SOFTWARE SECURITY DESCRIPTION (KDB 594280 D02 V01r03)

General Description	
Q1	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.
Ans	Software is updated by OTA. SW is accessed through CITECH website by management system of device, OTA module update it, bootloader is signed and secure boot is enabled during factory manufacturing.
Q2	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?
Ans	All the radio frequency parameters are transmit power, operating channel, modulation type which can be set in software version by authorized release. Although SW upgrade can change RF parameter, CITECH will execute internal tests to check and meet FCC requirements before upgrading SW. So that CITECH control the changes to meet FCC requirement
Q3	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.
Ans	RS201 is secured with SoC proprietary of security algorithm. So secured bootloader signed by CITECH is only allowed to be used to boot successfully. After the secure booting, secure OS check its effectiveness. The device won't be activated on before success of this signature authentications, firmware that will be allowed to update it only generated by CITECH with several security materials. Also OTA manager of device only connects CITECH certified distribution server that it has provisioned binary by CITECH SQE, The server requires specific credential for connection that the RS201 already have in binary level.
Q4	Describe in detail any encryption methods used to support the use of legitimate RF-related software/firmware.
Ans	We using X.509 certificates and signature algorithm like (RSASSA, ECDSA, DSA with SHA2) to secure SW/FW
Q5	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?
Ans	The device operates only as a client

Third-Party Access Control	
Q1	Explain if any third parties 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.
Ans	We are using Android open source platform, according to basic permission rule of AOSP then third party app only control their application boundary and it cannot harm platform setting without platform permission.
Q2	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 description include what controls and/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.
Ans	RS201 doesn't permit third-party firmware installation. The firmware installation can be handled only by CITECH.
Q3	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 outside the grant of authorization.
Ans	RS201 operates as a station.

SOFTWARE CONFIGURATION DESCRIPTION

Q1	Describe the user configurations permitted through the UI. If different levels of access are permitted for professional installers, system integrators or end-users, describe the differences.		
Ans	end user		
	a)	What parameters are viewable and configurable by different parties?	
	Ans	Signal strength and SSID is viewable on the UI. There is no any RF parameter is viewable to user	
	b)	What parameters are accessible or modifiable by the professional installer or system integrators?	
	Ans	Not applicable	
		(1)	Are the parameters in some way limited, so that the installers will not enter parameters that exceed those authorized?
		Ans	Not applicable
		(2)	What controls exist that the user cannot operate the device outside its authorization in the U.S.?
		Ans	Not applicable
	c)	What parameters are accessible or modifiable to by the end-user?	
	Ans	Not applicable	
		(1)	Are the parameters in some way limited, so that the installers will not enter parameters that exceed those authorized?
		Ans	Not applicable
		(2)	What controls exist that the user cannot operate the device outside its authorization in the U.S.?
		Ans	Not applicable
	d)	Is the country code factory set? Can it be changed in the UI?	
	Ans	Country code is factory set , user cannot change that in 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.?
		Ans	Not applicable, User is not allowed to change country code
	e)	What are the default parameters when the device is restarted?	
	Ans	This product boots with release parameter by the developer	
Q2	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.		
Ans	This product does not support a bridge mode or mesh mode.		
Q3	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?		
Ans	The device is only a client		
Q4	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))		
Ans	Not applicable		

Date: 25 April 2019

To whom it may concern,

Professional Install Justification:

CITECH CO.,LTD. the supplier of the device, declares that the **RS201** units are not sold or marketed to the general public and are only sold to wireless internet service providers and requires a professional installation.

The professional installers only shall have the account information which let them access to the configuration UI for the device. The account information for the professional installers shall not be revealed to end user.

Yu Jin KIM

General Manager
kyu6224@citech.kr