Date:10/20/2017
FCC ID:2ALT8GEAC200

# Software Security Description

We, BLOCKSI LLC, hereby declare that requirements of GEAC200 have been met and shown on the following question.

| Software Security Description | |
|---|---|
| **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.<br><br>Description: GEAC200 is a cloud managed access point. It software is pushed by the manufacturer automatically to the router via cloud managed firmware update. End user can not perform software/firmware update. |
| | 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?<br><br>Description:All radio frequency parameters are to be changed by a cloud based interface which is in full control by the manufacturer, Blocksi and which does not exceed the authorized parameters |
| | 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.<br><br>Description: Software/firmware image has a checksum signature that is created by manufacturer. GAEC200 only accepts firmware images with legitimate checksum signatures. Blocksi software is not release to the open source community and can not be modified. |
| | 4. Describe in detail the verification protocols in place to ensure that installed software/firmware is legitimate. |

| | |
|---|---|
| | Description:SHA256 algorithm is used to create a firmware signature. During upgrade process signature is pushed to the GAEC200 and when image is obtained GAEC200 runs SHA256 function, creates local hash and compare it against obtained checksum signature. If there is match upgrade is performed otherwise image gets refused. |
| | 5. Describe in detail any encryption methods used to support the use of legitimate software/firmware.<br><br>Description: SHA256 checksum algorithm is used to assure firmware image integrity |
| | 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?<br><br>Description: GEAC200 can not act as a client, it can act only as a master. |
| **Third-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.<br><br>Description: Only user that purchased GAEC200 can operate device. Device radio settings are lock to the location and regulatory domain using IP geolocation service. If device is installed in the USA geolocation sets parameters according to the USA regulatory domain. GAEC200 is a cloud managed device it can be operated outside USA, but radio parameters can not be modified because they are locked to the USA allowed settings. |
| | 2. What prevents third parties from loading non-US versions of the software/firmware on the device? Describe in detail how the device is protected from “flashing” and the installation of third-party firmware such as DD-WRT.<br><br>Description: DDWRT firmware for GAEC200 does not exist. GEAC200 access to OS is protected by login/password authentication. Flashing the hardware requires a specific cable to connect to the PCB and a manufacturer authentication password. |

| | |
|---|---|
| | 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.<br><br>Description:GEAC200 does not support transmitter modular devices. It is one PCB with all component soldered on the PCB |

| **Software Security Description** | |
|---|---|
| **User Configuration Guide** | 1. To whom is the UI accessible? (Professional installer, end user, other.)<br><br>Description: Only a end user cloud based dashboard User Interface is made available to the end user or to a professional installer. GEAC200 is a cloud managed Access point router, that requires to be connected to the internet so that an end user or installer can access the cloud based dashboard so to register it and configure it. |
| | a) What parameters are viewable to the professional installer/end-user?<br><br>Description: Wifi mode (b,g,n,ac) and channels/frequencies in the 2.4Ghz and 5 Ghz bands. User can also set WiFi security parameters like SSID name, encryption protocol, cipher and WiFi key. Other WiFi and radio settings are not supported on GAEC cloud management system.<br>Other settings are used for parental control and content filtering and are not wifi related. |
| | b) What parameters are accessible or modifiable by the professional installer? |

| | |
|---|---|
| | Description: Same as the user one. Professional installer does not have access to more parameter than the end user. Most of the time, the end user is the one to install GEAC 200 by himself. |
| | (1) Are the parameters in some way limited, so that the installers will not enter parameters that exceed those authorized?<br><br>Description:Yes, parameters are limited as per User interface and as per the one authorized. |
| | (2) What controls exist that the user cannot operate the device outside its authorization in the U.S.?<br><br>Description: Only the parameters that are available on the cloud based dashboard, which is under the control of the manufacturer (Blocksi) at all time can be used. User can not use parameters that are not allowed by Blocksi cloud based Dashboard. |
| | c) What parameters are accessible or modifiable to by the end-user?<br><br>Description: Wifi mode (b,g,n,ac) and channels/frequencies in the 2.4Ghz and 5 Ghz bands. User can also set WiFi security parameters like SSID name, encryption protocol, cipher and WiFi key. Other WiFi and radio settings are not supported on GAEC cloud management system.<br>Other settings are used for parental control and content filtering and are not wifi related. |
| | (1) Are the parameters in some way limited, so that the installers will not enter parameters that exceed those authorized?<br><br>Description:Only the parameters that are available on the cloud based dashboard, which is under the control of the manufacturer (Blocksi) at all time can be used. User can not use parameters that are not allowed by Blocksi cloud based Dashboard. |
| | (2) What controls exist that the user cannot operate the device outside its authorization in the U.S.?<br><br>Description:Only the parameters that are available on the cloud based dashboard, which is under the control of the manufacturer |

| | |
|---|---|
| | (Blocksi) at all time can be used. User can not use parameters that are not allowed by Blocksi cloud based Dashboard. WiFi related parameters are locked according to the device location obtained via IP geolocation service. |
| | d) Is the country code factory set? Can it be changed in the UI?<br><br>Description:Country code is factory set to USA. When device is connected to the internet and registered country code is set according to the IP geolocation service and can not be modified. |
| | (1) If so, what controls exist to ensure that the device can only operate within its authorization in the U.S.?<br><br>Description: GEAC200 is a cloud managed router through a cloud based portal. GEAC200 is geolocalized and from there the user interface restrict the country configurable parameter to the country the GEAC200 is located in. |
| | e) What are the default parameters when the device is restarted?<br><br>Description: When device is restarted it downloads the user parameters stored in the cloud. There is no default parameters except when the customer first install the GEAC200. There is no way to restore to default settings unless a specific procedure to factory default is processed (press the reset button for more than 10 sec). WiFi Country Code is by default set to USA. |
| | 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.<br><br>Description: Radio can NOT be configured in bridge or 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?<br><br>Description: GEAC200 can act only as a master |

| | |
|---|---|
| | 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))<br><br>Description:GEAC200 can act only as a master. |

If any questions regarding this declaration, please don't hesitate to contact us.

Sincerely

____Fouad BAHOU_____
(Signature/Title)

BLOCKSI LLC Fouad BAHOU

## Certificate Of Completion

Envelope Id: C8F16745CC2E425297F70A4988CC4298
Status: Completed
Subject: GEAC200 Software security question for FCC certification
Source Envelope:
Document Pages: 6
Signatures: 1
Envelope Originator:
Certificate Pages: 1
Initials: 0
Fouad BAHOU
AutoNav: Enabled
fbahou@block.si
EnvelopeId Stamping: Disabled
IP Address: 162.248.185.11
Time Zone: (UTC-08:00) Pacific Time (US & Canada)

## Record Tracking

Status: Original
11/20/2017 2:09:30 AM
Holder: Fouad BAHOU
fbahou@block.si
Location: DocuSign

| Signer Events | Signature | Timestamp |
|---|---|---|
| Fouad BAHOU<br>fbahou@block.si<br>Blocksi<br>Security Level: Email, Account Authentication (None) | Fouad BAHOU<br>Using IP Address: 69.193.94.124 | Sent: 11/20/2017 2:09:31 AM<br>Viewed: 11/20/2017 2:10:17 AM<br>Signed: 11/20/2017 2:19:07 AM<br>Freeform Signing |

**Electronic Record and Signature Disclosure:**
Not Offered via DocuSign

| In Person Signer Events | Signature | Timestamp |
|---|---|---|

| Editor Delivery Events | Status | Timestamp |
|---|---|---|

| Agent Delivery Events | Status | Timestamp |
|---|---|---|

| Intermediary Delivery Events | Status | Timestamp |
|---|---|---|

| Certified Delivery Events | Status | Timestamp |
|---|---|---|

| Carbon Copy Events | Status | Timestamp |
|---|---|---|

| Notary Events | Signature | Timestamp |
|---|---|---|

| Envelope Summary Events | Status | Timestamps |
|---|---|---|
| Envelope Sent | Hashed/Encrypted | 11/20/2017 2:09:31 AM |
| Certified Delivered | Security Checked | 11/20/2017 2:10:17 AM |
| Signing Complete | Security Checked | 11/20/2017 2:19:08 AM |
| Completed | Security Checked | 11/20/2017 2:19:08 AM |

| Payment Events | Status | Timestamps |
|---|---|---|