

SOFTWARE SECURITY DESCRIPTION (KDB 594280 D02 V01r02)

FCC ID: 2AMM6-EWN8822CSE2AA

General Description

According to KDB 594280 D02 U-NII Device Security v01r01, software security questions and answers as below:

Q1	Describe how any software/firmware update will be obtained, downloaded, and installed. Software that is accessed through manufacturer's website or device's management system, must describe the different levels of security.
Ans	The software updates are given to customer via official website.
Q2	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?
Ans	All the parameter limitations are hard-coded into special permanent memory space to not exceed the authorized limits. Professional installer has no access to change radio parameter limits.
Q3	Describe in detail the authentication protocols that are in place to ensure that the source of the software/firmware is legitimate. Describe in detail how the software is protected against modification.
Ans	To protect software copywriting or modifications every device has a license which is bonded to a MAC address. Any software modification will end up with a voided license which in turn will prohibit further product usage.
Q4	Describe in detail the verification protocols in place to ensure that installed software/firmware is legitimate.
Ans	All manufactured product have unique MAC address, unique license and a special product limitation parameters
Q5	Describe in detail any encryption methods used to support the use of legitimate software/firmware.
Ans	"openssl_sign()" method is used to sign the software license.
Q6	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?
Ans	This device is a client device.

Third-Party Access Control

Q1	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.
Ans	It is impossible for the third party to develop a software manufactured devices.
Q2	What prevents third parties from loading non-US versions of the software/firmware on the device? Describe in detail how the device is protected from “flashing” and the installation of third-party firmware such as DD-WRT.
Ans	The product Radio Frequency (RF) calibration information is written in non-standard way, thus making impossible for the third party to develop a software manufactured devices.
Q3	For Certified Transmitter modular devices, describe how the module grantee ensures that hosts manufactures 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 parameters are not modified outside the grant of authorization.
Ans	This device is not a transmitter modular device.

SOFTWARE CONFIGURATION DESCRIPTION

Q1	To whom is the UI accessible? (Professional installer, end user, other.)	
Ans	Professional installer and end user.	
	a)	What parameters are viewable to the professional installer/end-user?
Ans		The software has access to below listed radio parameters: - Operating frequency - Channel width (e.g. 20MHz, 40MHz) - Modulation and coding rate - Spacial streams number - Transmit power - Guard interval between transmitted symbols
	b)	What parameters are accessible or modifiable by the professional installer?
Ans		The professional installer may change below listed parameters: - Operating frequency - Channel width (e.g. 20MHz, 40MHz) - Modulation and coding rate - Spacial streams number - Transmit power - Guard interval between transmitted symbols
	(1)	Are the parameters in some way limited, so that the installers will not enter parameters that exceed those authorized?
	Ans	Yes.
	(2)	What controls exist that the user cannot operate the device outside its authorization in the U.S.?
	Ans	Radio driver has special code part where allowed frequency, TXpower, EIRP, DFS values are defined. Those values are hardcoded, compiled and cannot be changed.
	c)	What parameters are accessible or modifiable to by the end-user?
Ans		The same as for professional installer.
	(1)	Are the parameters in some way limited, so that the installers will not enter parameters that exceed those authorized?
	Ans	Yes.
	(2)	What controls exist that the user cannot operate the device outside its authorization in the U.S.?
	Ans	Radio driver has special code part where allowed frequency, TXpower, EIRP, DFS values are defined. Those values are hardcoded, compiled and cannot be changed.
	d)	Is the country code factory set? Can it be changed in the UI?
Ans		US country code is hardcoded in the driver and cannot be changed any way for the user.
	(1)	If so, what controls exist to ensure that the device can only operate within its authorization in the U.S.?
	Ans	Radio driver has special code part where allowed frequency, TXpower, EIRP, DFS values are defined. Those values are hardcoded, compiled and cannot be changed.
	e)	What are the default parameters when the device is restarted?

	Ans	Reply: regulatory domain, band and frequencies
Q2	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	
Ans	Reply: No support bridge mode	
Q3	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?	
	Reply: The device acts as client	
Q4	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))	
	Reply: In any mode, using the same antenna, and factory configuration does not allow replacement.	