REXING INC.

34 Ludwig St,Little Ferry, NJ, 07643 USA.

(08.27, 2025)

Federal Communications Commission
Authorization and Evaluation Division
7435 Oakland Mills Road
Columbia, MD 21046

Subject: **SOFTWARE SECURITY REQUIREMENTS FOR U-NII DEVICES for:**

FCC ID: 2AW5W-C2

SOFTWARE SECURITY REQUIREMENTS FOR U-NII DEVICES REF KDB 594280 D02 U-NII Device Security v01r03		
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.	End-user can not update the software/firmware
	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 nay other software/firmware changes will not allow the device to exceed the authorized RF characteristics?	All the radio frequency parameters are not modified by any software/firmware without any hardware changes, because the software/firmware can not changes the radio frequency parameters.
	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.	Software/firmware are digitally signed and encrypted using proprietary handshaking, authorization and provisioning protocols. Secure Sockets Layer is used protocol for encrypting information over the internet. Therefore, can ensure that the source of the software/firmware is legitimate.
	4. Describe in detail any encryption methods used to support the use of legitimate RF-related software/firmware.	RSA algorithm is used to sign and encrypt the software/firmware using a private key
	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 module can be configured as a client only. Verifies each mode to ensure the module for compliance in the FCC band range.

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.	The modules firmware is stored in the ROM, third parties could not access the system image because they have no private key to do this. Under this pre-condition, A third party cannot change radio parameters. different country has different mechanism (likeness country code). It can control the module’s parameter, such as Channel, Power, Bandwidth and etc. when sale to US/Canada, decided to device only have US/Canada mechanism (not certified frequencies are blocked). Out of US/Canada mechanism, the parameter (Channel, Power, Bandwidth and etc.) is un allow able. So, it cannot have capability to operate the device.
	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 device does not support third-party software or firmware installation
	3. For Certified Transmitter modular devices, describe how the module grantee ensures that hosts manufactures 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 parameters are not modified outside the grant of authorization.	The regulatory domain and frequencies are factory set. We do not provide the interface for third parties.
User Configuration	1. Describe the user configurations permitted through the UI. If different levels of access are permitted for professional installers, system	The UI is accessible to the end user by App Control, but the UI never gives access for specific operation parameters which are Channel, Power, Bandwidth,

Guide User Configuration Guide *(Continue)*	integrators or end-users, describe the differences.	or Country code settings
	a) What parameters are viewable and configurable by different parties?	regulatory domain
	b) What parameters are accessible or modifiable by the professional installer or system integrators?	Does not provide
	(1) Are the parameters in some way limited, so that the installers will not enter parameters that exceed those authorized?	The regulatory domain, band and frequencies are factory set and can not be changed.
	(2) What controls exist that the user cannot operate the device outside its authorization in the U.S.?	Only supports the channels specified by U.S.
	c) What parameters are accessible or modifiable to by the end-user?	Does not provide
	(1) Are the parameters in some way limited, so that the user or installers will not enter parameters that exceed those authorized?	The regulatory domain, band and frequencies are factory set and can not be changed.
	(2) What controls exist that the user cannot operate the device outside its authorization in the U.S.?	Only supports the channels specified by U.S.
	d) Is the country code factory set? Can it be changed in the UI?	factory set and can not 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.?	Can not be changed
	e) What are the default parameters when the device is restarted?	regulatory domain, band and frequencies
	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 support bridge 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?	No support bridge mode
	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	In any mode, using the same antenna, and factory configuration does not allow replacement

REXING INC.

34 Ludwig St,Little Ferry, NJ, 07643 USA.

	Section 15.407(a))	

Sincerely, Yuhe Sun

(Signature)

Title:Manager

Address:34 Ludwig St,Little Ferry, NJ, 07643 USA.

Tel.:2032144881

Company Name:REXING INC.