SOFTWARE SECURITY FOR U-NII DEVICES

FCC ID: 2AZR6-FRANBBAT10
IC Certification number: 27217-FRANBBAT10
Pursuant to FCC Part 15E 15.407(i) and KDB 594280 D02 U-NII Device Security v01r03 / IC RSS-247 issue 2 article 6.4(4).
applicant must describe the overall security measures and systems that ensure that only:
1. Authenticated software is loaded and operating the device.
2. The device is not easily modified to operate with RF parameters outside of the authorization
The description of the software must address the following questions in the operational description for the device and clearly demonstrate how the device meets the security requirements.

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.
	There is no downloadable software provided by the manufacturer that can modify critical radio transmitter parameters. All critical parameters are programmed in OTP memory at the factory and cannot be modified or overridden by third parties.
	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?
	There are no rf parameters that can be modified. All rf parameters are programmed in OTP memory at the factory and cannot be modified or overridden by third parties.
	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.
	The firmware is programmed at the factory and cannot be modified by third parties. The firmware is programmed at the factory and cannot be modified by third parties.
	4. Describe in detail any encryption methods used to support the use of legitimate RF-related software/firmware.
	The firmware is programmed at the factory and cannot be modified by third parties therefore no encryption is necessary.
	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 is a client module only.

3rd 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.
	Third parties do not the capability to operate in any manner that is violation of the certification 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.
	RF parameters are programmed into OTP memory at the factory and cannot be reprogrammed or re-flashed by third parties.
	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.
	There are no rf parameters that can be modified. All rf parameters are programmed in OTP memory at the factory and cannot be modified or overridden by third parties. The module is not controlled by driver software on the host and cannot override critical rf parameters stored in module OTP memory.

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.
	No UI provided.
	a) What parameters are viewable and configurable by different parties?
	None
	b) What parameters are accessible or modifiable by the professional installer or system integrators?
	None
	(1) Are the parameters in some way limited, so that the installers will not enter parameters that exceed those authorized?
	The module micro-code reads the parameters from the module OTP memory. These parameters cannot be modified or overridden by sw drivers.
	(2) What controls exist that the user cannot operate the device outside its authorization in the U.S.?
	Default mode is always FCC compliant. Other country modes cannot be activated without receiving three independent country codes from different APs, otherwise remains in FCC default mode (always FCC compliant)

User Configuration guide	c) What parameters are accessible or modifiable to by the end-user?
	None
	(1) Are the parameters in some way limited, so that the user or installers will not enter parameters that exceed those authorized?
	The module micro-code reads the parameters from the module OTP memory. These parameters cannot be modified or overridden by sw drivers.
	(2) What controls exist that the user cannot operate the device outside its authorization in the U.S.?
	Default mode is always FCC compliant. Other country modes cannot be activated without receiving three independent country codes from different APs, otherwise remains in FCC default mode (always FCC compliant)
	d) Is the country code factory set? Can it be changed in the UI?
	Default country code is set in the factory and no UI is provided for modification.
	(1) If it can be changed, what controls exist to ensure that the device can only operate within its authorization in the U.S.?
	Programmed for default mode which is always FCC compliant. Always set for default for all start-ups, resets, timeouts or other host or network events.
	e) What are the default parameters when the device is restarted?
	Always FCC compliant
	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.
	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 is not an access point.

Name and surname of applicant (or authorized representative): Nirav Patel

Date: August 29, 2022 **Signature:**