

SparkLAN Communications, Inc
8F., No.257, Sec. 2, Tiding Blvd., Neihu District, Taipei
City 11493, Taiwan.

Software Security Description – KDB 594280 D02v01r01 Section II	
1. Describe how any software/firmware update will be obtained, downloaded, and installed.	The User can download the firmware from PLANET website manually.
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?	Wi-Fi radio frequency parameters can be changed via UI without any hardware changes; The regulatory domain frequencies was limited by the country code, all were verified by HW RF validation and stored in device embedded FLASH memory
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	No, but has a signature verification and checksum in the firmware header to ensure the firmware is legitimate.
4. Are there any verification protocols in place to ensure that the software/firmware is legitimate? If so, describe in details.	A signature verification and checksum in the firmware header to ensure the firmware is legitimate.
5. Describe, if any, encryption methods used.	No encryption methods were applied in the firmware
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?	The device can be configured as a client. Chipset vendor ensures its can compliance for each band of operation.
1. How are unauthorized software/firmware changes prevented?	A signature verification and checksum in the firmware header to ensure the US version of firmware.
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.	1) A signature verification and checksum in the firmware header to ensure the US version of firmware. 2) Regarding the GPL release, will provide the UI's binary code instead of source code.
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.	A signature verification and checksum in the firmware header to ensure the US version of firmware.
4. What prevents third parties from loading non-US	1) A signature verification and checksum in the

SparkLAN Communications, Inc
8F., No.257, Sec. 2, Tiding Blvd., Neihu District, Taipei
City 11493, Taiwan.

versions of the software/firmware on the device?	firmware header to ensure the US version of firmware. 2) Regarding the GPL release, will provide the UI's binary code instead of source code.
5. For modular devices, describe how authentication is achieved when used with different hosts.	N/A.

Your Sincerely,

Robert Wang

Name/Title: Robert Wang / Executive Assistant to CEO

Company name: SparkLAN Communications, Inc

ADD: 8F., No.257, Sec. 2, Tiding Blvd., Neihu District, Taipei City 11493, Taiwan.

TEL: +886-2-2659-1880#340

FAX: +886 2 2659 5538

E-mail: robert.wang@sparklan.com

Date: 2016/1/22