Software Security Requirements Cover Letter

Refer to KDB 594280 D02 U-NII Device Security v01r03.

The applicant has response some questions as below, which can clearly demonstrate 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
	Response: Software/firmware (including all RF parameters) will be obtained by the factory, downloaded from the ODM website, and installed by the end user. *For the software/firmware, end user can't change any important RF parameters except the operating channel, Bandwidth, operating mode.*
	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?
	Response: *The RF parameters cannot be modified by software. All these parameters will not exceed the authorized parameters. The firmware has been complied as binary file. It couldn't change the setting RF parameter through this binary file. It is read-only without change.*
	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
	Response: No such authentication protocols. The RF parameters are put in the read-only partition of device's flash and could only be installed by the factory. RF parameters: frequency operation, power settings and country code.

	4. Describe in detail any encryption methods used to support the use of legitimate RF-related software/firmware.
	Response: *No encryption methods used.*
	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?
	Response: *The device ensures the compliance by checking the configured parameter and operation values according to the regulatory domain and country code in each band.*
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.
	Response: *No any third parties have the capability to operate a US 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.*
	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
	Response: *The RF Parameters is put in read-only partition of EUT's flash and are only installed in the factory. RF parameters including frequency of operation, power setting, modulation type, antenna types or country code setting will be locked in this*

	partition.
	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.
	Response: This is not a module device
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.
	Response: *Authorized channel, bandwidth, and modulation can be configured through the UI.* *There are no different levels of access*
	a) What parameters are viewable and configurable by different parties?
	Response: *Authorized channel, bandwidth, and modulation.*
	b) What parameters are accessible or modifiable by the professional installer or system integrators?
	Response: This is not professional install device.
	1) Are the parameters in some way limited, so that the installers will not enter parameters that exceed those authorized?
	Response: This is not professional install device.
	2) What controls exist that the user cannot operate the device outside its authorization in the U.S.?
	Response: *The RF Parameters is put in read-only partition of EUT's flash and are only installed in the factory. RF parameters including frequency of operation, power setting, modulation type,*

	antenna types or country code setting will be locked in this partition.
	c) What parameters are accessible or modifiable by the end-user?
	Response: The end user is able to configure the operation frequency, modulation, reduce the output power levels etc. 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?
	Response: This is not professional install device.
	2) What controls exist so that the user cannot operate the device outside its authorization in the U.S.?
	Response: The RF Parameters is put in read-only partition of EUT's flash and are only installed in the factory. RF parameters including frequency of operation, power setting, modulation type, antenna types or country code setting will be locked in this partition.
	d) Is the country code factory set? Can it be changed in the UI?
	Response: Yes, the country code is set by factory. It cannot 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.?
	Response: The country code cannot be changed in the UI.
	e) What are the default parameters when the device is restarted?
	Response: Factory setting.
	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.
	Response: 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?
	Response: Response: *No end user controls or user interface operation to change master/client operation.*
	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))
	Response: *This device cannot be configured as different types of access points.*

Note: Product (FCC ID: 2AXJ4XE75) when it is sale in Canada also satisfy the software security requirement that shown above table. It has individual country code when sale Canada.

Sincerely,

Abby Liang

_____

Name: Abby Liang

Position: Regulatory Compliance Manager

Date: 2021-11-17