ASUSTeK COMPUTER INC.
4F,NO. 150,Li-Te Rd. Peitou,Taipei Taiwan
TEL: +886-2-2894-3447 FAX: +886-2-2898-7364

Date: 2015-05-28

FCC ID: MSQ- RT0K00

Software Operational Description

We, **ASUSTeK COMPUTER INC.** hereby declare that requirements of KDB594280 have been met and shown on the following question.

1. Describe how any software/firmware update will be obtained, downloaded, and installed.

Description:

There are two ways to update firmware.

1. Users could upgrade their firmware manually. the latest software/firmware will be updated ASUS global website when it's available. You may click "Browse" from the Firmware Upgrade page for the upgrading.

2. Users may click "Check" on Firmware Update page to check the latest firmware from ASUS server for the auto update. You may decide for the updating.

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:

For devices sold in the United States, the programmed frequencies are:

Radio 2.4 GHz: 2.402GHz ~ 2.472GHz

Radio 5 GHz: 5.170GHz ~ 5.250GHz, 5.735GHz ~ 5.835GHz

The radio range is assigned by our software/firmware, and cannot be configured outside of the given range. The country of operation is programmed in the factory and is not able to be changed by users or installers.

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:

When user upgrades firmware manually, ASUS firmware will check the model name in the new firmware to see if it is the same with the current firmware in device. In addition, the header of the firmware information will be reviewed for its legality of authorized standard.

Furthermore, if the firmware is upgraded online automatically, not only check the header and model name for its legality of authorized standard, the firmware will also be reviewed through RSA key.

4. Are there any verification protocols in place to ensure that the software/firmware is legitimate? If so, describe in details.

Description:

> Yes, as described in the response to item 3 above, the secure boot process ensures the software/firmware binary image was created by a trusted and authorized party.

5. Describe, if any, encryption methods used.

Description:

> The distributed software/firmware image is not encrypted. However, it is using the process described in item 3 above to check does it is authorized.

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:

> We refer to the same radio parameters setting with master mode in client mode. These settings are controlled by country code. This country code is fixed at time of manufacture and it follows the certification rule.

Third Party Access Control
1. How are unauthorized software/firmware changes prevented?

Description:

> Please refer to item 3 of General Description above.

2. 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:

> Please refer to item 3 of General Description above.

3. 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:

> Devices sold in the United States are fixed to U.S. specifications at time of manufacture. The firmware does not support changing regulatory domain. The software/firmware for U.S.-bound devices is tested to operate the radio within the limits set forth in the FCC's regulations.

4. What prevents third parties from loading non-US versions of the software/firmware on the device?

Description:

> Please refer to item 3 of General Description above.

5. For modular devices, describe how authentication is achieved when used with different hosts.

Description:

> This device is not a modular device.

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?[5]

Description:

> The UI is accessible to end users.

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

Description:

> This device is not a professionally installed device.

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

Description:

> This device is not a professionally installed device.

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

Description:

> This device is not a professionally installed device.

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

Description:

> Wireless Network Name (SSID), Network credentials, DHCP address ranges, DNS server addresses, and Wireless Statistics, Bandwidth, Channel are viewable to an end user.

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

Description:

> The configuration parameters do not affect the operation of the radio with respect to the certification.

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

Description:

> The configuration parameters do not affect the operation of the radio with respect to the certification.

d) Is the country code factory set? Can it be changed in the UI?

Description:

> For devices sold in the United States, the country code setting is assigned to U.S. at the factory. The country code 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:

> The country code cannot be changed in the UI. Devices sold in the United States are fixed to U.S. specifications at time of manufacture.

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

Description:

> For devices sold in the U.S., the country code is set to U.S. at the time of manufacture. The device will boot up with U.S. configuration.

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 can be configured in bridge mode and follow the U.S. certification. The device doesn't support to work at DFS band.

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?
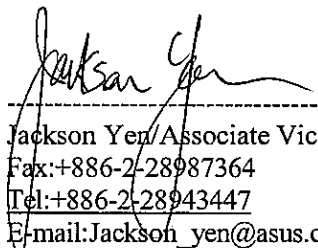
Description:

Yes, the radio setting is based on the same country code for both master and client mode.

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:

This device cannot be configured to use different types of antennas beyond those being tested for this certification.

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

Jackson Yen/Associate Vice President
Fax:+886-2-28987364
Tel:+886-2-28943447
E-mail:Jackson_yen@asus.com