Date: 11/22/2022

SOFTWARESECURITYREQUIREMENTS FORU-NII DEVICES
(594280 D02 U-NII Device Security 1.3, 11/12/15)

Company Name: CHITECH SHENZHEN TECHNOLOGY CO.,LTD
FCC ID: 2AXUI-103S
Product Name: 4G TABLET PC

SOFTWARE SECURITYDESCRIPTION
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 management system, describe the different levels of security as appropriate.
A.	It can update from wireless access based on WiFi, A system update service runs in the device, users could only upgrade the software from WiFi via the service. And, any new software/firmware can be obtained from the qualified database from a private OTA server of company. The OTA server is based on cloud service, mainly store the software/firmware, the system update service with communicate with the OTA server and negotiate the update process. The update does not affect RF parameter.
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 the radio frequency parameters are not modified by any software/firmware without any hardware changes, because the software/firmware can’t changes the radio frequency 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 are digitally signed and encrypted using proprietary handshaking, authorization and provisioning protocols. Secure Sockets Layer is used protocol for encrypting information over the internet. Therefore, Can ensure that the source of the software/firmware is legitimate
Q.	4. Describe in detail any encryption methods used to support the use of legitimate RF-related software/firmware.
A.	RSA algorithm is used to sign and encrypt the software/firmware using a private key
Q.	5. For a device that can be configured as a master and client (with active or passive scanning), explain how the deviceensurescomplianceforeachmode?Inparticular,ifthedeviceactsas master in some band of operation and client in another; how is compliance ensured in each band of operation?
A.	The equipment only can be configured as a client device, And user can’t access to change client feature per band.

Third-PartyAccessControl
1. Explain if any third parties have the capability tope rate 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.
The modules firmware is stored in the ROM, third parties could not access the system image because they have no private key to do this. Under this pre-condition, A third party cannot change radio parameters. different country have different mechanism(likeness country code).It can control the module’ s parameter, such as Channel, Power, Bandwidth and etc. when sale to US, decided to device only have US mechanism(not certified frequencies are blocked). Out of US mechanism, the parameter(Channel, Power, Bandwidth and etc) is un allow able. So it cannot have capability to operate the device.
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 parameter soft he device cannot be operated outside its authorization for operation in the U.S. In the description include what control sand/or agreements are in place with providers of third-party functionality to ensure the devices’ underlying RF parameters are unchanged and how the manufacturer verifies the functionality.
The underlying code of user program owned the company will prevents third party from loading non-US versions of the software/firmware on the device, the device will protected from “flashing” and the installation of third-party firmware Through judging the false identification code. No one can generate a legal image without private key, if a illegal image is flashed in the device, the device won’ t start up.
3. For Certified Transmitter modular devices, describe how the module grantee ensures that host manufacturers 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 RF parameters are not modified out side the grant of authorization.
N/A

SOFTWARE CONFIGURATIONDESCRIPTION	
USER-CONFIGURATIONGUIDE	
Q.	1. Describe the user configurations permitted through the UI. If different levels of access are permitted for professional installers, system integrator sorend-users, descry be the differences.
A.	The UI is accessible to the end user, but the UI never gives access for specific operation parameters which are Channel, Power, Bandwidth, or Country code settings
	a. What parameters are viewable and configurable by different parties?[9]
	All RF parameter is not viewable by User
	b. What parameters are accessible or modifiable by the professional installer or system

	integrators?
	N/A
	(1)Are the parameters in some way limited, sothattheinstallerswillnotenterparametersthatexceedthoseauthorized?
	N/A
	(2)What controls exist that the user cannot operate the device outside its authorization in the U.S.?
	N/A
	c. What parameters are accessible or modifiable by the end-user?
	All parameters have pre-defined range according to the certification test result. They are stored in the ROM, And user can’t access to change parameters. such as Channel, Power, Bandwidth, or Country code settings.
	(1)Are the parameters in some way limited, so that the user or installers will not enter parameters that exceed those authorized?
	All parameters have pre-defined range according to the certification test result. They are stored in the ROM, And user can’t access to change parameters. such as Channel, Power, Bandwidth, or Country code settings.
	(2)What controls exist so that the user cannot operate the device outside its authorization in the U.S.?
	All parameters (RF, Frequency and etc.) indicating different countries are permanent setting in the ROM. If a device is a product for US, it cannot be changed for another region, And user can’t access to change parameters(Country code setting)
	d. Is the country code factory set? Can it be changed in the UI?
	The factory set the country code and the set is not change in the UI
	(1)If it can be changed, what controls exist to ensure that the device can only operate within its authorization in the U.S.?
	All parameters (RF, Frequency and etc.) indicating different countries are permanent setting in the ROM. If a device is a product for US, it cannot be changed for another region
	e. What are the default parameters when the device is restarted?
	The default parameters is that user latest saved in the UI
Q.	2. Can the radio be configured in bridge or mesh mode? If yes, an at station may be required. Further information is available in KDB Publication 905462D02.
A.	The device cannot be configured in bridge mode , it can be distinguished through the device MAC
Q.	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, with in 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.	This driver only have client mode, and user can’t access to change parameters. such as Channel, Power, Bandwidth, or Country code settings.
Q.	4. For a device that can be configured as different types of access points, such as point-to-point or point-to-multi point, 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 cannot support different types of access, only support point to point access. And user can’t access to change feature per band.

Lydia Deng

Lydia Deng / Manager

Date/City: **22/11/2022 / Shenzhen**
Phone: **86-0755-21380496**
Fax: **86-0755-21380496**
E-mail: sales8@chitechgroup.com.cn