Date: 2024.11.01

SOFTWARE SECURITY REQUIREMENTS FOR U-NII DEVICES
(594280 D02 U-NII Device Security 1.3,11/12/15)

Company Name: CITAQ CO., LTD

FCC ID: 2AVZV-S1W05

Product Name: POS SYSTEM

SOFTWARE SECURITY DESCRIPTION	
General Description	
Q.	1. Describe how any software/firmware updates for elements than can affect the device's RF parameters will be obtained, downloaded, validated and installed. For software that is accessed through manufacturer's website or device's managment system, describe the different levels of security as appropriate.
A.	The user through the manufacturers web page download software/firmware upgrade will not affect the RF parameters. Because the software/firmware writing are the manufacturer in accordance with the requirements for the FCC rule, security level is high. WEP,TKIP,AES,WPA,WPA2
Q.	2. Describe the RF parameters that are modified by any software/firmware without any hardware changes. Are these parameters in some way limited such that any other software/firmware changes will not allow the device to exceed the authorized RF characteristics?
A.	All RF parameter is fixed at the chip level. Installer and user will not able to modify any of RF parameters.
Q.	3. Describe in detail the authentication protocols that are in place to ensure that the source of the RF-related software/firmware is valid. Describe in detail how the RF-related software is protected against modification.
A.	Software/firmware is digitally signed and encrypted using proprietary handshaking. Need authorized and provisioning protocols.
Q.	4. Describe in detail any encryption methods used to support the use of legitimate RF-related software/firmware.
A.	Software/firmware is digitally signed and encrypted using proprietary handshaking. Need authorized and provisioning protocols.
Q.	5. For a device that can be configured as a master and client (with active or passives canning),explain how the device ensures compliance for each mode? In particular, I the device acts as master in some band of operation and client in another; how is compliance ensure din each band of operation?
A.	Not applicable, this device is a client-only device.

Third-Party Access Control
1. Explain if any third part is have the capability to operate a U.S.-sold device on any other regulatory domain, frequencies, or in any manner that may allow the device to operate in violation of the device's authorization if activated in the U.S.
Only Grantee can release or make changes to the software/firmware using proprietary secure protocols.
2. Describe, if the device permits third-party software or firmware installation, what mechanisms are provided by the manufacturer to permit integration of such functions while ensuring that the RF parameters of the device cannot be operated outside its authorization for operation in the U.S. In the descriptionincludewhatcontrolsand/oragreementsareinplacewithproviders of third-party functionality to ensure the devices' underlying RF parameters are unchanged and how the manufacturer verifies the functionality.
If the third parties to operate, the device will not work.
3. For Certified Transmitter modular devices, describe how the module grantee ensures that host manufacturers fully comply with these software security equirements 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 RF parameters are not modified outside the grant of authorization.
N/A, This device is not a modular device.

SOFTWARE CONFIGURATION DESCRIPTION	
USER-CONFIGURATION GUIDE	
Q.	1. Describe the user configurations permitted through the UII f different levels of access are permitted for professional installers, system integrator so rend users, describe the differences.
A.	None
	a. What parameters are viewable and configurable by different parties?[9]
	None
	b. What parameters are accessible or modifiable by the professional installer or system integrators?
	None
	(1)Are the parameters in some way limited, so that the installers will not enter parameters that exceed those authorized?
	Parameters of the factory limited, whether to upgrade the firmware or restart, will not change the original parameters.
	(2)What controls exist that the user cannot operate the device outside its authorization in the U.S.?
	All RF parameter is fixed at the chip level. Installer and user will not able to modify any of RF parameters.
	c. What parameters are accessible or modifiable by the end-user?
	None

	(1)Are the parameters in some way limited, so that the user or installers will not enter parameters that exceed those authorized?
	Parameters of the factory limited, whether to upgrade the firmware or restart, will not change the original parameters.
	(2)What controls exist so that the user cannot operate the device out side its authorization in the U.S.?
	All RF parameter is fixed at the chip level. Installer and user will not able to modify any of RF parameters.
	d. Is the country code factory set? Can it be changed in the UI?
	Cannot.
	(1)If it can be changed, what controls exist to ensure that the device can only operate within its authorization in t he U.S.?
	All RF parameter is fixed at the chip level. Installer and user will not able to modify any of RF parameters.
	e. What are the default parameters when the device is restarted?
	The device will operate on last saved parameter.
Q.	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 905462D02.
A.	No
Q.	3. For a device that can be configured as a master and client (with active passives canning), 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?
A.	Not applicable, this device is a client-only device.
Q.	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.
A.	The device can't be configured as different types of access points. Device will operate in 5150~5850MHz. Antenna cannot be changed.

Signature: 

Name: Huang Bifeng

Phone: +86-754-88990426

E-Mail: huangbifeng@citaq.com