SOFTWARE SECURITY FOR U-NII DEVICES

Date: 27 October 2016

FCC ID: TYM-J129

IC: 3794C-J129

Pursuant to FCC Part 15E 15.407(i) and KDB 594280 D02 U-NII Device Security, applicant must describe the overall security measures and systems that ensure that only:

1. Authenticated software is loaded and operating the device.
2. The device is not easily modified to operate with RF parameters outside of the authorization

The description of the software must address the following questions in the operational description for the device and clearly demonstrate how the device meets the security requirements.

SOFTWARE SECURITY DESCRIPTION	
General Description	1. Q: 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. A: Software to the card is never updated; device software is digitally signed and obtained from Avaya website, device authenticate the software by validating the signature using pre-install trust certificate..
	2. Q: 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? A: Only authorized parameters are available and can be set in software, like changing the band.
	3. Q: 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. A: The Avaya software runs a load validation during the software upgrade process to ensure that the software is legitimate, unaltered and downloaded correctly. Software image is digest using SHA256 and signed using digital certificates (2048 key length) which is authenticated using pre-installed in root CA. RFS (Root file system) of the device (Avaya phone) is read-only.

	4. Q: Describe in detail the verification protocols in place to ensure that installed software/firmware is legitimate. A: The Avaya software runs a load validation before the software upgrade process to ensure that the software is legitimate, unaltered and downloaded correctly. Software image is digest using SHA256 and signed using digital certificates (2048 key length) which is authenticated using pre-installed in root CA.
	5. Q: Describe in detail any encryption methods used to support the use of legitimate software/firmware. A: Software is not encrypted, only signed.
	6. Q: 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? A: The device is only a client.
Third-Party Access Control	1. Q: 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. A: Device can only be controlled by Avaya software. Third party software cannot control the device.
	2. Q: 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. A: Only software signed by Avaya can be installed, as a result, only Avaya software can be loaded.
	3. Q: 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. A: Parameters are stored in the WiFi module. These parameters are based on country/region code. Driver software (using cfg80211) can set requested country/code into WiFi modules firmware. Based on set country/region code corresponding regulatory domain is activated in WiFi module. Only application administer level user (with password protected settings file) have ability to set the country/region code. For RF tests purpose only (not a part of production software), WiFi modules can be loaded with special firmware in which manufacturer mode is enabled. To enable this mode, Authorized debug feature control file needs to be generated and installed on the phone to get a console access. Once WiFi modules are loaded with special firmware, a special test tool (Labtool) running on PC can communicate with Avaya phone over Ethernet and can set/get regulatory domain parameters like RF channel, data rate, Band etc. When WiFi modules are loaded with special firmware (manufacturer mode enabled), it can perform regular WiFI operations like scan, connect etc.

SOFTWARE CONFIGURATION DESCRIPTION GUIDE	
USER CONFIGURATION GUIDE	1. Q: To whom is the UI accessible? (Professional installer, end user, other.) A: End user and Professional Installer (Advance configurations such as setting a country/region code are accessible to only Admin users, with password protected settings file)
	a) Q: What parameters are viewable to the professional installer/end-user? A: Disable/Enable Wi-Fi, viewing available network, connect/disconnect and forget.
	b) Q: What parameters are accessible or modifiable by the professional installer? A: Disable/Enable Wi-Fi, viewing available network, connect/disconnect and forget. Authorized professional installer can set country only by changing a password

	protected setting file
	i) Q: Are the parameters in some way limited, so that the installers will not enter parameters that exceed those authorized? A: Authorized progression installer can only modify the country by changing a password protected setting file. Authorized user cannot modify parameter in any other way.
	ii) Q: What controls exist that the user cannot operate the device outside its authorization in the U.S.? A: User cannot change any setting to unauthorized parameters (Admin can change only country/region code and regulatory domain is selected internally in WiFi module)
	c) Q: What parameters are accessible or modifiable to by the end-user? A: None, the user can only enable/disable Wi-Fi, view available network connect/disconnect from specific network and forget a network
	i) Q: Are the parameters in some way limited, so that the installers will not enter parameters that exceed those authorized? A: Authorized professional installer can set country only by changing a password protected setting file. User cannot change any setting to unauthorized parameters
	ii) Q: What controls exist that the user cannot operate the device outside its authorization in the U.S.? A: There are no parameters that user can change.
	d) Q: Is the country code factory set? Can it be changed in the UI? A: Factory set has default country code as Worldwid which is the most restrictive (hence benign) set of frequencies. Country cannot be set from the user visible UI. Only password protected setting file by authorized professional installer.
	i) Q: If so, what controls exist to ensure that the device can only operate within its authorization in the U.S.?

	A: N/A since country cannot be changed from UI, only password protected setting file by authorized professional installer.
	e) Q: What are the default parameters when the device is restarted? A: After reset device boot with previous/default parameters
	2. Q: 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. A: No
	3. Q: 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? A: N/A. Device is operating in client mode only
	4. Q: 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)) A: N/A. Device is operating in client mode only