The information provided in this document applies to the following Wireless Adapter Modules.

Model FCC ID: URZ-PHRPAD60

Software Security Description – KDB 594280 D02v01r03 Section II

General Description

1. Describe how any software/firmware update will be obtained, downloaded, and installed. Software that is accessed through manufacturer's website or device's management system, must describe the different levels of security as appropriate.

Software and Firmware updates are not released to the public. Units can be updated only at the OEM or by a remote update procedure controlled by the OEM.

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, it will not exceed the authorized RF characteristics?

Parameters that control radio frequency output are stored in non-volatile memory by the manufacturer at time of manufacture. They will not exceed regulatory requirements.

3. Describe in detail the authentication protocols that are in place to ensure that the source of the RF related software/firmware is legitimate. Describe in detail how the software is protected against modification.

Only radio firmware obtained directly from the chip manufacturer is used in the OS. Software and Firmware is verified legitimate and installed during the manufacturing and testout process prior to shipment. Updates are not released to the public. Units can be updated only at the OEM or by remote update controlled by the OEM.

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

This is an application specific device where the software and Firmware is only installed by the OEM. Updates are not released to the public.

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?

Device is client only. There are no configuration options that allow for master mode.

Third-Party Access Control

1. 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 device's authorization if activated in the U.S.

Third parties do not have the capability to access or change radio parameters. Device is sold for US market only and can only be updated at the OEM or by remote update controlled by the OEM.

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.

Third party software and firmware installation is not permitted.

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 parameters are not modified outside the grant of authorization.

Not a modular certified device.

SOFTWARE CONFIGURATION DESCRIPTION – KDB 594280 D02v01r03 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.

There are two levels of configuration, end users and Installers. End users have no access to Wireless control settings. Installers have access to WiFi network setup configuration.

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

Users have no access to Wireless control settings. There is a connection status symbol on the screen.

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

Installer configuration has WiFi network connection setup including network selection by SSID and band of operation, encryption type and password as shown in configuration guide.

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

Yes parameters are limited to Wifi network settings that do not effect authorized operation.

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

No options exist to change parameters that would allow operation outside of US authorization.

c) What parameters are accessible or modifiable by the end-user?

None – End user has no access to wireless parameters and control settings.

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

Yes parameters are limited to Wifi network settings that do not effect authorized operation.

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

No options exist to change parameters that would allow operation outside of US authorization.

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

The country code is factory set and cannot be changed from 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.?

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

RF parameters are stored in non-volatile memory. At startup parameters are restored and operation is resumed with previously configured WiFi connection.

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 – These modes are not supported.

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?

Master mode is not supported. There are no options that allow for changing master/client modes.

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))

These features are not supported.