APTIV

SOFTWARE SECURITY REQUIREMENTS FOR U-NII DEVICES

Date: 09th January 2023

ATTN: FCC
ISED

Subject: Attestation Letter regarding UNII devices

FCC ID: LTQVTSEMNAR, **IC:** 3659A-VTSEMNAR, Software security questions and answers per KDB 594280 D02 v01r03:

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. **There is no downloadable software provided by the manufacturer that can modify critical radio transmitter parameters. All critical parameters are programmed in Software and cannot be modified or overridden by third parties.**
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? **Software can control band selection. This is limited by country code and can only be changed by authorized local workshop.**
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. **Software/firmware can only be updated through an image update, this can only be done by local authorized workshop and is digitally signed.**
4	Describe in detail any encryption methods used to support the use of legitimate RF-related software/firmware. **Software/firmware can only be updated through an image update, this image is digitally signed.**
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? **The device ensures compliance by checking the configured parameters and operation values according to the regulatory domain and country code on each band.**
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. **Third parties do not have the capability to operate in any manner that is violation of the certification in the U.S.**

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. **Third party software doesn´t have access to RF Parameters. The device doesn´t permit firmware installation by third parties.**
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. **Not applicable, device is not a module.**
	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. **No UI for configuration provided.**
	a) What parameters are viewable and configurable by different parties? **The Only RF parameter that can be changed by user: wireless band for Wi-Fi from 2.4Ghz to 5GHz in access point mode. If the country code allows for this band to be selected.**
	b) What parameters are accessible or modifiable by the professional installer or system integrators? **Country code can be changed by authorized workshop only.**
	1) Are the parameters in some way limited, so that the installers will not enter parameters that exceed those authorized? **Country code can be changed by authorized workshop only. Parameters also limited by graphical interface options. User can´t select bands not allowed by Country code.**
	2) What controls exist that the user cannot operate the device outside its authorization in the U.S.? **Country code is set at factory, country code can be changed by authorized workshop only. The country code and regulatory domain, control the limit of all the parameters set by the UI, so user cannot change the Parameters.**
	c) What parameters are accessible or modifiable by the end-user? **The Only RF parameter that can be changed by user: is wireless band from 2.4Ghz to 5GHz access point mode. IF the country code allows for this band to be selected.**
	d) Is the country code factory set? Can it be changed in the UI? **Default country code is set in the factory and no UI is provided for modification.**
	1) If it can be changed, what controls exist to ensure that the device can only operate within its authorization in the U.S.? **Country code cannot be changed in the UI.**
	e) What are the default parameters when the device is restarted? **First boot device will have WLAN active but not connected, Bluetooth active but not connected. After restart device will have last user defined settings.**
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. **No, it can't work in the bridge or the 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? **The device does not support these modes/features.**
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,

Printed Name: Torbjorn Hildesson

Position: Software Engineer

Company Name: Aptiv Services Deutschland GmbH