TOPPOWER

Jiangsu Toppower Automotive Electronics Co.,Ltd 江苏天宝汽车电子有限公司

Federal Communications Commission 2019-10-15
Oakland Mills Road
Columbia MD 21046
Model： ZS11E, ZS11MCE3
FCC ID: 2AFIXISMART
Product name:ISMART1.0

Subject: Software security requirements for U-NII device.
The information within this section of the Operational Description is to show compliance against the Software Security Requirements laid out within KDB 594280 D02 U-NII Device Security v01r03.

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.	The user or installer cannot modify the software/firmware contect. FW version will only be deployed over the air. The cloud platform can push a new firmware version to the device when it is available.
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?	WiFi channel area code ID is only set in factory, all RF parameters (include Frequency range, transmitter output power etc.) cannot be access by the user.
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 programmed at the factory and cannot be modified by third parties.
4. Describe in detail the verification protocols in place to ensure that installed software/firmware is legitimate.	The software/firmware is legitmate.
5. Describe in detail any encryption methods used to support the use of legitimate software/firmware.	The firmware is programmed at the factory and cannot be modified by third parties therefore no encryption is necessary.
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?	This is a client device only.
3 rd Party Access Control	
1. 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 party have no the capability.
2. What prevents third parties from loading non-US versions of the software/firmware on the	The firmware is programmed at the factory and cannot be modified by third parties.

device? Describe in detail how the device is protected from "flashing" and the installation of third-party firmware such as DD-WRT.	
3. For Certified Transmitter modular devices, describe how the module grantee ensures that hosts manufactures 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 parameters are not modified outside the grant of authorization.	No applicable
SOFTWARE CONFIGURATION DESCRIPTION	
1. To whom is the UI accessible? (Professional installer, end user, other.)	No UI provided
a) What parameters are viewable to the professional installer/end-user?	No parameters
b) What parameters are accessible or modifiable to the professional installer?	No parameters
i) Are the parameters in some way limited, so that the installers will not enter parameters that exceed those authorized?	Yes
ii) What controls exist that the user cannot operate the device outside its authorization in the U.S.?	Firmware does not provide any interface to user to operate outside its authorization.
c) What configuration options are available to the end-user?	No parameters
i) Are the parameters in some way limited, so that the installers will not enter parameters that exceed those authorized?	Yes
ii) What controls exist that the user cannot operate the device outside its authorization in the U.S.?	Firmware does not provide any interface to user to operate outside its authorization
d) Is the country code factory set? Can it be changed in the UI?	Yes. No.
i) If so, what controls exist to ensure that the device can only operatewithin its authorization in the U.S.?	None
e) What are the default parameters when the device is restarted?	Same as factory set.
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
3. For a device that can be configured as a master	This is a client device

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?	

Best Regards

Name:Guo Fengyuan
Company: Jiangsu Toppower Automotive Electronics Co., Ltd
Address: No. 19 Fenghuang (Phoenix) Avenue, Xuzhou Economic And Technological Development Zone, Jiangsu Province, P. R. China
E-mail: fguo@yfve.com.cn
Tel: +86 (0)516 80567843

Guo Feng Yuan