Software Security Description

KDB 594280 D02 U-NII Device Security v01r03 Section II

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.	FW：Customer can't change nor modify it. SW：it will be obtained by OEM factory. The user or installer cannot modify the content.
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?	The RF parameter is written inside the firmware and in Binary coding sequence. It is fixed at the time of production. Customers cannot change or modify it.
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.	The RF related part is inside the firmware and in Binary coding sequence. Customers cannot change or modify it.
4. Describe in detail any encryption methods used to support the use of legitimate RF-related software/firmware.	Use the same encryption methods with 2.4GHz
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?	Compliant with FCC requirement, both active and passive scanning.

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.	Firmware is in binary coding sequence, third parties cannot change or modify it.
2. Describe, if the device permits 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	Firmware is in binary coding sequence, third parties cannot change or modify it.

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.	
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.	Firmware is in binary coding sequence, host manufacturers cannot change or modify it. Driver is the same for US or other countries.

SOFTWARE CONFIGURATION DESCRIPTION – KDB 594280 D02v01r02 Section III

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.	Professional installers
a) What parameters are viewable and configurable by different parties?	Professional installers can upgrade the firmware. End-Users can only see general information. (channel of operation, connection status)
b) What parameters are accessible or modifiable by the professional installer or system integrators?	WiFi/BT coexistence parameters, configuration of channel / frequency under FCC rules.
(1) Are the parameters in some way limited, so that the installers will not enter parameters that exceed those authorized?	Yes, configuration of channel / frequency, modulation type and transmit power are not modifiable by installers or users.
(2) What controls exist that the user cannot operate the device outside its authorization in the U.S.?	User cannot control. The UI cannot allow access to parameter settings.
c) What parameters are accessible or modifiable by the end-user?	No configuration accessible by end-users. Users can only see general status. Regulatory parameters are not accessible.
(1) Are the parameters in some way limited, so that the user or installers will not enter parameters that exceed those authorized?	No configuration accessible by end-user. Regulatory parameters are not accessible.
(2) What controls exist so that the user cannot operate the device outside its authorization in the U.S.?	No configuration accessible by end-user. Regulatory parameters are not accessible.
d) Is the country code factory set? Can it be changed in the UI?	It cannot be changed 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.?	It cannot be changed in the UI
e) What are the default parameters when the device is restarted?	US
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.	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?	End-user cannot configure it.
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))	End-user cannot configure it