FCC DTS&UII declaration

Oct 25, 2024
Federal Communications Commission
7435 Oakland Mills Road
Columbia, Maryland 21046
USA
FCC ID:2A2UU-N4
Gentlemen:

Please be advised that the Mobile phone is manufactured for the global market but when marketed in the U.S. under FCC ID:2A2UU-N4412 . The nonvolatile memory (NVM) will be programmed at the factory to only actively scan and operate on these specific channels during normal WLAN operation. During Wi-Fi Direct mode the device may act as a group owner (GO) to establish a peer-to-peer (P2P) network including conditions when no master device is present on these specific channels.
Channels 1-11,2412-2462MHz 802.11b mode
Channels 1-11, 2412-2462MHz 802.11g mode
Channels 1-11, 2412-2462MHz 802.11n mode (20MHz channel)
Channels 3-11, 2422-2462MHz 802.11n mode (40MHz channel)

The device operates as a client without radar detection capability and will be programmed at the factory to passively scan on the following dynamic frequency selection (DFS) channels and will only listen for a master device and cannot send a probe request to initiate communication on these DFS channels. Accordingly passive scanning provides protection for TDWR operations and preventing transmission in the 5600MHz – 5650MHz frequency band. Client software and drivers will never enable the device to act as a master or GO for operation in DFS frequency bands and therefore ad-hoc mode is always disabled on these passive scan DFS channels.
Channels 52-64, 5260-5320MHz 802.11a mode
Channels 52-64, 5260-5320MHz 802.11n mode (20 MHz channel)
Channels 52-64, 5260-5320MHz 802.11ac mode (20 MHz channel)
Channels 54-62, 5270-5310MHz 802.11n mode (40MHz channel)
Channels 54-62, 5270-5310MHz 802.11ac mode (40MHz channel)
Channel 58, 5290MHz 802.11ac mode (80MHz channel)
Channels 100-140, 5500-5700MHz 802.11a mode
Channels 100-140, 5500-5700MHz 802.11n mode (20 MHz channel)
Channels 100-144, 5500-5720MHz 802.11ac mode (20 MHz channel)
Channels 102-134, 5510-5670MHz 802.11n mode (40MHz channel)
Channels 102-142, 5510-5710MHz 802.11ac mode (40MHz channel)
Channels 106 &138, 5540 & 5690MHz 802.11ac mode (80MHz channel)

This device meets the requirements of FCC Part 15.202 and accordingly will be programmed at the factory to active scan on the following non-DFS channels to

initiate communication during normal WLAN operation. When operating in Wi-Fi Direct mode on these non-DFS channels, it may operate as a P2P client device or GO to establish a P2P network if, and only if, a master device is present and network communication is maintained between a master device and the GO.
Channels 36-48, 5180-5240MHz 802.11a mode
Channels 36-48, 5180-5240MHz 802.11n mode (20 MHz channel)
Channels 36-48, 5180-5240MHz 802.11ac mode (20 MHz channel)
Channels 38-46, 5190-5230MHz 802.11n mode (40MHz channel)
Channels 38-46, 5190-5230MHz 802.11ac mode (40MHz channel)
Channel 42, 5210MHz 802.11ac mode (80MHz channel)
Channels 149-165, 5745-5825MHz 802.11a mode
Channels 149-165, 5745-5825MHz 802.11n mode (20 MHz channel)
Channels 149-165, 5745-5825MHz 802.11ac mode (20 MHz channel)
Channels151-159, 5755-5795MHz 802.11n mode (40MHz channel)
Channels151-159, 5755-5795MHz 802.11ac mode (40MHz channel)
Channel 155, 5775MHz 802.11ac mode (80MHz channel)

This information when programmed into the NVM will not be accessible and cannot be changed by the end user. The transmitter is approved as a non-software defined radio and OEMs and third party system integrators do not have the ability through software to allow configuration controls that would permit the device to operate outside the grant conditions per FCC KDB 594280.

Title: Project Manager
Print name: Claudia Chen
Shanghai Xiangcheng Communication Technology Co.,Ltd

Software Security Requirement Description for UNII Devices

II. SOFTWARE SECURITY DESCRIPTION FCC ID:2A2UU-N4

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. Reply:The user can download upgrade software on readme website, and by devices' upgrade management system (OTA). But both two upgrade methods only can upgrade the operating system and built-in application software, the radio frequency parameter will not change.
	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? Reply:The radio frequency parameter stored in non-volatile memory, and it cannot be modified by end user except our professional service engineer used special tools and drivers. And before refresh non-volatile memory a build-in upgrade software will compare the new parameter with the devices. (e.g US version, EU version), if another MCC parameter refresh in a US version devices, the upgrade process will be automatically forced stop by devices upgrade software.
	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. Reply:The devices radio frequencies was controlled by the radio frequency parameter which store in non-volatile memory. If the radio frequency parameter missing the radio frequencies module will not working anymore. And the radio frequency parameter need special tools and special drivers to re-flesh.

	4. Describe in detail any encryption methods used to support the use of legitimate RF-related software/firmware. Reply:The radio frequency parameter was produced by special software after calibrated. And the radio frequency parameter packed encrypt used Message Digest Algorithm MD5 method. And the radio frequency parameter packed contain the software version, hardware vision and series number information. And these information are differences in each country. If the radio frequency parameter is not matched with the devices, the upgrade process will be automatically forced stopped by devices upgrade 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? Reply:The devices was design as a client without radar detection function. For the DFS compliance, please refer DFS test report.

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. Reply:No, there is no body can re-flash the radio frequency parameter except our-self.
	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

	Reply: The radio frequency parameter is not easily be re-fresh by the third parties, it must be re-fresh by a special tools and special drivers, what more our devices upgrade software will compare the new parameter, if it's not correct the upgrade process will be automatically forced.
	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. Reply:Our devices is a end product not a modular devices, and its function cannot working as a modular devices.

III. SOFTWARE CONFIGURATION DESCRIPTION GUIDE

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. Reply:There is no need a professional installer for our devices. The UI had same level for the all user.
	a) What parameters are viewable and configurable by different parties? Reply:There is no need a professional installer for our devices. The UI had same level for the all user.
	b) What parameters are accessible or modifiable by the professional installer or system integrators? Reply:There is no need a professional installer for our devices. The UI had same level for the all user.
	(1) Are the parameters in some way limited, so that the installers will not enter parameters that exceed those authorized? Reply:There is no need a professional installer for our devices. The UI had same level for the all user.
	(2) What controls exist that the user cannot operate the device outside its authorization in the U.S.? Reply:There is no need a professional installer for our devices. The UI had same level for the all user.
	b) What parameters are accessible or modifiable to by the end-user? Reply:The end user only authorized tune on/off radios, and 2.4G band/ 5G band mode selection, and cannot modify any radio parameters.

	(1) Are the parameters in some way limited, so that the installers will not enter parameters that exceed those authorized? Reply:The end user only authorized tune on/off radios, and 2.4G band/ 5G band mode selection, and cannot modify any radio parameters.
	(2) What controls exist that the user cannot operate the device outside its authorization in the U.S.? Reply:The end user only authorized tune on/off radios, and 2.4G band/ 5G band mode selection, and cannot modify any radio parameters.
	c) Is the country code factory set? Can it be changed in the UI? Reply:Yes, we had country code in factory set, device can got its physical address by GPS, IP address, ISP MCC code and etc. The frequency parameter will force to US/Canada use only when devices detected it location within the territory of US/Canada, the end user cannot change it in the UI.
	(1) If so, what controls exist to ensure that the device can only operate within its authorization in the U.S.? Reply:Per our technology design, this device can be get its physical address by GPS, IP address, operator / ISP MCC code and etc., and device will automatic import the correct RF parameter. And will adjust its radio frequency in accordance with local laws and regulations. This geo location function was controlled by built-in operating software with a high priority, the end user cannot select and control this function;
	e) What are the default parameters when the device is restarted? Reply:If devices restarted the built-in operating software will re-check his location and automatic import the correct RF parameter.
	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.

	Reply:No, this devices cannot be configured 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? Reply:This device was designed only as a client without radar detection function.
	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)) Reply:During hotspot mode, devices only used 2.4GHz band, 5150~5250 MHz and 5725-5825MHz band by soft control, the end user cannot open other bands.