Software Security Requirements Cover Letter

Refer to KDB 594280 D02 U-NII Device Security v01r03.

The applicant has response some questions as below, which can clearly demonstrate how the device meets the security requirements

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
	Response: User can contact a Honeywell technical support representative for information on available software/firmware upgrades
	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?
	Response: The radio frequency parameters are fixed at the time of production. Any future software/firmware release is verified by Honeywell before release. If required, Honeywell will follow FCC permissive change procedure
	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
	Response: The software/firmware and update package are digitally signed and encrypted using proprietary handshaking, authorization and provisioning protocol
	4. Describe in detail any encryption methods used to support the use of legitimate RF-related software/firmware.
	Response: The encryption using proprietary internal software
	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?
	Response: Not applicable, this device is a client-only device

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.
	Response: No, only Honeywell can release or mark changes to the software/firmware using proprietary secure protocol
	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
	Response: Honeywell proprietary hardware platform software tools and proprietary protocol are required to replace firmware. No 3rd party can access to change firmware on device
	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.
	Response: This device is not a module

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.
	Response: End-users can do the configuration except RF power and operation frequency. There is no different level permitted
	a) What parameters are viewable and configurable by different parties?
	Response: 802.11d can be enable/disable etc. except RF power and operation frequency
	b) What parameters are accessible or modifiable by the professional installer or system integrators?
	Response: This device is not subject to professional installation
	1) Are the parameters in some way limited, so that the installers will not enter parameters that exceed those authorized?
	Response: All above parameters have pre-defined range according to

	the certification test result. They are stored in the ROM, which not allow installers to adjust beyond there-set value
	2) What controls exist that the user cannot operate the device outside its authorization in the U.S.?
	Response: Both RF power and operation frequency are permanent setting in the ROM., it cannot be changed by end users
	c) What parameters are accessible or modifiable by the end-user?
	Response: The parameters related to RF characteristics and compliance are not accessible to end users
	1) Are the parameters in some way limited, so that the user or installers will not enter parameters that exceed those authorized?
	Response: 802.11d can be enable/disable etc. except RF power and operation frequency
	2) What controls exist so that the user cannot operate the device outside its authorization in the U.S.?
	Response: The parameters related to RF characteristics and compliance are not accessible to end users
	d) Is the country code factory set? Can it be changed in the UI?
	Response: No, the country code is factory set and cannot be changed by UI
	1) If it can be changed, what controls exist to ensure that the device can only operate within its authorization in the U.S.?
	Response: Both RF power and operation frequency are permanent setting in the ROM., it cannot be changed by end users
	e) What are the default parameters when the device is restarted?
	Response: Both RF power and operation frequency are permanent setting in the ROM., it cannot be changed by end users
	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.
	Response: 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 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?
	Response: Not 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))

	Response: Not applicable