**BeagleBoard.org Foundation**
4467 Ascot Court, Oakland Township, Michigan, US 48306
Tel: 586-764-1992 Fax: N/A

Federal Communication Commission
Equipment Authorization Division, Application Processing Branch
7435 Oakland Mills Road
Columbia, MD 21046

**2019-07-19**
Attn: Office of Engineering and Technology
Subject: Attestation Letter regarding UNII devices

FCC ID: 2ATUT-BBONE-AI
Software security questions and answers per KDB 594280 D01:

| Software Security description – 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. | We do not release the firmware on our website fordownloading. Our direct host manufacturer (OEM) canrequest the firmware from us and it will be made availablevia secure server. |
| 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? | Radio frequency parameters are limited by US regulatorydomain and country code to limit frequency and transmitpower levels. These limits are stored in non-volatile memoryby the module manufacturer at the time of production. Theywill not exceed the authorized values. |
| 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. | The firmware is installed on each single module duringmanufacturing process. The correct firmware is verified and installed by the module manufacturer.<br>In addition, the firmware binary is encrypted using |

| | | |
|---|---|---|
| | | openSSLencryption and the firmware updates can only be stored innon-volatile memory when the firmware is authenticated.<br>The encryption key is known by the module manufactureronly. |
| 4 | Describe in detail any encryption methods used to support the use of legitimate RF-related software/firmware. | The firmware binary is encrypted. The process to flash anew firmware is using a secret key to decrypt the firmware,only correct decrypted firmware is stored in non-volatilememory (see #3). |
| 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 the compliance by checking theconfigured parameter and operation values according to theregulatory domain and country code in each band. |
| Software Security description – 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. | No, third parties don’t have the capability to access and change radio parameters. US sold modules are factoryconfigured to US. |
| 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 thedevice 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 | Unauthorized firmware is not accepted by the firmwareupdate process. See General Description #5, #3 |

| | | |
|---|---|---|
| | unchanged and how the manufacturer verifies the functionality. | |
| 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. | The module is not available for sale or installation outside ofcompany licensing agreements. Modules are alwaysinstalled in host systems in a factory by end integrators(OEM) responsible for loading authorized software. |
| SOFTWARE CONFIGURATION DESCRIPTION– USER CONFIGURATION GUID | | |
| 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. | The UI is accessible to anyone using the device. |
| | a. What parameters are viewable and configurable by different parties? | Various device status information is made availablelike log information, connection status, operationmode, operation frequency, etc. Radio parameters are described in c.i |
| | b. What parameters are accessible or modifiable by the professional installer or system integrators?<br>i. Are the parameters in some way limited, so thatthe installers will not enter parameters thatexceed those authorized?<br>ii. What controls exist that the user cannot operatethe device outside its authorization in the U.S.? | This device is not subject to professional installation |
| | c. What parameters are accessible or modifiable by the end-user? | The end user is able to configure the operationfrequency, modulation, reduce the output powerlevels etc. The end user cannot |

| | | |
|---|---|---|
| | i. Are the parameters in some way limited, so thatthe user or installers will not enter parameters thatexceed those authorized?<br>ii. What controls exist so that the user cannot operatethe device outside its authorization in the U.S.? | change the antennagain and country code, those settings areprogrammed at factory production time.<br>Yes, the parameters can only be changed within thelimits of country code US.<br>The country code and regulatory domain control dolimit all the parameters set by UI |
| | d. Is the country code factory set? Can it bechanged in the UI?<br>i. If it can be changed, what controls exist to ensure that the device can only operate within its authorization in the U.S.? | The country code is factory set and is neverchanged by UI.<br>The country code is factory set and is neverchanged by UI |
| | e. What are the default parameters when thedevice is restarted? | At each boot up the country code and the antennagain are read from the non-volatile memory, thosevalues are configured during module production. |
| 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 | 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 user controls or user interface operation tochange master/client operation. |
| 4 | For a device that can be configured as different types of access points, such as point-to-point or | The device does not support these |

| | | |
|---|---|---|
| | 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.<br>(See Section 15.407(a)) | modes/features. |

***Dated this*** ***07-19-2019***

***Agency agreement expiration date:*** ***07-18-2020***

***By :*** ***Jason Kridner***
***Signature*** ***Printed***

***Title:*** ***President of the Board***

***On behalf of :*** ***BeagleBoard.org Foundation***

***Telephone*** ***586-764-1992***