

Shenzhen Sang Fei Consumer Communications Co., Ltd.

11 Science and Technology Road, Shenzhen Hi-tech Industrial Park Nanshan District, Shenzhen city,
GuangDong Province, P.R.China 518057

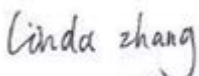
Software Security Description	
General Description	1. Describe how any software/firmware update will be obtained, downloaded, and installed. Software that is accessed through manufacturer's website or device's management system, must describe the different levels of security.
	The software updates are given to customer via official website. The software/firmware update is bundled, as part of the Android software update, and the user or installer cannot modify the content. The installation and/or update proceeds automatically once the user accepts to install/update the 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?
	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.
	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.
	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.
	4. Describe in detail the verification protocols in place to ensure that installed software/firmware is legitimate.
	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.
	5. Describe in detail any encryption methods used to support the use of legitimate software/firmware.
	"openssl_sign()" method is used to sign the software license.
	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?
	Since the software can work in Client mode, software was developed to update limitations, during configuration, instantly to meet compliance in any operating mode. Only authorized operating bands are allowed to configure by the professional installer.
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.
	It is impossible for the third party to develop a software manufactured devices.

Shenzhen Sang Fei Consumer Communications Co., Ltd.

11 Science and Technology Road, Shenzhen Hi-tech Industrial Park Nanshan District, Shenzhen city,
GuangDong Province, P.R.China 518057

	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.
	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.
	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.
	Products, which are certified as modular transmitters, are used only with original software as well. This way protecting illegal device configuration or use.

Name: Linda zhang

Sign: 

Date: 2016-3-28

Email: linda.zhang@sangfei.com

Phone
No: 010-68300097