Sony Corporation, Head Office
1-7-1 Konan Minato-ku, Tokyo, 108-0075 Japan

Federal Communication Commission
Equipment Authorization Division, Application Processing Branch
7435 Oakland Mills Road
Columbia, MD21048

2015-08-07

Attn: Office of Engineering and Technology
Subject: Attestation Letter regarding UNII devices

FCC ID: **AK8-CBK-WA02**

Software security questions and answers per KDB 594280 D02:

Software Security description – General Description		
1	Describe how any software/firmware update will be obtained, downloaded, and installed. Software that is accessed through manufacturer's website or device's management system, must describe the different levels of security.	We do not release the firmware on our website for downloading. Our direct host manufacturer (OEM) can request the firmware from us and it will be made available via secure server.
2	Describe all the radio frequency parameters that are modified by any software/firmware without any hardware changes. Are these parameters in some way limited, such that, it will not exceed the authorized parameters?	Radio frequency parameters are limited by US regulatory domain and country code to limit frequency and transmit power levels. These limits are stored in non-volatile memory by the module manufacturer at the time of production. They will not exceed the authorized values.
3	Describe in detail the authentication protocols that are in place to ensure that the source of the software/firmware is legitimate. Describe in detail how the software is protected against modification	The firmware is installed on each single module during manufacturing process. The correct firmware is verified and installed by the module manufacturer.
4	Describe in detail the verification protocols in place to ensure that installed software/firmware is legitimate	Only correct firmware is stored in SROM (see #3).
5	Describe in detail the verification protocols in place to ensure that installed software/firmware is legitimate	Only correct firmware is stored in SROM (see #3).
6	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?	The device ensures the compliance by checking the configured parameter and operation values according to the country code in each band.

Software Security description – Third-Party Access Control		
1	How is unauthorized software/firmwarechanges prevented?	Unauthorized firmware is not accepted by the firmware update process. See General Description #5, #3
2	Is it possible for third parties to load device drivers that could modify the RF parameters, country of operation or other parameters which impact device compliance? If so, describe procedures to ensure that only approved drivers are loaded.	No, third parties don't have the capability to modify the RF parameters.
3	Explain if any third parties have the capability to operate a US sold device on any other regulatory domain, frequencies, or in any manner that is in violation of the certification.	No, third parties don't have the capability to access and change radio parameters. US sold modules are factory configured to US.
4	What prevents third parties from loading on -US versions of the software/firmware on the device?	No, third parties don't loading software/firmware on the device.
5	For modular devices, describe how authentication is achieved when used with different hosts.	The module is not available for sale or installation outside of company licensing agreements. Modules are always installed in host systems in a factory by end integrators (OEM) responsible for loading authorized software.
Software Security description – USER CONFIGURATION GUID		
1	To whom is the UI accessible? (Professional installer, end user, other.)	We don't have UI.
	a. What parameters are viewable to the professional installer/end user?	We don't have UI.
	b. What parameters are accessible or modifiable to the professional installer? 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.?	We don't have UI.
	c. What configuration options are available to the end-user? 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.?	We don't have UI.

	d. Is the country code factory set? Can it be changed in the UI? i. If so, what controls exist to ensure that the device can only operate within its authorization in the U.S.?	We don’t have UI.
	e. What are the default parameters when the device is restarted?	We don’t have UI.
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.	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 control sexist, 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?	No end user controls or user interface operation to change master/client operation.
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 does not support these modes/features.

Sincerely

Y Fujita

Name: Yutaka FUJITA
Company: Sony Corporation
Address: 1-7-1 KonanMinato-kuTokyo108-0075Japan
E-mail: dipf-diec-ps-appl@jp.sony.com
Telephone: 81-3-6748-4405
Fax: 81-3-6748-4409