July 24, 2014

Federal Communications Commission

7435 Oakland Mills Road

Columbia MD 21046

Subject: Attestation letter regarding client device without DFS

FCC ID: A3LSMG7508Q

The operation of this device as a Group owner for WiFi-Direct or TDLS in the U-NII bands is limited; it is permitted only where it is communicating with a device approved as a master according to the requirements of Section 15.202. This device does not support Wi-Fi "Hotpot" mode in DFS bands.

Software and associated drivers on this device will not initiate any transmission on DFS frequencies without initiation by a master device. This includes restriction on transmission for beacons and support for ad-hoc peer-to-peer modes.

This device does not provide user interface or allow user to configure the device in manner outside of what was intended by the grantee.

Software security questions and answers from KDB 594280 D02

Section	Questions	Answers
General Description	1. Describe how any software/firmware update will be obtained, downloaded, and installed.	Software/Firmware release is pushed from the grantee's authorized servers by means of proprietary encryption; therefore, user cannot obtain unauthorized software/firmware.
	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?	Radio parameters are fixed at time of production per FCC certification permitted. Future firmware release will be verified by the grantee before release. If required, grantee will follow FCC permissive change procedure.
	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, software/firmware are digitally signed and encrypted using proprietary handshaking, authorization and provisioning protocols.
	4. Are there any verification protocols in place	Yes, see answers to #1 and #3.

	to ensure that the software/firmware is legitimate? If so, describe in details	
	5. Describe, if any, encryption method is used.	Yes, by means of proprietary public key encryption.
	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 a master in some band of operation and client in another; how is compliance ensured in each band of operation?	Not applicable, see answers #1 and #2. End user cannot alter or update firmware.
Third-Party access Control	1. How are unauthorized software/firmware changes prevented?	Grantee releases the firmware/software directly from Grantee's servers through proprietary encryption protocol.
	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, refer to the answers #1, 2, and 3 under General Description.
	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 FCC ID device is a networked client, its radio parameters are controlled by the base stations.
	4. What prevents third parties from loading non-US versions of the software/firmware on the device?	Grantee proprietary hardware platform and software tool chain are required to replace firmware.
	5. For modular devices, describe how authentication is achieved when used with different hosts.	Not applicable, the FCC ID device is not a module.