Operation Description

SOFTWARE SECURITY REQUIREMENTS FOR U-NII DEVICES

FCC ID:2AAGE5081SB4898W

Pursuant to KDB 594280 D02, the overall security measures and systems that ensure that:

1. Only properly authenticated software is loaded and operating the device; and
2. The device is not easily modified to operate with RF parameters outside of the authorization.

are described.

The following questions are addressed the description of the software in the operational description for the device and clearly how the device meets the security requirements.

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.	Re: Customers can obtain software/firmware from the RF module vendor website. Software/firmware is a compiled binary file and cannot modify any parameters. The software can be only updated and installed manually.
	2. Describethe 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?	Re: Radio frequency parameters are limited by regulatory domain and transmit power levels. These limits are stored in non-volatile memory by the manufacture 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.	Re: The firmware is installed on each product during the manufacturing process. The correct firmware is verified and installed by the manufacturer. In addition, the firmware updates can only be stored in non-volatile memory when the firmware is authenticated. This prevents modification of RF-related software as well as installation of unauthorized firmware.
	4. Describe in detail any encryption methods used to support the use of legitimate RF-related software/firmware.	Re: No encryption methods used.
	5. For a device that can be configured as a master and client (with active or passive	Re: The default mode is client mode. And it can be configured as the master mode by system

	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?	settings.In both master or client mode, RF parameters are limited by both the regulatory domain and the transmit power level. These restrictions are stored by the manufacturer in non-volatile memory at the time of production. They do not exceed the authorization value.
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.	Re: No third parties have the capability to operate this device on any 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 United States.
	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.	Re: The device's underlying RF parameters are stored in non-volatile memory through system updates. These storage spaces cannot be accessed and changed by third-party software, which prevents third-party software from modifying RF-related parameters and installing unauthorized firmware.
	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.	Re: The driver is installed on each product during the manufacturing process. The correct driver is verified and installed by the manufacturer. It's not modified outside the grant of authorization.

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 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.	Re: User configurations allowed by system commands are limited to basic WLAN configurations and security settings (SSID, encryption, password phrases). There is no access level difference for professional installers,

		system integrators or end-users.
	a. What parameters are viewable and configurable by different parties?	Re: For the end user, they are only permitted to select modulation mode (like 802.11 a/b/g/n and etc.) and channel.
	b. What parameters are accessible or modifiable by the professional installer or system integrators?	Re: For professional installer, they are only permitted to select modulation mode (like 802.11 a/b/g/n and etc.) and channel, the drivers were released by the module Vendors. They will not be able to change the parameters of the RF modules.
	(1) Are the parameters in some way limited, so that the installers will not enter parameters that exceed those authorized?	Re: Yes. They will not be able to change the parameters of the RF modules.
	(2) What controls exist that the user cannot operate the device outside its authorization in the U.S.?	Re: The drivers of the module was built in binary code by the vendor and the end user has no way to access or modify the driver except the opened limited settings.
	c. What parameters are accessible or modifiable by the end-user?	Re: For the end user, they only are permitted to select modulation mode (like 802.11 a/b/g/n and etc.) and channel.
	(1) Are the parameters in some way limited, so that the user or installers will not enter parameters that exceed those authorized?	Re: Yes, the parameters are in some way limited.
	(2) What controls exist so that the user cannot operate the device outside its authorization in the U.S.?	Re: End user have no way to make the device operate outside its authorization in the U.S. for the frequency band is limited by the firmware.
	d. Is the country code factory set? Can it be changed in the UI?	Re: Yes, the country code factory has been set up. It can't be changed in 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.?	Re: It can be changed in terminal commands for U.S.
	e. What are the default parameters when the device is restarted?	Re: The previously used settings will be loaded. Only authorized default parameters will be used when the device is restarted.
	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.	Re: Radio can operate in bridge mode. It shares an IP with Ethernet via bridge in master 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?	Re: For the end user, they only permit to select modulation mode (like 802.11 a/b/g/n and etc.) and channel whatever the device is active or passive scanning. The compliance status was tested during the certification.
	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))	Re: There is no change to the antenna, for each mode of operation, the device work in a compliance status since the authorized parameters will not be modified during the operation mode change.

Xi Wang

Signature

2022-03-16

Date

Printed Name of Signee: Xi Wang

Company: Chengdu Vantron Technology Co., Ltd.

Address:No.5 GaoPeng Road, Hi-Tech Zone, Chengdu, SiChuan, P.R. China 610045

Phone: 86-28-8512-3930 Fax:86-28-8512-3935

Email:x.wang@vantrontech.com.cn