Christie Digital Systems Canada

Wi-Fi Operations declaration

TUV SUD BABT TCB
Octagon House,
Segensworth Road,
Fareham,
Hampshire,
PO15 5RL

ATTN: Reviewing Engineer

Date: **April . 28, 2017**

Ref: **Attestation letter regarding WiFi client device without radar detection capability for FCC ID: XU6-UHD651-L**

To whom it may concern:

This device operates is programed to operate only in the following frequencies:

2.4 GHz Band,

Channels 1-11, Frequency Range **2.412 - 2.462 GHz**
All channels operate with 20MHz Bandwidth.

5GHz Band,

Channels 36-134, Frequency Range **5.18 – 5.67 GHz**
Device won't operate in the frequency range **5.6 – 5.65 GHz**
For 802.11 a, all channels operate with 20 MHz Bandwidth
For 802.11 n, channels operate with 20 MHz and 40 MHz Bandwidth.

This device does not support Ad-Hoc / Wi-Fi hotspot mode in 5 GHz frequency band where the device operates as a client device without Radar detection. Ad-hoc / Wi-Fi hotspot feature is limited to 11 channels available in 2.4 GHz frequency band.

As client device, this product does not initiate transmission of any probes, beacons and does not initiate Ad-Hoc operations when not associated with and under the control of a certified master device, according to Section 15.202 of FCC rules.

Future changes in this device will not change theses operational characteristics, in any mode of operation.

Software security questions and answers per KDB 594280 D02:

Section	Questions	Answers
General Description	1. Describe how any software/firmware update will be obtained, downloaded, and installed.	The software/firmware update is bundled as part of the operating system software update, and the user or installer cannot modify the content. The installation and/or update proceeds automatically once the user accepts to install/update the software/firmware.
	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 parameters are fixed at time of production as required by the FCC certification. Any future software/firmware release is verified by Vestel Trade Co. before release. If required, Vestel Trade Co. will follow FCC permissive change procedure.
	3. Are there any authentication protocols in place to ensure that the source of the software/firmware is legitimate? If so, describe in details; if not, explain how the software is secured from modification.	Yes, software/firmware is digitally signed and encrypted using proprietary handshaking, authorization and provisioning protocols.

	4. Are there any verification protocols in place to ensure that the software/firmware is legitimate? If so, describe in details.	Yes, see answers to #1 and #3.
	5. Describe, if any, encryption method is used.	Yes, encryption using proprietary internal software.
	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 a master in some band of operation and client in another; how is compliance ensured in each band of operation?	Not applicable, this device is a client-only Device for all 5 GHz frequency bands.
Third-Party Access Control	1. How are unauthorized software/firmware changes prevented?	Only Vestel Trade Co. can release or make changes to the software/firmware using proprietary secure protocols.
	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, refer to the answers #1, 2, and 3 under General Description.
	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, refer to the answers above.
	4. What prevents third parties from loading non-US versions of the software/firmware on the device?	Vestel Trade Co. proprietary hardware platform, software tools and proprietary protocols are required to replace firmware.
	5. For modular devices, describe how authentication is achieved when used with different hosts.	Not applicable, this device is not a module.

Sincerely,

PA

Mr. Masud Attayi
Manager Product Compliance
Christie Digital Systems Canada.