Declaration of Software Security Requirements Letter

Date : 2024-01-30

Subject : SW Security Requirement for U-NII DEVICE per KDB 594280 D02

FCC ID : YCK-DR970XP

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 RFsecurity 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	Wifi driver and firmware are embedded in system firmware and there is not any installation process.
	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?	All default parameters approved by the FCC are programmed in both driver and firmware which would be embedded in system firmware. End-user cannot access them.
	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.	Wifi driver and firmware are embedded in system firmware and there is no any installation process. All default parameters are programmed in both driver and firmware which would be embedded in system firmware. End-user cannot access them.

	4. Describe in detail any encryption methods used to support the use of legitimate RF-related software/firmware.	The wifi device needs specific driver and firmware to operate; the driver and firmware would recognize some IDs to confirm if the chip is correct. The driver would read the country code regulatory parameter to limit product to operate the device under its authorization in the U.S.
	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 Master device on all supported channels.
	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.	Wifi driver and firmware are embedded in system firmware and there is not any installation process. System firmware is programmed and protected in flash memory with users are not able to modify the content.
	a. What parameters are viewable and configurable by different parties?	All default parameters are programmed 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 user could change SSID, password and the use of security in the master mode.
	b. What parameters are accessible or modifiable by the professional installer or system integrators?	No
	(1) Are the parameters in some way limited, so that the installers will not enter parameters that exceed those authorized?	Some parameters are programmed in wifi driver and firmware which are embedded in system firmware, installer cannot access them. The system firmware is programmed and protected in flash memory. The professional installer/end-user cannot access the flash memory
	(2) What controls exist that the user cannot operate the device outside its authorization in the U.S.?	There is a country code regulatory parameter to limit user to operate the device outside its authorization in the U.S
	c. What parameters are accessible or modifiable by the end-user?	End user could change SSID, password and the use of security in the master mode
	(1) Are the parameters in some way limited, so that the user or installers will not enter parameters that exceed those authorized?	Yes. Some parameters are programmed in wifi driver and firmware which are embedded in system firmware, installer cannot access them. 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?	Yes, country code is factory set, and 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.?	It cannot be changed by end-user.
	e. What are the default parameters when the device is restarted?	All default parameters are programmed 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.
	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.	Refer to the provided attestation document, operational methodology.
	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?	The device can be configured as a master and client. Changing between master and client can be done with the selection in the UI. And 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 master or client to meet UNII requirements.
	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 can be configured as a master and client. Changing between master and client can be done with the selection in the UI. And 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 master or client to meet UNII requirements

Name : MINHO SHIN
Position : Principal Research Engineer
Date : 2023-01-30