Shenzhen Hollyland Technology Co.,Ltd

Declaration of Software Security Requirements Letter

Federal Communications Commission
Authorization and Evaluation Division
1435 Oakland Mills Road
Columbia, MD 21046

Date: 2022-6-7

SUBJECT: FCC UNII Software Security Description for FCC ID: 2ADZC-9802HR

To Whom It May Concern:

The information within this section of the Operational Description is to show compliance per the Software Security Requirements laid out within KDB 594280 D02 U-NII Devicee Security.

An applicant must describe the overall security measures implemented in the device that ensure that the device cannot be modified by any RF-related software changes by third parties to operate outside the authorized RF parameters without further approval from the FCC.

The following description of the RF-related software addresses the following questions in the operational description for the device and demonstrates how the device meets the RF-security requirements.

Software Security description – General Description		
	Question	**Answer**
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.	We do not release the firmware on our website for downloading. Our direct host manufacturer (OEM) can request the firmware from us and it will be made available upon request, not public accessible to end user.
	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?	Radio frequency parameters are limited by US regulatory domain and country code to limit frequency and transmit power levels. These limits are stored in non-volatile memory 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.	The firmware is installed on each single module during manufacturing process. The correct firmware is verified and installed by the manufacturer. In addition, the firmware binary is encrypted and the firmware updates can only be stored in non-volatile memory when the firmware is authenticated.
	4. Describe in detail any encryption methods used to support the use of legitimate RF-related software/firmware.	The firmware binary is encrypted. The process to flash a new firmware is using a secret key to decrypt the firmware, only correct decrypted firmware is stored in non-volatile memory .
	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?	There is a country code regulatory parameter to limit product to operate the device under its authorization in the U.S. This regulatory parameter would define which channel would be available to operate in active or passive scan to meet UNII requirements. The device would be set as a client device on all channels but also support access point mode on the non-DFS bands only.
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.	No, third parties don't have the capability to access and change radio parameters. US sold units are factory configured to US.
	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.	No. The device does not permit third-party software or firmware installation

	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.	Not Applicable. This device is not modular device.

In addition to the general security consideration, 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 Guide		
	Question	**Answer**
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.	There is not any UI to access setting.
	a. What parameters are viewable and configurable by different parties?	All default parameters are programmed or in both driver and firmware which would be embedded in system firmware. The system firmware is programmed and protected in flash memory. The professional installer/end-user cannot access the flash memory. End-use only could select which master (AP) to connect.
	b. What parameters are accessible or modifiable by the professional installer or system integrators?	There is not any parameter which is accessible or modifiable to the professional installer.
	(1) Are the parameters in some way limited, so that the installers will not enter parameters that exceed those authorized?	This device is not subject to professional installation
	(2) What controls exist that the user cannot operate the device outside its authorization in the U.S.?	This device is not subject to professional installation

	c. What parameters are accessible or modifiable by the end-user?	This device is not subject to professional installation The end user cannot change the antenna gain and country code, those settings are programmed at factory production time.
	(1) Are the parameters in some way limited, so that the user or installers will not enter parameters that exceed those authorized?	Yes. The system firmware is programmed and protected in flash memory. The professional installer/end-user cannot access the flash memory.
	(2) What controls exist so that the user cannot operate the device outside its authorization in the U.S.?	There is a country code regulatory parameter to limit product to operate the device outside its authorization in the U.S.
	d. Is the country code factory set? Can it be changed in the UI?	The country code is factory set and is never changed by 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.?	The country code is factory set and is never changed by UI
	e. What are the default parameters when the device is restarted?	At each boot up the country code and the antenna gain are read from the non-volatile memory, those values are configured during production
	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.	Not supported
	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. End-user cannot configure the device to be as a master or client.
	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))	The device does not support these modes/features

Sincerely,

Client's signature: Vincent Ma.

Client's name & title: Vincent Ma&Sales Director

Contact information / address: +86-755-86000682
vincent.ma@hollyland-tech.com

8F, Building 5D, Skyworth Innovation Valley, Tangtou Road. Shiyan Street, Baoan District Shenzhen, China.