FCC - ISED - Wi-Fi Operations declaration

Date: **March 24th, 2021**

ATTN:

Regulatory Certification Body

DEKRA Testing and Certification, S.A.U.

Parque Tecnológico de Andalucía
C/ Severo Ochoa 2 & 6
29590 Campanillas
Málaga, España

Ref: **Attestation letter regarding WIFI without radar detection capability for FCC ID: A269ZUA163**

To whom it may concern: The equipment MGU21 APN with FCC ID: **A269ZUA163** will operate only

in the following frequencies:

2.4 GHz Band,

Channels 1-11, Frequency Range **2.412 - 2.462 GHz**

The final user cannot use the channels 12 and 13, and can not change the configuration.

5GHz Band,

Channels 1-13, in the sub-band **5.15 - 5.25 GHz**
-For IEEE 802.11a, all the channels operates in 20MHz
-For IEEE 802.11n, all the channels operates in 20MHz and 40MHz
-For IEEE 802.11ac, all the channels operates in 20MHz, 40MHz and 80MHz.

Channels 149-165, in the sub-band **5.725-5.85 GHz**.
-For IEEE 802.11a, all the channels operates in 20MHz
-For IEEE 802.11n, all the channels operates in 20MHz and 40 MHz
-For IEEE 802.11ac, all the channels operates in 20MHz , 40 MHz and 80 MHz.

This device does not support DFS, and limited to the channels listed above in Client and Access point mode, thus the criteria for FCC are the same.

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 only allowed in authorized locations, and directly installed by authorized professionals and using SW provided by the manufacturer.
	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 before release. If required, Alpine Electronics GmbH, 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 (esp. Kernel and Bootloader) is digitally signed. Additionally periodic validation of SW parts is performed. Furthermore the SoC safeguards through a security engine that no modified Kernel is executed.

	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?	This device is working in both UNI-1 and UNII-3 frequency bands without DFS where the criteria are common for client and Master
Third-Party Access Control	1. How are unauthorized software/firmware changes prevented?	Only ALPS ALPINE EUROPE GmbH 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?	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.

By: Mitsuru Yoshida
Company: ALPS ALPINE CO., LTD.
Telephone: +81-246-36-4111
e-mail: yoshida-mtr@apn.alpine.co.jp