Operation Description

SOFTWARE SECURITY REQUIREMENTS FOR U-NII DEVICES

FCC ID: 2ADZRG240WB

Pursuant to KDB 594280 D02, the overall security measures and systems that ensure that only:

1. Authenticated software is loaded and operating the device; and
2. The device is not easily modified to operate with RF parameters outside of the authorization.

are described.

The following questions are addressed the description of the software in the operational description for the device and clearly how the device meets the security requirements.

SOFTWARE SECURITY DESCRIPTION		
General Description	1. Describe how any software/firmware update will be obtained, downloaded, and installed.	It will be obtained by the factory. It will be downloaded by ODM website. It will be installed by the end user.
	2. Describe all the radio frequency parameters that are modified by any software/firmware without any hardware changes. Are these parameters in some way limited, such that, it will not exceed the authorized parameters?	The RF parameters cannot be modified by software. The firmware has been complied as binary file. It couldn't change the setting of RF Parameters through this binary file. It is read-only without change.
	3. Are there any authentication protocols in place to ensure that the source of the software/firmware is legitimate? If so, describe in details; if not, explain how the software is secured from modification.	Yes. The RF Parameters is put in read-only partition of the product's flash and is only installed by the factory. RF Parameters will be locked in this partition.
	4. Are there any verification protocols in place to ensure that the software/ firmware is legitimate? If so, describe in details.	No.
	5. Describe, if any, encryption methods used.	No.
	6. 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	This device cannot be configured as a master and client.

	each band of operation?	
Third-Party Access Control	1. How are unauthorized software/ firmware changes prevented?	The RF parameters are Read-Only and are only installed by the factory.
	2. Is it possible for third parties to load device drivers that could modify the RF parameters, country of operation or other parameters which impact device compliance? If so, describe procedures to ensure that only approved drivers are loaded.	No, The RF parameters are put in read-only partition and are only installed by factory.
	3. Explain if any third parties have the capability to operate a US sold device on any other regulatory domain, frequencies, or in any manner that is in violation of the certification.	No. The RF parameters are put in read-only partition and are only installed by factory.
	4. What prevents third parties from loading non-US versions of the software/firmware on the device?	The RF parameters are put in read-only partition and are only installed by factory.
	5. For modular devices, describe how authentication is achieved when used with different hosts.	This is not a module device.

SOFTWARE CONFIGURATION DESCRIPTION GUIDE

For devices which have “User Interfaces” (UI) to configure the device in a manner that may impact the operational parameter, the following question is to 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		
USER CONFIGURATION GUIDE	1. To whom is the UI accessible? (Professional installer, end user, other.)	End user.
	a) What parameters are viewable to the professional installer/end-user?	Authorized channel.
	b) What parameters are accessible or modifiable to the professional installer?	This is not professional install device.
	i) Are the parameters in some way limited, so that the installers will not enter parameters that exceed those authorized?	This is not professional install device.

	ii) What controls exist that the user cannot operate the device outside its authorization in the U.S.?	This is not professional install device.
	c) What configuration options are available to the end-user?	Authorized channel.
	i) Are the parameters in some way limited, so that the installers will not enter parameters that exceed those authorized?	Yes.
	ii) What controls exist that the user cannot operate the device outside its authorization in the U.S.?	The RF parameters are put in read-only partition and are only installed by factory.
	d) Is the country code factory set? Can it be changed in the UI?	Yes. It cannot be changed in UI.
	i) If so, what controls exist to ensure that the device can only operate within its authorization in the U.S.?	RF Parameters (frequency of operation, power settings, antenna types. Or country code settings) is Read-Only and is obtained by the factory.
	e) What are the default parameters when the device is restarted?	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.	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 device cannot be configured as a master and 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))	This device cannot be configured as different types of access points.