Non-SDR (Software Defined Radio) Cover Letter

Date: October 30, 2017

Refer to KDB 442812 D01 SDR apps Guide v02r03.

The following six questions can be used for determining if a radio can elect to be, or must be an SDR.

1. Can the RF parameters of the device be altered through software?

Yes - go to 2.

No, not an SDR

Yes

2. Can third parties not permitted by the Commission through specific filings modify, configure, or load different software, or make configuration settings to operate the device or host hardware radio frequency parameters (frequency range, modulation type, maximum output power or other radio parameters) in any other way than granted (or expected to be granted)?

Yes, must be an SDR.

No - go to 3.

No

3. Is the device capable of operating in any other in any other way than granted, or will be, granted?

Yes, - go to 4.

No - go to 5.

No

4. Is this a Part 15 client Device as defined in Section 15.202 (as opposed to a master device)?

Yes, qualifies as a part 15 client devices - go to 5.

No, must be an SDR.

5. Does the manufacturer elect SDR?

Yes, elects to be an SDR.

No, Not an SDR

No

Final conclusion:

According to the above questions reply, we can confirm this AC1900 **Wireless Dual Band Gigabit Router** must be a Non-SDR.

Software Security Requirements Cover Letter

Refer to KDB 594280 D02 U-NII Device Security v01r03.

The applicant has response some questions as below, which can clearly demonstrate how the device meets the security requirements

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
	Response: New firmware versions are posted at http://www.tp-link.com and can be downloaded for free. To install the new firmware, choose "Advanced → System Tools → Firmware Upgrade" and then follow the tips in the webpage.
	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?
	Response: For devices sold in the United States, the programmed frequencies are: Radio 2.4 GHz: 2.412GHz ~ 2.462GHz. Radio 5 GHz: 5.180GHz ~ 5.240GHz, 5.745GHz ~ 5.825GHz. The Radio range is fixed by our software/firmware, and can't be configured out of the giving range.
	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
	Response: The country code and original firmware is put in device's flash and could only be installed by the factory. Other RF parameters including frequency operation and power settings is compiled in firmware. Digital sign is used to protect the firmware against modification.
	4. Describe in detail any encryption methods used to support the use of legitimate RF-related software/firmware.

	Response: The firmware is compiled as binary file, and it has a digital sign in it. Only verified firmware can be upgraded. This prevent change the RF parameter through this binary file.
	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?
	Response: There are no differences between the master and client mode in our device for the RF mode, channel, and power. If the mast mode is compliance for the certification , so is the client mode.
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.
	Response: The firmware does not support changing regulatory domain. Devices sold in the United States are fixed to U.S. specifications at time of manufacture. The software/firmware for U.S.-bound devices is tested to operate the radio within the limits set forth in the FCC's regulations.
	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
	Response: The device not permits the use of software/firmware created by third parties. The country code is fixed to the US at the time of manufacture.
	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.
	Response: This device is not a modular device.

Software Configuration Description	
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.
	Response: SSID, Security Type, Encryption Type, Security Key, IP Address.Different levels of access are not permitted.
	a) What parameters are viewable and configurable by different parties?
	Response: SSID, Security Type, Encryption Type, Security Key, IP Address.
	b) What parameters are accessible or modifiable by the professional installer or system integrators?
	Response: This device is not a professionally installed device.
	1) Are the parameters in some way limited, so that the installers will not enter parameters that exceed those authorized?
	Response: This device is not a professionally installed device.
	2) What controls exist that the user cannot operate the device outside its authorization in the U.S.?
	Response: This device is not a professionally installed device.
	c) What parameters are accessible or modifiable by the end-user?
	Response: Wireless Mode, SSID, Security Type, Encryption Type, Security Key, IP Address.
	1) Are the parameters in some way limited, so that the user or installers will not enter parameters that exceed those authorized?
	Response: Yes, the parameters are in some way limited.
	2) What controls exist so that the user cannot operate the device outside its authorization in the U.S.?

	Response: The firmware is compiled as binary file and cannot change the RF parameter through this binary file.It is read-only without the change to change the setting.
	d) Is the country code factory set? Can it be changed in the UI?
	Response: For devices sold in the United States, the country code setting is assigned to U.S. in the factory at the time of manufacture. The country code 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.?
	Response: The country code cannot be changed in the UI.
	e) What are the default parameters when the device is restarted?
	Response: Transmit Power, Bandwidth Mode, Radio Mode, Channel.
	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.
	Response: The radio cannot currently be configured in bridge or mesh mode.
	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?
	Response: User can configure the device to master only mode, and master + client mode. Only the running mode can be configure within the UI. The RF parameters of each mode are preset in the firmware, and the preset parameters are compliance. No. User cannot configure the running mode in each band,and all allowable modes are tested and shows compliance.
	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))
	Response:

	This device cannot be configured as different types of access points. This device also does not support external antennas configuration. Hence, the device cannot be configured to use different types of antennas beyond those that are shipped with the device and tested for this certification.