Tablet of Software Security Description Guide

Software Security Description		
General description	1. Describe how any software/firmware updates for elements than can affect the device's RF parameters will be obtained, downloaded, validated and installed. For software that is accessed through manufacturer's website or device's management system, describe the different levels of security as appropriate.	Answer 1: The Software/firmware only can be obtained by the manufacturer and download from the internet. Answer 2:For software that is accessed through manufacturer's website or device's management system they have the same level of security for the reason of Note 1 and 2(Please see below). The software only provided basic setting rather than frequency range and power level setting.
	2. Describe the RF parameters that are modified by any software/firmware without any hardware changes. Are these parameters in some way limited such that any other software/firmware changes will not allow the device to exceed the authorized RF characteristics?	Answer: The RF parameters will not changes without hardware change for the software/firmware can't changes the frequency range parameters and power levels.
	3. Describe in detail the authentication protocols that are in place to ensure that the source of the RF-related software/firmware is valid. Describe in detail how the RF-related software is protected against modification.	Answer 1: For the first question please see note 1. Answer 2: For the second question please see note 2.
	4. Describe in detail any encryption methods used to support the use of legitimate RF-related software/firmware.	Answer: For the question please see note 1.
	5. 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?	Answer: For this product it can work as a master and is satisfied with the FCC standards. It is only certificated as a master device.
Third-party access control	1. Explain if any third parties have the capability to operate a U.S.-sold device on any other regulatory domain, frequencies, or in any manner that may allow the device to operate in violation of the device's authorization if activated in the U.S.	Answer: The third parties don't 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. For more details please see note 2
	2. Describe, if the device permits third-party	Answer: The device don't permit third-party

	software or firmware installation, what mechanisms are provided by the manufacturer to permit integration of such functions while ensuring that the RF parameters of the device cannot be operated outside its authorization for operation in the U.S. In the description include what controls and/or agreements are in place with providers of third-party functionality to ensure the devices' underlying RF parameters are unchanged and how the manufacturer verifies the functionality.	software or firmware installation for the reason describe in the note 1 and 2.
	3. For Certified Transmitter modular devices, describe how the module grantee ensures that host manufacturers 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 RF parameters are not modified outside the grant of authorization.	Answer: Not applied

Note:

1. The legitimate software/firmware have a 16 bytes verification code and the code can be identified by the underlying code of the main control IC. If the IC can't read the verification code it will recognize it as a illegitimate software/firmware.
2. The frequency range is set as the country code and end-user/third parties can not change the frequency range and power level parameter for the parameter is set in the underlying code of the RF IC. The software have no way to change the frequency range and power level.

SOFTWARE CONFIGURATION DESCRIPTION	
USER CONFIGURATION GUIDE	1.Describe the user configurations permitted through the UI. If different levels of access are permitted for professional installers, system integrators or end-users, describe the differences. Answer 1: For the end user, they only permit to select modulation mode(like 802.11b/g/n and etc.) and channel. The modulation mode and channel is underlying code in the RF IC and the RF parameter accord with FCC standards. Answer 2: No different levels of access are permitted for professional installers, system integrators or end-users.
	a) What parameters are viewable and configurable by different parties? Answer: For the end user, they only permit to select modulation mode(like 802.11b/g/n and etc.) and channel. The modulation mode and channel is underlying code in the RF IC and the RF parameter accord with FCC standards.
	b) What parameters are accessible or modifiable by the professional installer or system integrators? Answer: For the end user, they only permit to select modulation mode(like 802.11b/g/n and etc.) and channel. The modulation mode and channel is underlying code in the RF IC and the RF parameter accord with FCC standards.
	(1) Are the parameters in some way limited, so that the installers will not enter parameters that exceed those authorized? Answer: YES, please see the above note 2.
	(2) What controls exist that the user cannot operate the device outside its authorization in the U.S.? Answer: In the software end user only permit to select modulation mode(like 802.11b/g/n and etc.) and channel. The modulation mode and channel is underlying code in the RF IC and the RF parameter accord with FCC standards.
	c) What configuration options are available to the end-user? Answer: In the software end user only permit to select modulation mode(like 802.11b/g/n and etc.) and channel.
	(1) Are the parameters in some way limited, so that the installers will not enter parameters that exceed those authorized? Answer: YES, please see the above note 2.
	(2) What controls exist that the user cannot operate the device outside its authorization in the U.S.? Answer: End user have no way to make the device operate outside its authorization in the U.S. for the frequency band is limited by the underlying code
	d) Is the country code factory set? Can it be changed in the UI? Answer: The country code is factory set and can't change in the UI
	(1) If it can be changed, what controls exist to ensure that the device can only operate within its authorization in the U.S.? Answer: Not applied.
	e) What are the default parameters when the device is restarted? Answer: When the device is restarted the modulation mode and channel

	selection window will show that the parameter will be auto selected.
	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. Answer: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? Answer: No matter in which mode the transmit power, channel number and frequency range is not changed and control by the country code. These parameters can't be change.And this product not support DFS bands
	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)) Answer: Not supported different types of access.