< 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>

Federal Communication Commission
Equipment Authorization Division, Application Processing Branch
7435 Oakland Mills Road
Columbia, MD21048

Date: <2020-02-24>

Attn: Office of Engineering and Technology
Subject: Attestation Letter regarding UNII devices

FCC ID: TE7WA1201V2
IC ID: 8853A-WA1201V2

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.	The RF parameters are put in the read-only partition of device's flash and could only be installed by the factory. The software 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.
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 frequency parameters are limited by US regulatory domain and country code to limit frequency and transmit power levels. These limits are stored in non-volatile memory by the module manufacturer at the time of production. They will not exceed the authorized values.
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 firmware is installed on each single module during manufacturing process. The correct firmware is verified and installed by the module manufacturer. In addition, the firmware binary is encrypted using open SSL encryption and the firmware updates can only be stored in

		non-volatile memory when the firmware is authenticated. The encryption key is known by the module manufacturer only.
4	Describe in detail any encryption methods used to support the use of legitimate RF-related software/firmware.	The firmware binary is encrypted. The process to flash anew firmware is using a secret key to decrypt the firmware; only correct decrypted firmware is stored in non-volatile memory (see #3).
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?	The device ensures the compliance by checking the configured parameter and operation values according to the regulatory domain and country code in each band.
Software Security description – Third-Party Access Control		
1	Explain if any third parties have thecapability to operate a US sold device onany other regulatory domain, frequencies,or in any manner that is in violation of thecertification.	No, third parties don’t have the capability to access and change radio parameters. US sold modules are factory configured to US.
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 thedevice 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 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.
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	The module is not available for sale or installation outside of company licensing agreements. Modules are always installed in host systems in a factory by end integrators (OEM) responsible for loading authorized software.

	modified outside the grant of authorization.	
Software Security description – USER CONFIGURATION GUID		
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.	Authorized channel, bandwidth, and modulation can be configured through the UI.
	a. What parameters are viewable and configurable by different parties?	Various device status information is made available like log information, connection status, operation mode, operation frequency, etc. Radio parameters are described in c.i
	b. What parameters are accessible or modifiable tothe professional installer? i. Are the parameters in some way limited, so thatthe installers will not enter parameters thatexceed those authorized? ii. What controls exist that the user cannot operatethe device outside its authorization in the U.S.?	This device is not subject to professional installation
	c. What configuration options are available to theend-user? i. Are the parameters in some way limited, so thatthe installers will not enter parameters thatexceed those authorized? ii. What controls exist that the user cannot operatethe device outside its authorization in the U.S.?	The end user is able to configure the operation frequency, modulation, reduce the output power levels etc. The end user cannot change the antenna gain and country code, those settings are programmed at factory production time. Yes, the parameters can only be changed within the limits of country code US. The country code and regulatory domain control do limit all the parameters set by UI
	d. Is the country code factory set? Can it bechanged in the UI?	The country code is factory set and is never changed by UI. The country code is factory set and

	i. If so, what controls exist to ensure that thedevice can only operate within its authorizationin the U.S.?	is never changed by UI
	e. What are the default parameters when thedevice is restarted?	RF parameters including frequency operation, power settings and country code are the default factory settings when the device is restarted.
2	Can the radio be configured in bridge or meshmode? If yes, an attestation may be required.Further information is available in KDBPublication 905462 D02.	Not supported.
3	For a device that can be configured as a masterand client (with active or passive scanning), ifthis is user configurable, describe what controlsexist, within the UI, to ensure compliance foreach mode. If the device acts as a master insome bands and client in others, how is thisconfigured to ensure compliance?	No end user controls or user interface operation to change master/client operation.
4	For a device that can be configured as differenttypes of access points, such as point-to-point orpoint-to-multipoint, and use different types ofantennas, describe what controls exist to ensurecompliance with applicable limits and the properantenna is used for each mode of operation.See Section 15.407(a).	The device does not support these modes/features.