BABT FCB

Balfour House,

Churchfield Road,

Walton-on-Thames,

Surrey,

KT12 2TD

Date: 06/20/2016.

Software Security Description – KDB 594280 D02v01r02 Section II

General Description

1. 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 or overridden by third parties.	The software/firmware update is bundled, as part ofthe handset software update, and the user or installer cannot modify the content. The installation and/or update proceeds automatically once the useraccepts to install/update the software/firmware.
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?	The Software/Firmware in the device, controls the following RF parameters: 1. Transmitter Frequency 2. Transmitter Output Power 3. Receiver Frequency 4. Channel Bandwidth 5. RSSI calibration The Software/Firmware controls the RF parameters listed above so as to comply with the specific set of regulatory limits in accordance with the FCC grants issued for this device. The RF parameters are limited to comply with FCC rules and requirements during calibration of the device in the factory. Security keys (certificationcertificates) are in place to ensure that these parameters cannot be access by the User and/or a 3rd party.
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	software is digitally and encrypted using proprietary handshaking authorization and provisioning protocols
4. Describe in detail the verification protocols in place to ensure that installed software/firmware is legitimate.	software is digitally and encrypted using proprietary handshaking authorization and provisioning protocols
5. Describe in detail any encryption methods used to support the use of legitimate	Software/firmware is not encrypted.

software/firmware.	
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?	NA. this device is a client-only device.

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.	Third parties do not the capability to operate in any manner that is violation of the certification in the U.S.
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.	3rd party cannot access SW/FW
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.	Not applicable – this is not a modular device

SOFTWARE CONFIGURATION DESCRIPTION – KDB 594280 D02v01r02 Section III

USER CONFIGURATION GUIDE

1. To whom is the UI accessible? (Professional installer, end user, other.)	NA
a) What parameters are viewable to the professional installer/end‐user?	NA
b) What parameters are accessible or modifiable to the professional installer?	NA
i) Are the parameters in some way limited, so that the installers will not enter parameters that exceed those authorized?	NA
ii) What controls exist that the user cannot operate the device outside its authorization in the U.S.?	NA
c) What configuration options are available to the end‐user?	NA
i) Are the parameters in some way limited, so that the installers will not enter parameters that exceed those authorized?	NA
ii) What controls exist that the user cannot operate the device outside its authorization in the U.S.?	NA

d) Is the country code factory set? Can it be changed in the UI?	NA
i) If so, what controls exist to ensure that the device can only operate within its authorization in the U.S.?	NA
e) What are the default parameters when the device is restarted?	NA
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	NA
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?	NA
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))	NA

Name: John Mark Harrison

Title: Head of Product Compliance and Certification

Telephone Number: +44 1254 290630

Email: bryan.lofthouse@prometheanworld.com