Date: 2019-11-07
FCC ID: **2AUYB-TXXX**

Software Operational Description

We,LEONTON Technologies, Co. Ltd.. hereby declare that requirements of KDB 594280 D02 U-NII Device Security v01r03 have been met and shown on the following question. Further we declare that the info listed below are correct and represent the product in consideration under this filing.

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.

Description:

(1) Obtain and download
The firmware could be obtained at below link address:
https://www.leonton.com/

(2) Install The product has provided user a WEB UI interface, with which user could upgrade new firmware

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?

Description:

Two radio frequency parameters can 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 RF-related software/firmware is valid. Describe in detail how the RF-related software is protected against modification.

Description:

The source is a read-only web page. And the web server is secured with firewalls.
Besides, firmware itself has a private checksum value and MD5 value inside. If firmware is modified, then its checksum and MD5 value cannot be verified, and then it cannot be allowed to be upgraded.

4. Describe in detail any encryption methods used to support the use of legitimate RF-related software/firmware.

Description:

Firmware itself has a private checksum value and MD5 value inside. If firmware is modified, then its checksum and MD5 value cannot be verified, and then it cannot be allowed to be upgraded.
SSL / AES / TKIP

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?

Description:

Our device has two radios, one for 2.4G band and another for 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. When each mode is selected, the wireless driver will be configured with specific settings for selected mode to let it work in that mode.

6. 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.

Description:

The device don't permits third-party software or firmware installation.

7. 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 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.

Description:

It is impossible. Because RF parameters, country and other parameters (related to device compliance) are permanent settings in the ROM.

All parameters indicating different countries are permanent settings in the ROM. The software/firmware itself doesn't contain these parameters and so it will not be affected by version of software.

8. 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.

Description:

Because RF parameters, country and other parameters (related to device compliance) are permanent settings in the ROM.

All parameters indicating different countries are permanent settings in the ROM. The software/firmware itself doesn't contain these parameters and so it will not be affected by version of software.

9. 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.

a) What parameters are viewable and configurable by different parties?

Description:

Both professional installer and end user can modify below parameters:
Mode, Channel Bandwidth, Primary Channel, Channel, Transmit Power, Beacon Interval, Legacy Rate Sets, SSID, Security Type, but only within ROM pre-set authorized range.

b) What parameters are accessible or modifiable by the professional installer or system integrators?

Description:

Same as above.

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 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, Frequencies and etc.) indicating different countries are permanent settings 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 by the end-user?

Description:

Mode, Channel Bandwidth, Primary Channel, Channel, Transmit Power, Beacon Interval, Legacy Rate Sets, SSID, Security Type, but only within ROM pre-set authorized range.

i) Are the parameters in some way limited, so that the user or 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 the pre-set value.

ii) What controls exist so 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 settings 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 it can be changed, 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 settings 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

10. 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:

Mesh mode is not supported. For bridge mode our device can only connect to the access point with specific SSID.
Our device supports bridge mode, but does not operate on any DFS channels.
Our device will communicate with the access point after receiving beacon packet from the access point with specific SSID.

11. 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, and GUI has limited the selectable channel, so user has no way to break compliance on our device.

12. 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 (three PIFA antennas) are for Point to Multipoint only, and antennas are fixed internally (or antenna with unique connector supplied with device.) and are not suppose to be changed by user.

If you should have any question(s) regarding this declaration, please don’t hesitate to contact us.
Thank you!

Eva Wu 數位簽署者：Eva Wu 日期：2019.11.07 19:14:36+08'00'

Name: / Title:
Eva Wu / Product Specialist

Tel: +886-2-2218-3113
Fax: +886-2-2218-7391
E-mail: eva.wu@leonton.com