TUV SUD BABT UNLIMITED
Octagon House,
Segensworth North,
Fareham, Hampshire,
PO15 5RL, United Kingdom
FCC ID: 2AEBL-H8249
IC: 20060-H8249
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.	There is no downloadable software provided by the manufacturer that can modify critical radio transmitter parameters. All critical parameters are programmed in OTP memory at the factory and cannot be modified by third parties.
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?	There are no RF parameters that can by modified. All RF parameters are programmed in OTP memory at the factory and cannot be modified by third parties.
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 NVRAM of the module can only be written once and cannot be written after delivery.
4. Describe in detail the verification protocols in place to ensure that installed software/firmware is legitimate.	The NVRAM of the module can only be written once and cannot be written after delivery.
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 can only act as client mode. The device cannot act as a master in all bands
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 are not approved to operate in any manner that is violation of the certification in the U.S.

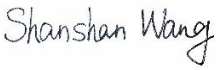
2. Describe, if the device permits third-party software or firmware installation, what mechanisms are provided by the manufacturer to permit integration of such functions while ensuring that the RF parameters of the device cannot be operated outside its authorization for operation in the U.S. In the 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.	The firmware is programmed at the factory and cannot be modified by third parties.
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.	Default mode is always FCC compliant, and the NVRAM of the module can only be written once and cannot be written after delivery.

SOFTWARE CONFIGURATION DESCRIPTION	
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.	Professional installer and end users
a) What parameters are viewable and configurable by different parties?	Wireless network
b. What parameters are accessible or modifiable by the professional installer or system integrators?	Connection to specific wireless network.

(1) Are the parameters in some way limited, so that the installers will not enter parameters that exceed those authorized?	The module micro-code reads the parameters from the Module OTP memory. These parameters cannot be modified by SW driver.
(2) What controls exist that the user cannot operate the device outside its authorization in the U.S.?	Default mode is always FCC compliant. Other country modes cannot be activated without writing in the drive's bin files. However, bin files can only be modified at the factory
c. What parameters are accessible or modifiable by the end-user?	Wireless network names, encryption methods, and wireless network passwords.
1) Are the parameters in some way limited, so that the user or installers will not enter parameters that exceed those authorized?	The module micro-code reads the parameters from the Module OTP memory. These parameters cannot be modified by SW driver.
2) What controls exist so that the user cannot operate the device outside its authorization in the U.S.?	Default mode is always FCC compliant. Other country modes cannot be activated without writing in the drive's bin files. However, bin files can only be modified at the factory
d. Is the country code factory set? Can it be changed in the UI?	Default country code is set in the factory and 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.?	N/A
e. What are the default parameters when the device is restarted?	Always FCC compliant.
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 and client (with active or passive scanning), if this is user configurable, describe what controls exist, within the UI, to ensure	The device can only act in client mode. The device cannot act as a master in all bands.

compliance for each mode. If the device acts as a master in some	
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))	Not support

Best Regards

Signature: 

Contact name: Testing & Laboratory Specialist / Shanshan, Wang
Company name: ABB Xiamen Smart Technology Co., Ltd.
Address: 4th Floor, No. 881, FangShanXiEr Road, Xiang'An Industrial Area, Torch Hi-Tech Industrial Development Zone, 361000 Xiamen S.E.Z, Fujian Province, PEOPLE'S REPUBLIC OF CHINA
E-mail: sylvia-shanshan.wang@cn.abb.com
Tel: 0592-7616016