

ZTE Corporation

Software Operational Description

FCC ID: SRQ-Z6251

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 that 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.	All the software parameters which determine RF configuration and tuning are part of the device firmware. The firmware is provided to the factory in a secure procedure for flashing the newly produced devices. It is not possible to manipulate any of these data by a third party software tool or application. Third party applications can only modify the user level parameters only.
	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?	Any RF related software parameter is part of the binary only. They can be only updated by another approved software binary which will also go through the formal certification.
	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.	The firmware update procedure validates the initial device software configuration and a finger print which includes the device IMEI, model and version information, checksum and the firmware signature. The distribution of the update is controlled through the web based service hosted by Google.
	4. Describe in detail any encryption methods used to support the use of legitimate RF-related software/firmware.	Secure ftp
	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?	UNII-1 and UNII-3 can be Master (hotspot) and Slave mode.
Third-Party	1. Explain if any third parties have the capability to operate a U.S.-sold device on any other	No third parties have the capability to operate this device on any regulatory

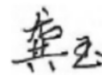
ZTE Corporation

Access Control	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.	domain frequencies, or in any manner that may allow the device to operate in violation of the device's authorization if activated in the United States.
	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-party firmware installation is not permitted on the device
	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.	The device is not a module
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.	None of the mentioned parameters are viewable, thus not configurable (frequency of operation, power settings, antenna types, DFS settings, receiver thresholds, or country code settings).
	a. What parameters are viewable and configurable by different parties?	No parameters are accessible or modifiable by any parties
	b. What parameters are accessible or modifiable by the professional installer or system integrators?	No parameters are accessible or modifiable by professional installers or system integrators
	(1) Are the parameters in some way limited, so that the installers will not enter parameters that exceed those authorized?	None of the mentioned parameters are adjustable or viewable
	(2) What controls exist that the user cannot operate the device outside its authorization in the U.S.?	None of the mentioned parameters are adjustable or viewable, thus not configurable
	c. What parameters are accessible or modifiable by the end-user?	None of the mentioned parameters are adjustable or viewable, thus not configurable (frequency of operation, power settings, antenna types, DFS settings, receiver thresholds, or country code settings).
	(1) Are the parameters in some way limited, so that the user or installers will not enter	There is no access to the parameters either by UI or application, so it is not

ZTE Corporation

	parameters that exceed those authorized?	possible to modify any parameter at all.
	(2) What controls exist so that the user cannot operate the device outside its authorization in the U.S.?	None of the mentioned parameters are adjustable or viewable, thus not configurable (frequency of operation, power settings, antenna types, DFS settings).
	d. Is the country code factory set? Can it be changed in the UI?	Yes. It cannot be changed 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.?	None of the mentioned parameters are adjustable or viewable, thus not configurable (frequency of operation, power settings, antenna types, DFS settings, receiver thresholds, or country code settings).
	e. What are the default parameters when the device is restarted?	The previously used settings will be loaded.
	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.	The radio cannot be operated in bridge or mesh mode.
	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?	Not relevant, the device operates in client mode with wifi 5G.
	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))	The device complies with the requirements as per Section 15.407(a). All RF configurations are part of the device software and factory controlled procedures only. It is not possible for an end user to alter the parameters.

Company Information: ZTE Corporation



Signature