

## SOFTWARE SECURITY INFORMATION

**FCC ID: WUQ-MIB3VBTWIFI**  
**IC : 216R-MIB3VBTWIFI**

Pursuant to:

FCC Part 15E 15.407(I) and KDB 594280 D02 UNII Device Security v01r03 / IC RSS-247article 6.4(4).

The information within this section is to show compliance against the SW Security Requirements laid out within KDB 594280 D02 U-NII Device Security v01r03. The information below describes how to maintain the overall security measures and systems so that only:

1. **Authenticated software is loaded and operating on the device.**
2. **The device is not easily modified to operate with RF parameters outside of the authorization.**

SOFTWARE SECURITY DESCRIPTION		
	Requirement	Answer
<b>General Description</b>	1. Describe how any software/firmware updates for elements that 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.	<p>Bluetooth and Wifi firmware can be part of the Service Update package, of the BT Customer Update package and Wifi Customer Update package.</p> <p>Service Update and Customer update packages are directly delivered by Panasonic to Skoda/VW/SEAT through secure encrypted channel.</p> <p>Service Update and Customer Update packages contain artifacts which are encrypted. The packages contain meta information which describes the checksum calculation for each artifact. The meta-information itself is protected by a main checksum calculation which is finally protected by a signature which is generated by Skoda/VW/SEAT and validated before starting the update procedure. Installation starts only if the signature validation and the checksum verification succeed.</p> <p>Service Update packages are distributed by Skoda/VW/SEAT to the respective car dealers, security measures cannot be known to Panasonic. Customer Update packages can be downloaded through Skoda/VW/SEAT website, security measures cannot be known to Panasonic. The user or installer cannot modify the content. All Installation &amp; update proceeds automatically once user accepts to update and install.</p>
	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?	<p>The channel/mode and associated power allocation are defined in a product specific country code regulatory parameter.</p> <p>The power levels and regulatory domain used by the wireless module are defined based upon Taiwan certification. This regulatory domain is specific to this custom designed wireless module and only to specific customers/host integrators. The Skoda/VW/SEAT are responsible for the domain programming of the wireless module during manufacturing process and configuring their systems. Skoda/VW/SEAT agrees to the terms of the Letter of Authorization which explicitly</p>

		<p>states that they will not change critical regulatory parameters (e.g. regulatory domain). To ensure compliance with local regulations, the device will be set to a single sku country domain that is compliant in the countries to which it ships. All parameters approved by the Taiwan regulatory are programmed in OTP or in both driver and firmware which would be embedded</p> <p>Available to final user via HMI:</p> <ul style="list-style-type: none"> <li>- SSID</li> <li>- PSK</li> <li>- channel</li> <li>- channel width</li> </ul> <p>Hypothetically could be changed:</p> <ul style="list-style-type: none"> <li>- Short Guard Interval - not available to user, only via Factory Inspection Commands</li> <li>- hidden SSID - not available to final user</li> </ul>
	<p>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.</p>	<p>This is a Limited approval for specific customers and hosts. The software version is distributed to the host integrators as a pre-built binary driver preventing any end user modifications. The Firmware/SROM/Flash is released to the host integrator /wireless module CM in Agile so it is a controlled release. Further to this the regulatory domain is programmed at the CM wireless module factory using an internal manufacturing tool. The internal manufacturing tool that is used to program the module's regulatory domain during the manufacturing process is proprietary and is not distributed to end-users.</p> <p>The firmware binaries are protected against modification by encryption of the binaries and checksum calculation stored in the respective metafile in the package. Metafiles modification is protected by main checksum calculation and stored in the package itself in the main metafile, main metafile checksum calculation is protected by package signature.</p> <p>The signature process is based on RSA 3072bits algorithm.</p> <p>The checksum calculation is based on SHA256 algorithm</p>
	<p>4. Describe in detail any encryption methods used to support the use of legitimate RF-related software/firmware.</p>	<p>Firmware binaries in the update package are encrypted using AES 128 algorithm.</p>
	<p>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?</p>	<p>There is a country code regulatory parameter to limit product to operate the device under its authorization in Taiwan. This regulatory parameter would define which channel would be available to operate in active or passive scan to meet UNII requirements.</p> <p>The device would be set as a client device on all channels but also support P2P group owner mode on the non-DFS bands only.</p>

	<b>Requirement</b>	<b>Answer</b>
<b>Third Party Access Control</b>	1. Explain if any third parties have the capability to operate a U.S./Canada -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./Canada.	Regulatory restrictions - can be changed via access to command line (which is not available after production at all), via special ODIS tool (also not available to general public), and via Customer Update of WIFI driver & firmware (which include DB of regulatory restrictions)
	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./Canada. 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 or firmware installation is not allowed, only Panasonic generated update packages signed by Skoda/VW/SEAT are accepted by the unit.
	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.	There is an identifier in the BIOS of the host (PC model) that the driver keys off to ensure that the correct SKU is selected for the card in that particular host. This verifies the adaptor's regulatory domain to ensure a match during the production process and is another mechanism in place to ensure that the regulatory configuration of the module in the shipping systems is correct. This is an internal Pass/Fail confirmation to ensure that the correct card is being installed in the host. The mechanism has no means of changing the regulatory configuration.

This section is required for devices which have a “User Interface” (UI) to configure the device in a manner that may impact the operational parameter. The operation description must address if the device supports any of the country code configurations or peer-peer mode communications discussed in KDB 594280 D01.

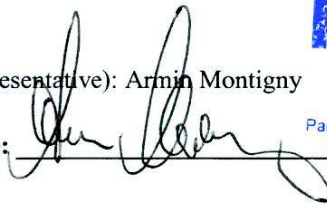
<b>SOFTWARE CONFIGURATION DESCRIPTION</b>		
	<b>Requirement</b>	<b>Answer</b>
<b>USER CONFIGURATION GUIDE</b>	1. Describe the user configurations permitted through the UI. If different levels of access are permitted for professional installers, system integrators or end-users, describe the differences.	User: - on/off - SSID - PSK  Engineering Menu: (only in current power cycle, not available to consumer) - frequency (channel), only ones allowed by current country regulatory - channel width in 5GHz band
	a) What parameters are viewable and configurable by different parties?	User: - on/off - SSID - PSK  Engineering Menu: (only in current power cycle, not available to consumer) - frequency (channel), only ones allowed by current country regulatory - channel width in 5GHz band
	b) What parameters are accessible or modifiable by the professional installer or system integrators?	Via ODIS tool or command line (not available to consumer): - default channels and channel widths (which are ignored if not valid) - country - availability of 2.4 or 5 GHz band - availability of WIFI AP at all
	(1) Are the parameters in some way limited, so that the installers will not enter parameters that exceed those authorized?	Yes. Some parameters are programmed in OTP and Wi-Fi driver and firmware are embedded in system firmware, installer cannot access them. The system firmware is programmed and protected in flash memory. The professional installer/end-user cannot access the flash memory.
	(2) What controls exist that the user cannot operate the device outside its authorization in the U.S./Canada?	There is a country code regulatory parameter to limit user to operate the device outside its authorization in Taiwan.
	c) What parameters are accessible or modifiable by the end-user?	End-use only could select which master to connect (SSID & PSK).
	(1) Are the parameters in some way limited, so that the user or installers will not enter parameters that exceed those authorized?	Yes. Some parameters are programmed in OTP and wifi driver and firmware are embedded in system firmware, installer cannot access them. The system firmware is programmed and protected in flash memory. The professional installer/end-user cannot access the flash memory.
	(2) What controls exist so that the user cannot operate the device outside its authorization in the U.S./Canada?	There is a country code regulatory parameter to limit product to operate the device outside its authorization in the Taiwan.
	d) Is the country code factory set? Can it be changed in the UI?	The country code is set during manufacturing configuration in the factory and cannot be changed in UI.

	(1) If it can be changed, what controls exist to ensure that the device can only operate within its authorization in the U.S./Canada?	The country code cannot be changed.
	e) What are the default parameters when the device is restarted?	- on/off - same as before restart - SSID - same as before restart - PSK - same as before restart
	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, function is 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 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?	No. End-use cannot configure the wifi device to be as a master or client.
	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)).	Cannot have different types.

Name and surname of applicant (or authorized representative): Armin Montigny

Date: 15/08/2019

Signature:



**Panasonic**  
AUTOMOTIVE

Panasonic Automotive Systems Europe GmbH  
Robert-Bosch-Str. 27-29, 63225 Langen