Shenzhen Zowee Technology Co., Ltd.

Date: 29/9/2015

FCC ID: 2AAP6ZM1100B1

Software Security Description

We, Shenzhen Zowee Technology Co., Ltd., hereby declare that requirements of Tablet PC have been met and shown on the following question.

Software Security Description	
General Description	1. Describe how any software/firmware update will be obtained, downloaded, and installed. Software that is accessed through manufacturer's website or device's management system, must describe the different levels of security. Description: The software only can be downloaded from Broadcom's website and installed by end user.and there is a detail doc for end users
	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: The radio frequency can not be configured via UI:Channel and Channel Bandwidth. All above two parameters are limited as a pre-set list for user to select from UI.
	3. Describe in detail the authentication protocols that are in place to ensure that the source of the software/firmware is legitimate. Describe in detail how the software is protected against modification. Description: The source is a read-only websit.
	4. Describe in detail the verification protocols in place to ensure that installed software/firmware is legitimate. Description: Firmware itself has a private checksum value inside ,if verified and then it cannot be allowed to be updated.
	5. Describe in detail any encryption methods used to support the use of legitimate software/firmware. Description: Ssl /aes /tkip
	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: Our device has two radios ,2.4G and 5G band.when client mode is enabled ,the working band also must be selected.and the master mode working on that band will be disabled automatically.
Third-Party Access Control	1. 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 impossible.Because RF parameters,country and other parameters are permanent settings in the rom
	2. What prevents third parties from loading non-US versions of the software/firmware on the device? Describe in detail how the device is protected from “flashing” and the installation of third-party firmware such as DD-WRT. Description: All parameters indicating different countries are permanent settings in the ROM.The software itselt doesn’t contain these parameters and so it will not be affected by version of software.
	3. For Certified Transmitter modular devices, describe how the module grantee ensures that hosts manufactures fully comply with these software security requirements for U-NII devices. If the module is controlled through driver software loaded in the host, describe how the drivers are controlled and managed such that the modular transmitter parameters are not modified outside the grant of authorization. Description: The product is not a modular device.

Software Security Description	
User Configuration Guide	1. To whom is the UI accessible? (Professional installer, end user, other.) Description: all of them
	a) What parameters are viewable to the professional installer/end-user? Description: Mode,Channel Bandwidth,Primary Channel.
	b) What parameters are accessible or modifiable by the professional installer? Description: Same as above.
	(1) Are the parameters in some way limited, so that the installers will not enter parameters that exceed those authorized? Description: All the 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 the pre-set value
	(2) What controls exist that the user cannot operate the device outside its authorization in the U.S.? Description: All the parameters indicating different countries are permanent settinds in the rom .so if a device is a product for US,it cannot be changed for another region.
	c) What parameters are accessible or modifiable to by the end-user? Description: Mode ,Channel Bandwidth ,Primary Channel

Shenzhen Zowee Technology Co., Ltd.

	(1) Are the parameters in some way limited, so that the installers will not enter parameters that exceed those authorized? Description: All the 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 the pre-set value
	(2) What controls exist that the user cannot operate the device outside its authorization in the U.S.? Description: All the parameters indicating different countries are permanent settinds 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: cannot
	(1) If so, what controls exist to ensure that the device can only operate within its authorization in the U.S.? Description: Cannot be changed
	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: The radio cannot be configured in bridge or mesh mode.
	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: User can only change channel for GUI.
	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: These antennas are for point to multipoint only,and antennas are fixed internally and are not suppose to be changed by user.

If any questions regarding this declaration, please don't hesitate to contact us.

Sincerely

Qiao Ying

Qiaoying Manager

Company name: Shenzhen Zowee Technology Co., Ltd.