< TP-Link Technologies Co., Ltd.>
<Building 24 (floors 1,3,4,5) and 28 (floors1-4), Central Science and Technology Park,Nanshan Shenzhen, 518057 China>

Operation Description

SOFTWARE SECURITY REQUIREMENTS FOR U-NII DEVICES

Federal Communication Commission

Equipment Authorization Division, Application Processing Branch

7435 Oakland Mills Road

Columbia, MD21048

Date: <2019-10-18>

Attn: Office of Engineering and Technology

Subject: Attestation Letter regarding UNII devices

FCC ID: TE7CPE510V32

Software security questions and answers per KDB 594280 D02:

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.	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?	Radio 5G: 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.	No, the RF parameters are put in the read-only partition of device's flash and could only be installed by the factory. RF parameters: frequency operation, power settings and country code.
	4. Describe in detail any encryption methods used to support the use of legitimate RF-related software/firmware.	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 setting.

	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?	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.The device cannot be configured as a master and client simultaneously.
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.	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.	The secure booting process prevents the use of software/firmware created by third parties. The locale is fixed to the U.S. 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.	This device is not a modular device.

SOFTWARE CONFIGURATION DESCRIPTION GUIDE

For devices which have "User Interfaces" (UI) to configure the device in a manner that may impact the operational RF parameters, the following questions shall be answered by the applicant and the information included in the operational description. The description must address if the device supports any of the country code configurations or peer-peer mode communications discussed in KDB 594280 Publication D01.

< TP-Link Technologies Co., Ltd.>
<Building 24 (floors 1,3,4,5) and 28 (floors1-4), Central Science and Technology Park,Nanshan Shenzhen, 518057 China>

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.	SSID, Security Type, Encryption Type, Security Key, IP Address.Different levels of access are notpermitted.
	a. What parameters are viewable and configurable by different parties?	SSID, Security Type, Encryption Type, Security Key, IP Address.
	b. What parameters are accessible or modifiable by the professional installer or system integrators?	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?	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.?	This device is not a professionally installed device.
	c. What parameters are accessible or modifiable by the end-user?	Wireless Mode, Channel-Width, Channel, Transmit Power, 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?	Yes, the parameters are in some way limited.The firmware provides legal options and prompts the user to select among them.
	(2) What controls exist so that the user cannot operate the device outside its authorization in the U.S.?	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?	Yes,the factory setting is US. No, 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.?	The country code cannot be changed in the UI.
	e. What are the default parameters when the device is restarted?	Country code is US.

	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, the radio can't 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?	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.The device cannot be configured as a master and client simultaneously.
	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))	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.