**< SHENZHEN TENDA TECHNOLOGY CO.,LTD. >**
**<6-8 Floor, Tower E3, No. 1001, Zhongshanyuan Road, Nanshan District, Shenzhen, China. 518052>**

Federal Communication Commission
Equipment Authorization Division, Application Processing Branch
7435 Oakland Mills Road
Columbia, MD 21048

Date: <2021-12-23>

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

FCC ID: V7TMESH3V3

Software security questions and answers per KDB 594280 D02:

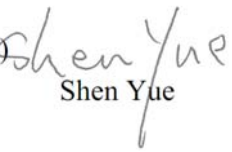
| Software Security description – General Description | | |
|---|---|---|
| 1 | Describe how any software/firmware updates for elements than can affect the device's RF parameters will be obtained, downloaded, validated and installed. For software that is accessed through manufacturer's website or device's management system, describe the different levels of security as appropriate. | Software/firmware will be obtained by the factory, downloaded from the ODM website, and installed by the end user.<br>Software is accessed through Web UI 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.<br>All these parameters will not exceed the authorized parameters. The firmware has been complied as binary file. It couldn't change the setting RF parameter through this binary file. It is read-only without change. |
| 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 flash and are only installed in the factory. 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), | This device cannot be configured as a master and client. |

| | | |
|---|---|---|
| | 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? | |
| Software Security description – 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 certification. | 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 is put in read-only partition of EUT's flash and are only installed in the factory. RF parameters including frequency of operation, power setting, modulation type, antenna types or country code setting will be locked in this partition. |
| 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 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.<br>There are no different levels of access. |
| | a. What parameters are viewable and configurable by different parties? | Authorized channel, bandwidth, and modulation. |
| | b. What parameters are accessible or modifiable to the professional installer?<br>i. Are the parameters in some way | This is not professional install device.<br>This is not professional install device. |

| | | |
|---|---|---|
| | limited, so that the installers will not enter parameters that exceed those authorized?<br>ii. What controls exist that the user cannot operate the device outside its authorization in the U.S.? | The RF Parameters is put in read-only partition of EUT's flash and are only installed in the factory. RF parameters including frequency of operation, power setting, modulation type, antenna types or country code setting will be locked in this partition. |
| | c. What configuration options are available to the end-user?<br>i. Are the parameters in some way limited, so that the installers will not enter parameters that exceed those authorized?<br>ii. What controls exist that the user cannot operate the device outside its authorization in the U.S.? | Authorized channel, bandwidth, and modulation.<br><br>This is not professional install device.<br><br>The RF Parameters is put in read-only partition of EUT's flash and are only installed in the factory. RF parameters including frequency of operation, power setting, modulation type, antenna types or country code setting will be locked in this partition. |
| | d. Is the country code factory set? Can it be changed in the UI?<br>i. If so, what controls exist to ensure that the device can only operate within its authorization in the U.S.? | Yes, the country code is set by factory. It cannot be changed in the UI.<br><br>The country code cannot be changed in the UI. |
| | e. What are the default parameters when the device is restarted? | The default RF parameters include frequency of operation, power setting, modulation type, country code(U.S.). For operation in the U.S, the default parameters of the device cannot be modified to operate outside its authorization. |
| 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, this device cannot be configured in both bridge and 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 | This device cannot be configured as a master and client. |

| | | |
|---|---|---|
| | bands and client in others, how is this configured to ensure 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). | This device cannot be configured as different types of access points. |

Sincerely

(Signed) 
Name: Shen Yue

Company: SHENZHEN TENDA TECHNOLOGY CO.,LTD

Address: 6-8 Floor, Tower E3, No. 1001, Zhongshanyuan Road, Nanshan District, Shenzhen, China. 518052
Phone: 86-755-27657098
Fax: 866-755-27657178
E-Mail: cert@tenda.cn