unauthorized software/firmware changes prevented? Description: 1. Firmware are protected by encryption and its checksum for integrity check 2. Without passing the firmware integrity check, no upgrade will be performed

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 modify below parameters:

Mode, channel bandwidth, primary channel, channel, transmit power, Beacon interval, Legacy rate sets, SSII security type, but only within ROM pre-set authorized rang.

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

Description:

Mode, channel bandwidth, primary channel, channel, transmit power, Beacon interval, Legacy rate sets, SSII security type, but only within ROM pre-set authorized rang.

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

Description:

All above parameters have pre-defined rang according to the certification test result. They are stored in the ROM and shown in UI, which not allow user to adjust beyond the pre-set value

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

Description:

All parameters (RF, Frequency and etc.) indicating different countries are permanent setting in the ROM. If a device is a product for US, it cannot be changed for another region

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

Description:

Mode, Channel bandwidth, primary channel, Channel, transmit power, Beacon interval, Legacy rate sets, SSII security type, but only ROM pre-set authorized rang

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

Description:

All above parameters have pre-defined range according to the certification test result. They are stored in the ROM and shown in UI, which not allow user to adjust beyond there-set value

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

Description:

All parameters (RF, Frequencies and etc.) indicating different countries are permanent setting in the ROM. So if a device is a product for US, it cannot be changed for another region

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:

All parameters (RF, Frequencies and etc.) indicating different countries are permanent setting in the ROM. So if a device is a product for US, it cannot be changed for another region

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

Description:

The parameters that user latest saved in the UI

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.

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? Description: 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)) 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.