Hewlett-Packard Company

1501 Page Mill Road, Palo Alto, California 94304, USA

May 07, 2015

Attestation letter
(SW Security Ops Description Per KDB 594280 D02)

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.
	Over The air 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?
	Radio parameters are fixed at time of production as required by the FCC certification. Any future software/Firmware release is verified by the module maker before release. If required, module maker will follow FCC permissive change procedure, and no RF parameter will be modifying after SW upgrade.
	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.
	Yes, Software/Firmware is digitally signed with Windows WHQL authorization and provisioning protocols,
	4. Describe in detail the verification protocols in place to ensure that installed software/firmware is legitimate.
	Yes, only can download SW/FW via Windows update server with WHQL digital signature.
	5. Describe in detail any encryption methods used to support the use of legitimate software/firmware
	Yes, Windows WHQL digital signature.
	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?
	No applicable, this device is a client-only device.

3rd 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, please refer to answer to #2, #3 #4 and #5 under General Description. This is locked into the manufacturing data and cannot be changed even product be brought to others country.
	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.
	The non-US version software can't upload via user interface or OTA that SW/FW only can download with Windows WHQL digital signature. This device installs with Windows, and the system protects itself with WHQL digital signature; therefore, users could not download any third-party firmware to flash the device.
	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 device is not a module device.

User Configuration guide	1. To whom is the UI accessible? (Professional installer, end user, other.)
	The UI is accessible to the end user.
	a)What parameters are viewable to the professional installer/end-user?
	The end user only can view RF channel
	b)What parameters are accessible or modifiable by the professional installer?
	The RF channel can only be set to FCC approved channels.
	(1) Are the parameters in some way limited, so that the installers will not enter parameters that exceed those authorized?
	Yes, all radio parameters are limited by SW settings pre-determine by the FCC radio regulatory approval process.
	(2) What controls exist that the user cannot operate the device outside its authorization in the U.S.?
	Yes, the radios are configured at manufacturing to be US only.
	c) What parameters are accessible or modifiable to by the end-user?
	No, All parameters are configured at manufacturing and canot modify via UI.
	(1) Are the parameters in some way limited, so that the installers will not enter parameters that exceed those authorized?
	Yes, all radio parameters are limited by module maker and pre-determine by the FCC radio regulatory approval process.
	(2) What controls exist that the user cannot operate the device outside its authorization in the U.S.?
	Yes, the radios are configured at manufacturing to be US only.
	d) Is the country code factory set? Can it be changed in the UI?
	Yes, the country code is factory set, it cannot be changed by user interface.
	(1) If so, what controls exist to ensure that the device can only operate within its authorization in the U.S.?
	The radio are configured at manufacturing to be US only and cannot modify via UI
	e) What are the default parameters when the device is restarted?
	The device goes to a default (approved) TX channel and power level base on factory country setting
	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 applicable,
	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 applicable, this device is a client-only device.
	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 applicable,

Walter Overcash
Product Regulator Engineer
281-514-2756
Walter.overcash@hp.com

Hewlett-Packard Company

Company Address: 1501 Page Mill Road, Palo Alto, California 94304, USA

Date: 2015/05/12

DTS-UNII Device Declaration Letter

To whom it may concern:
We have declared below featured for FCC equipment authorization,

Device FCC ID: B94HNQ93CSPN / B94HNQ93CSPNWR / B94HNQ93CSPNAC

(1) DFS Device -- ☐ Master , ☐ Client with Radar detection capability ,
☑ Client without radar detection capability, ☐ N/A

(2) Active / Passive Scanning , adhoc mode access point capability

Frequency Band (MHz)	Active Scanning (the device can transmit a probe (beacon))	passive scanning (where the device is can listen only with no probes)	Ad Hoc Mode or WIFI Direct capability	Access point capability
2412 - 2462MHz	☐ Yes , ☑ No	☑ Yes , ☐ No	☐ Yes , ☑ No	☐ Yes , ☑ No
5150 - 5250MHz	☐ Yes , ☑ No	☑ Yes , ☐ No	☐ Yes , ☑ No	☐ Yes , ☑ No
5250 - 5350MHz	☐ Yes , ☑ No	☑ Yes , ☐ No	☐ Yes , ☑ No	☐ Yes , ☑ No
5470 - 5725MHz	☐ Yes , ☑ No	☑ Yes , ☐ No	☐ Yes , ☑ No	☐ Yes , ☑ No
5725 - 5850MHz	☑ Yes , ☐ No	☐ Yes , ☑ No	☐ Yes , ☑ No	☐ Yes , ☑ No

(3) Country code selection ability - ☐ Yes , ☑ No
If yes, pls explain how it was implemented : (pls also help to provide detail of options for each country selection)

(4) Meet 15.202 requirement - ☑ Yes , ☐ No ,
pls check below :
☐A master device is defined as a device operating in a mode in which it has the capability to transmit without receiving an enabling signal. In this mode it is able to select a channel and initiate a network by sending enabling signals to other devices
☑A client device is defined as a device operating in a mode in which the transmissions of the device are under control of the master. A device in client mode is not able to initiate a network…

(5) For client devices that have software configuration control to operate in different modes (active scanning in some and passive scanning in others) in different bands (devices with multiple equipment classes or those that operate on non-DFS frequencies) or modular devices which configure the modes of operations through software, the application must provide software and operations description on how the software and / or hardware is implemented to ensure that proper operations modes can not be modified by end user or an installer.
☑ Apply , "Yes , please see SW security Description". ☐ No Apply , (If apply , pls help to provide explanation on it was implement , and how software was controlled)

Name / Title: Walter Overcash / Product Regulator Engineer

Signature:

Address: 1501 Page Mill Road, Palo Alto, California 94304, USA