SEMES

77, 4sandan 5-gil, Jiksan-eup Seobuk-gu, Cheonan-si,

Chungcheongnam-do, Korea

Attestation letter

Date : December 15, 2017
Subject : SW Security Requirement for U-NII DEVICE per KDB 594280 D02
FCC ID : 2AN5BGIS-PAMSC3
Model No. : GIS-PAMSC3

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. Module firmware (refer to as below FW) updated can only be done by grantee, updated the FW via USB port on the engineering too. The tool will check the firmware version, enable the update mode 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? All RF parameter is hardcoded at factory, any future SW upgrade will no able to modify and RF parameters.
	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. This device has an 802.11a/g/b protocol, but not use DFS band, The FW on the device does not support writing to NVM(non-volatile memory) including FW, except through the use of our FW update tools. The FW update too that has been provided by SEMES permit programming of FW.
	4.	Describe in detail any encryption methods used to support the use of legitimate RF-related software/firmware. WPA2-PSK, WAP2-PEAP, AES
	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? This device does not use DFS channel, so met this requirement.

SEMES

77, 4sandan 5-gil, Jiksan-eup Seobuk-gu, Cheonan-si,

Chungcheongnam-do, Korea

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. No. any 3rd parties don't have capability to access and change this module. When US locked devices reach they have to be returned for replace non US locked devices. There is no method to alter or unlock them.
	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. Not permits to install third-part software or firmware into 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 All RF parameter in the device was hardcoded at the factory, so any 3rd party cannot able to modify

SOFTWARE CONFIGURATION DESCRIPTION	
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.
	a. What parameters are viewable and configurable by different parties? N/A
	b. What parameters are accessible or modifiable by the professional installer or system integrators? N/A
	(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? N/A
	(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? N/A
	(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? N/A
	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. This device cannot be configured in a 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? This device support only Wi-Fi 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)) N/A

BAEK SEUNG CHEOL