**<TP-LINK CORPORATION PTE.LTD.>**
< 7 Temasek Boulevard #29-03 Suntec Tower One, Singapore 038987 >

# 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: <2025-01-21>

Attn: Office of Engineering and Technology

Subject: Attestation Letter regarding UNII devices

FCC ID: 2BCGWER706W4G

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. | Software/Driver will be obtained by the factory, downloaded from the ODM website, and installed by the end user. Software is accessed through windows device management when computer is connected. |
| | 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 parameters cannot be modified by software/driver. The RF parameters will be written into e-fuse, e-fuse needs to be opened with special production tools, which will not be provided to end users. |
| | 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 any authentication protocol is used. The RF Parameters is put in read-only partition of EUT's e-fuse and are only inside in main IC chip. RF parameters including frequency of operation, power setting, modulation type, antenna types or country code setting will be locked in this partition. |
| | 4. Describe in detail any encryption methods used to support the use of legitimate RF-related software/firmware. | No encryption methods used. |

| | | |
|---|---|---|
| | 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? | This device cannot be configured as a slave. |
| **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. | No any third parties have the capability to operate a US 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. |
| | 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 RF parameters cannot be modified by software/driver. The RF parameters will be written into e-fuse, e-fuse needs to be opened with special production tools, which will not be provided to end users or other third-party software or firmware installation. |
| | 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 is not a module 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.

| SOFTWARE CONFIGURATION DESCRIPTION | | |
|---|---|---|
| **USER** | 1. Describe the user configurations permitted | There is no web ui for the device. |

**<TP-LINK CORPORATION PTE.LTD.>**
**< 7 Temasek Boulevard #29-03 Suntec Tower One, Singapore 038987 >**

| | | |
|---|---|---|
| **CONFIGURATION GUIDE** | 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 will follow master device. |
| | a. What parameters are viewable and configurable by different parties? | There is no web ui for the device. Parameters can not be viewable. |
| | b. What parameters are accessible or modifiable by the professional installer or system integrators? | This is not professional install device. |
| | (1) Are the parameters in some way limited, so that the installers will not enter parameters that exceed those authorized? | This is not professional install device. |
| | (2) What controls exist that the user cannot operate the device outside its authorization in the U.S.? | The RF parameters cannot be modified by software/driver. The RF parameters will be written into e-fuse, e-fuse needs to be opened with special production tools, which will not be provided to end users or other third-party software or firmware installation. |
| | c. What parameters are accessible or modifiable by the end-user? | The end user is able to select ssid and input password. The end user cannot change the antenna gain and country code, those settings are programmed at factory production time. |
| | (1) Are the parameters in some way limited, so that the user or installers will not enter parameters that exceed those authorized? | This is not professional install device. |
| | (2) What controls exist so that the user cannot operate the device outside its authorization in the U.S.? | The RF parameters cannot be modified by software/driver. The RF parameters will be written into e-fuse, e-fuse needs to be opened with special production tools, which will not be provided to end users or other third-party software or firmware installation. |
| | d. Is the country code factory set? Can it be changed in the UI? | Yes, the country code is set by factory. It 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? | Factory setting. |
|  | 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. | 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? | This device cannot be configured as a slave. |
|  | 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 can only configured as an access points with point-to-multipoint. |

Name: Sarah Wang *Sarah Wang*

Position: Regulatory Compliance Manager

Company Name:TP-LINK CORPORATION

PTE.LTD.