U-NII Device SW Security Statement

Model Name : ASM

FCC ID : XYCASM

The information within this section of the Operational Description is to show compliance against the Software Security Requirements laid out within KDB 594280 D02 U-NII Security v01 r03.

The information below describes how we maintain the overall security measures and systems so that only:

1. Authenticated software is loaded and operating on the device
2. The device is not easily modified to operate with RF parameters outside of the authorization

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] Update the firmware via from Server PC. The Website will check the firmware version and enable the downloading firmware and install it.
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] Center Frequencies of channels, channel bandwidth, modulations and transmit power levels are defined in software. There is no acess to modify frequency parameter.
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] The firmware upgrade functions only allow programming of firmware that has been provided by Aramhuvis Co.,Ltd., Check firmware with own file description in it
4. ***Describe in detail*** any encryption methods used to support the use of legitimate RF-related software/firmware.	No.
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] Support master and client mode. Changeable in UI.

3rd 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.	[Answer] Country domain is set in non-valatile memory during manufacture. The software and user interface does not provide any option to choose a country of operation.
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.	[Answer] No.
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[1]	[Answer] No.

[1] Note that Certified Transmitter Modules must have sufficient level of security to ensure that when integrated into a permissible host the device's RF parameters are not modified outside those approved in the grant of authorization. (See, KDB Publication 99639). This requirement includes any driver software related to RF output that may be installed in the host, as well as, any third-party software that may be permitted to control the module. **A full description of the process for managing this should be included in the filing.**

U-NII Device SW Security Statement

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.	[Answer] No.
a) What parameters are viewable and configurable by different parties?	[Answer] No.
b) What parameters are accessible or modifiable by the professional installer or system integrators?	[Answer] Only professional installer can change configuration for master and/or client mode through UI
i) Are the parameters in some way limited, so that the installers will not enter parameters that exceed those authorized?	
ii) What controls exist that the user cannot operate the device outside its authorization in the U.S.?	
c) What parameters are accessible or modifiable by the end-user?	[Answer] No.
i) Are the parameters in some way limited, so that the user or installers will not enter parameters that exceed those authorized?	
ii) What controls exist so that the user cannot operate the device outside its authorization in the U.S.?	
d) Is the country code factory set? Can it be changed in the UI?	[Answer] No.
i) If it can be changed, what controls exist to ensure that the device can only operate within its authorization in the U.S.?	
e) What are the default parameters when the device is restarted?	[Answer] No.
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.	[Answer] Not supported.
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?	[Answer] Only support client mode
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))	[Answer] Not supported.