FCC ID: XEK-MTRAYT8

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.

Not applicable. Software/ firmware update of the WIFI module is not available.

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 (e.g. RF power table, frequency channel table) is written in the FW and NVRAM. NVRAM is written in driver, only manufacture can modify it. FW is Binary, only Chipset Vender can update it. Therefore, when the authorized RF parameter is set by the WIFI module's manufacturer, no one can change 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 FW is compiled in binary code, only Chipset vender can provide the FW which contains the authorized setting. The chipset will detect and verify the FW internally. Using wrong FW won't make the module / device working. Neither the module maker nor the manufacture can modify the FW.

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

In order to change the FW of the product, the updated FW must match the check-sum for the Driver and Device ID (MAC address). Since only manufacture will know the check-sum, no one can write illegitimate FW into the device.

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?

Not applicable. This device is a client 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.

Not applicable. There is no means for third parties to change the setting.

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 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.

Not applicable. There is no means for third parties to install software/ firmware.

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.

Not applicable. This device is not certified as module.

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.

a. What parameters are viewable and configurable by different parties?
None. It is not an AP.

b. What parameters are accessible or modifiable by the professional installer or system integrators?
None

(1) Are the parameters in some way limited, so that the installers will not enter parameters that exceed those authorized?
Not applicable

(2) What controls exist that the user cannot operate the device outside its authorization in the U.S.?
Not applicable

c. What parameters are accessible or modifiable by the end-user?
None. It is not an AP.

(1) Are the parameters in some way limited, so that the user or installers will not enter parameters that exceed those authorized?
Not applicable

(2) What controls exist so that the user cannot operate the device outside its authorization in the U.S.?
Not applicable

d. Is the country code factory set? Can it be changed in the UI?
None. It is not an AP.

(1) If it can be changed, what controls exist to ensure that the device can only operate within its authorization in the U.S.?
Not applicable

e. What are the default parameters when the device is restarted?
The default parameter will be same as those approved factory pre-set parameter.

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?
Not applicable. This device work as a client only.

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))
Not applicable. This device is a client device and cannot be operated as access point. The antenna is integral. User cannot change the antennas.

By signing this document, we declare that the information stated on this document is true and correct

Company name: Megabyte Limited
Name: Henry Ho
Title: CFO
Date: 4 Nov 2016