Federal Communications Commission 2022-06-30
Oakland Mills Road
Columbia MD 21046

FCC ID: 2ASJLAP6398S2

Subject: Statement for 5G Wi-Fi TM
The information within this section of the Operational Description is to show compliance against the Software Security Requirements laid out within KDB 594280 D02 U-NII Device Security v01r03.
The information below describes how we maintain the overall security measures and systems so that only:
1. Authenticated software is loaded and operating on the device
2. The device is not easily modified to operate with RF parameters outside of the authorization

Software Security Description – KDB 594280 D02v01r03 Section II	
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 user or installer cannot modify the software/firmware content. FW version will only be deployed over the air. There are two main scenarios for this (1) When the user associates the device to their account, the platform pushes a new firmware version if available. (2) The cloud platform can push a new firmware version to the device when it is available
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?	WiFi channel area code ID is only set in factory, all RF parameters (include Frequency range, transmitter output power etc.) cannot be access by the user. NVRAM can not be modified by the user.
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.	Firmware itself has a private checksum value and MD5 value inside. If firmware is modified, then its checksum and MD5 value cannot be verified, and then it cannot be allowed to be upgraded. Firmware is also pushed as an AES encrypted file, where the AES key is shared with the device via a separate channel.
4. Describe in detail any encryption methods used to support the use of legitimate RF-related software/firmware.	Firmware itself has a private checksum value and MD5 value inside. If firmware is modified, then its checksum and MD5 value cannot be verified, and then it cannot be allowed to be upgraded. SSL / AES / Base64

6. 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?	Our device has two radios, one for 2.4G band and another for 5G band. When client mode is enabled, the working band also must be selected, and the master mode working on that band will be disabled automatically. When each mode is selected, the wireless driver will be configured with specific settings for selected mode to let it work in that 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.	There is checksum information in firmware upgrade bin file and flash ROM.
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.	It is impossible to load device drivers.
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.	No,it didn't have API or interface for third-party.

SOFTWARE CONFIGURATION DESCRIPTION	
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.	No configurations permitted for any party
a) What parameters are viewable and configurable by different parties?	No parameters are viewable.
b) What parameters are accessible or modifiable by the professional installer or system integrators?	No parameters are accessible.

i) Are the parameters in some way limited, so that the installers will not enter parameters that exceed those authorized?	End user cannot access to the parameters
ii) What controls exist that the user cannot operate the device outside its authorization in the U.S.?	Firmware does not provide any interface to user to operate outside its authorization
c) What parameters are accessible or modifiable by the end-user?	End-user have not configuration options
i) Are the parameters in some way limited, so that the user or installers will not enter parameters that exceed those authorized?	Yes
ii) What controls exist so that the user cannot operate the device outside its authorization in the U.S.?	Default mode is always FCC compliant.
d) Is the country code factory set? Can it be changed in the UI?	Yes, No
i) If it can be changed, what controls exist to ensure that the device can only operate within its authorization in the U.S.?	cannot change
e) What are the default parameters when the device is restarted?	Same as factory set
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
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 is a client device with passive scanning, End user cannot configured
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))	End user cannot configured

Company Officer: Chloe Peng Chloe Peng

Telephone Number: 86-755-83230448

Email: chloe.peng@robotemi.com