ZTECorporation.

ZTE Plaza, Keji Road South,Hi-Tech, Industrial Park, Nanshan District,Shenzhen, P.R.China

Tel: +86-21-68895397

Software Security Description

FCC ID: SRQ-ZTE-MF971V

We, ZTE Corporation hereby declare that the requirements of KDB594280 D02 U-NII Device Security v01r03

have been met and shown on the following questions.

SOFTWARE SECURITY DESCRIPTION

	Question	Answer
General Description	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.	The software/firmware update is bundled, as part of system 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 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?	The RF parameters can't be modified by updating software/firmware.
	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.	see answers to #1 Users cannot modify software in the field. Any update in the field happens via an over the air update which has to be digitally signed.
	4. Describe in detail any encryption methods used to support the use of legitimate RF-related software/firmware.	Yes, encryption using proprietary internal software.
	5. 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?	For compliance, device will transmit under approval power and user can't access to change Master/client feature per band.

ZTECorporation.

ZTE Plaza, Keji Road South,Hi-Tech, Industrial Park, Nanshan District,Shenzhen, P.R.China

Tel: +86-21-68895397

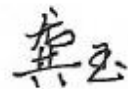| Third-Party Access Control	1. Explain if any third parties have the capability to operate a U.S.-sold device on any other regulatory domain, frequencies, or in any manner that may allow the device to operate in violation of the device's authorization if activated in the U.S.	This is set up during manufacturing and cannot be modified in the field as explained by questions 1, 2, and 3 in the General Description section.
	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 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.	Third parties cannot modify the RF parameters as explained by questions 1, 2, and 3 in the General Description section.
	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 outside the grant of authorization.	Not applicable. The device isn't a modular.
USER CONFIGURATION GUIDE	1. 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.	No user configuration UI is accessible. All the settings are pre programmed during manufacturing and cannot be changed by users.
	a. What parameters are viewable and configurable by different parties?	No.
	b. What parameters are accessible or modifiable by the professional installer or system integrators?	No.
	(1) Are the parameters in some way limited, so that the installers will not enter parameters that exceed those authorized?	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?	No.

ZTECorporation.

ZTE Plaza, Keji Road South,Hi-Tech, Industrial Park, Nanshan District,Shenzhen, P.R.China

Tel: +86-21-68895397

	(1) Are the parameters in some way limited, so that the user or installers will not enter parameters that exceed those authorized?	N/A.
	(2) What controls exist so that the user cannot operate the device outside its authorization in the U.S.?	N/A.
	d. Is the country code factory set? Can it be changed in the UI?	No.
	(1) If it can be changed, what controls exist to ensure that the device can only operate within its authorization in the U.S.?	N/A.
	e. What are the default parameters when the device is restarted?	The default parameters is the same as before the device is restarted .
	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.	No.
	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?	User can't configure device as a master and client .
	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))	No, This device is only support single mode client or master.

Company Information:

_____

Signature