MOTOROLA SOLUTIONS

May 13, 2019

Software Operational Description

FCC ID: **AZ489FT7119**

We, **The Development Team,** 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	
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.
	Answer: Device software is obtained through a portal that requires customer sign in with username and password. The portal is through the world wide web using SSL/TLS security.
	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?
	Answer: RF parameters are not modified through user level software and WiFi band selection / country code configuration are also locked per region.
	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.
	Answer: RF source code protocols are integrated in the Qualcomm IC and related firmware. MSI obtains the firmware directly from Qualcomm through an account registered with Qualcomm and protected by a fused secure boot mechanism.
	4. Describe in detail any encryption methods used to support the use of legitimate RF-related software/firmware.
	Answer: Standard encryption protocols are used with Bluetooth (E0 encryption) and WiFi (WPA).
	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?

	Answer: The device can only be configured as a WiFi client (STA) and BT master/client using standard Android mechanisms. Compliance is ensured through device configurations that are not modifiable by the user.
Third-Party Access Control	6. 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.
	Answer: The WiFi configuration is set through the use of a country code, which is locked and all other bands (LTE) are supported as declared to the FCC.
	7. 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.
	Answer: Third party android applications cannot be installed on this device. Secure Android mechanisms ensure that applications do not have the authority to change RF parameters.
	8. For Certified Transmitter modular devices, describe how the module grantee ensures that hosts manufactures 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.
	Answer: The RF parameters are stored in a specific file that is not modifiable by driver software. The RF parameters comply with U-NII band limits.
SOFTWARE CONFIGURATION DESCRIPTION	
USER CONFIGURATION GUIDE	9. 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.
	Answer: There are no separate modes of operation permitted through the UI.
	a. What parameters are viewable and configurable by different parties?
	Answer: User can control and view parameters that are viewable

	and controllable in standard Android devices.
	b. What parameters are accessible or modifiable by the professional installer or system integrators?
	Answer: Authorized device manager users can access and modify parameters per customer needs.
	i. Are the parameters in some way limited, so that the installers will not enter parameters that exceed those authorized?
	Answer: Yes, device manager can only modify parameters that they are authorized to modify.
	ii. What controls exist that the user cannot operate the device outside its authorization in the U.S.?
	Answer: The FCC limits are specified in a specific RF parameter file that is not accessible or modifiable by the user.
	c. What parameters are accessible or modifiable by the end-user?
	Answer: User can control and view parameters that are viewable and controllable in standard Android devices.
	i. Are the parameters in some way limited, so that the user or installers will not enter parameters that exceed those authorized?
	Answer: Yes
	ii. What controls exist so that the user cannot operate the device outside its authorization in the U.S.?
	Answer: The FCC limits are specified in a specific RF parameter file that is not accessible or modifiable by the user.
	d. Is the country code factory set? Can it be changed in the UI?
	Answer: The country code set in SW for US (United States) region and cannot be changed in the UI
	i. If it can be changed, what controls exist to ensure that the device can only operate within its authorization in the U.S.?
	Answer: The country code cannot be changed in the UI.
	e. What are the default parameters when the device is restarted?
	Answer: The device complies with FCC rules. The settings/parameters will not be changed even after restarting the device.

	10. 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.
	Answer: The device cannot be configured into bridge or mesh modes.
	11. 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?
	Answer: The UI in default acts as a client and cannot be configured as a master. Compliance is ensured through device configurations that are not modifiable by the user.
	12. 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))
	Answer: This device cannot be configured as an access point.

If you should have any question(s) regarding this declaration, please don't hesitate to contact us. Thank you!

Melissa A. Ley

Name: Melissa Ley
Title: Engineering Manager
Tel: (954) 605-3922
E-mail: Melissa.Ley@motorolasolutions.com