Software Security Description – KDB 594280 D02v01r02 Section II

General Description

1. 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.	There is no downloadable software provided by the manufacturer that can modify critical radio transmitter parameters. All critical parameters are programmed in OTP memory at the factory and cannot be modified or overridden by third parties.
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?	There are no rf parameters that can be modified. All rf parameters are programmed in OTP memory at the factory and cannot be modified or overridden by third parties.
3. 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.	The firmware is programmed at the factory and cannot be modified by third parties.
4. Describe in detail the verification protocols in place to ensure that installed software/firmware is legitimate.	The firmware is programmed at the factory and cannot be modified by third parties.
5. Describe in detail any encryption methods used to support the use of legitimate software/firmware.	The firmware is programmed at the factory and cannot be modified by third parties therefore no encryption is necessary.
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 each band of operation?	This is a client module only.

Third-Party Access Control

1. 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.	Third parties do not the capability to operate in any manner that is violation of the certification in the U.S.
2. 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. *(See, for example,* http://www.dd-	RF parameters are programmed into OTP memory at the factory and cannot be reprogrammed or re-flashed by third parties.

wrt.com/)	
3. 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.	There are no rf parameters that can be modified. All rf parameters are programmed in OTP memory at the factory and cannot be modified or overridden by third parties. The module is not controlled by driver software on the host and cannot override critical rf parameters stored in module OTP memory.

SOFTWARE CONFIGURATION DESCRIPTION – KDB 594280 D02v01r02 Section III

USER CONFIGURATION GUIDE

1. To whom is the UI accessible? (Professional installer, end user, other.)	No UI provided.
a) What parameters are viewable to the professional installer/end-user?	None
b) What parameters are accessible or modifiable to the professional installer?	None
i) Are the parameters in some way limited, so that the installers will not enter parameters that exceed those authorized?	The module micro-code reads the parameters from the module OTP memory. These parameters cannot be modified or overridden by sw drivers.
ii) What controls exist that the user cannot operate the device outside its authorization in the U.S.?	Default mode is always FCC compliant. Other country modes cannot be activated without receiving three independent country codes from different APs, otherwise remains in FCC default mode (always FCC compliant)
c) What configuration options are available to the end-user?	None
i) Are the parameters in some way limited, so that the installers will not enter parameters that exceed those authorized?	The module micro-code reads the parameters from the module OTP memory. These parameters cannot be modified or overridden by sw drivers.
ii) What controls exist that the user cannot operate the device outside its authorization in the U.S.?	Default mode is always FCC compliant. Other country modes cannot be activated without receiving three independent country codes from different APs, otherwise remains in FCC default mode (always FCC compliant)
d) Is the country code factory set? Can it be changed in the UI?	Default country code is set in the factory and no UI is provided for modification.
i) If so, what controls exist to ensure that the device can only operate within its authorization in the	Programmed for default mode which is always FCC compliant. Always set for default for all start-ups, resets, timeouts or other host or network events.

U.S.?	
e) What are the default parameters when the device is restarted?	Always FCC compliant
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 is a client device.
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 is not an access point.

Name and surname of applicant (or authorized representative):

Date: March 1, 2020 **Signature:**