CaptionCall®

Date: May 2 2017
FCC ID: 2AA6ZCR2

Software Security Description

We, CaptionCall, LLC, hereby declare that requirements of CR2 have been met and shown on the following question.

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. Description: The equipment network connection is automatically downloaded from the manufacturer's official website to update the latest software. Other users on the official website cannot make modifications, only the system administrator can modify the file permissions.
	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? Description: The software settings do not modify the RF parameters of the hardware;
	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. Description: The software is developed by the R & D software team according to the SDK compiled and tested and released with the complete intellectual property. The software is directly installed in the device's flash chip and cannot be modified by users or installers.
	4. Describe in detail the verification protocols in place to ensure that installed software/firmware is legitimate. Description: The R&D test team does rigorous testing on the SW/FW according to test specifications. If there are no problems the SW/FW is released.
	5. Describe in detail any encryption methods used to support the use of legitimate software/firmware. Description: Wireless encryption supports WEP, WPA-PSK (TKIP), WPA2-PSK (AES) and WPA-PSK (TKIP) + WPA2-PSK (AES)
	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? Description: The device support 802.11b/g/n/ac wireless bands

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. Description: The unit does not support third-part software modifications.
	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. Description: The Hardware flash size does not support third parties, such as DD-WRT software.
	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. Description: The driver cannot be managed as a separate module, but must be compiled into the software firmware.

Software Security Description	
User Configuration Guide	1. To whom is the UI accessible? (Professional installer, end user, other.) Description: Professional installers and end users can access the UI.
	a) What parameters are viewable to the professional installer/end-user? Description: Basic system parameters, network settings parameters and wireless basic and encryption parameters.
	b) What parameters are accessible or modifiable by the professional installer? Description: Basic system parameters, network settings parameters and wireless basic and encryption parameters
	(1) Are the parameters in some way limited, so that the installers will not enter parameters that exceed those authorized? Description: NA
	(2) What controls exist that the user cannot operate the device outside its authorization in the U.S.? Description: NA
	c) What parameters are accessible or modifiable to by the end-user? Description: Basic system parameters, network settings parameters and wireless basic and encryption parameters
	(1) Are the parameters in some way limited, so that the installers will not enter parameters that exceed those authorized? Description: NA

	(2) What controls exist that the user cannot operate the device outside its authorization in the U.S.? Description: NA
	d) Is the country code factory set? Can it be changed in the UI? Description: The country code is set at production and cannot be modified through the UI;
	(1) If so, what controls exist to ensure that the device can only operate within its authorization in the U.S.? Description: NA
	e) What are the default parameters when the device is restarted? Description: Country code defaults to FCC
	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. Description: It just support bridge mode, it does not support mesh.
	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? Description: the device support 802.11b/g/n/ac each wireless band.
	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)) Description: The device support 802.11b/g/n/ac each wireless band；

If any questions regarding this declaration, please don't hesitate to contact us.

Sincerely

Jasper Pan

(Jasper Pan, Director of Hardware Engineering)

CaptionCall