Software Security Requirements For U-NII Devices

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.

   Ans:

   (a) It will be obtained by the factory : ☒ Yes ☐ No

   (b) It will be downloaded by ODM website : ☒ Yes ☐ No

   (c) It will be installed by user : ☒ Yes ☐ No

   For download , SW updates are available from Amped wireless on the secure support web site. Users need to login with security credentials to access the SW update. For the authentication / verification protocols, the Amped wireless firmware is unique frame format and composed by symbols. There are three parts of symbols in one frame. First part is "product code" for each Amped wireless product , second part is "address" to record which partition of flash will be loaded for this data of frame. Third part is data. All information is recorded in source code. The firmware is compiled by Amped wireless source code and coding to execution file which can't be reversed to source code . So there is no chance for others than Amped wireless to modify the firmware to create un-authentication firmware for product.

2. Describe the RF parameters that are modified by any software/firmware without any hardware changes.
   Ans: SW can modify all parameters except for (a) radio calibration data to ensure Tx power (Transmit power) accuracy is maintained,(b) maximum transmit power limits established during product certification are not exceeded under each mode and each channel, and (c) Country code setting to indicate "FCC" regulatory region. Parameters that limit items a) and b) are contained in Read Only Memories in the radio drivers and (c) in the flash memory of the product only accessable by factory software.

   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?

   Ans: The firmware has been compiled as binary file. It couldn't change the setting RF parameter through this binary file. It is read-only without change.

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.

   Ans: Any software that is loaded on the device is verified to ensure that its cryptographic signature matches Amped wireless public-private keypair. Only if the signature matches is the software

loaded onto the device.

4. Describe in detail any encryption methods used to support the use of legitimate RF-related software/firmware.

   Ans: The verification protocols are based on standard Public Key encryption (RSA, 2048bit length signing keys, and SHA256 for digest)

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?

   Ans: This device cannot be configured as a master and client.

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.

   Ans: ☐ Yes ☒ No

   The RF parameters is put in read-only partition of EUT's flash and is only installed by the factory. RF parameters: power settings, antenna types or country code settings will be locked in this partition.

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.

   Ans: The model information is built in the firmware. When the firmware upgrade is performed, CPE checks if the model information between old and new firmware is equal. If model information is not equal, the firmware upgrade cannot be performed.

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.

   Ans: This is not module device.

SOFTWARE CONFIGURATION DESCRIPTION GUIDE

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.

   Ans: ☐ Professional installers ☐ System Integrators ☒ End-users

   (a) What parameters are viewable and configurable by different parties?

   Ans:

   ☐ Antenna types ☐ Power settings ☐ Country code

   ☒ Other: Authorized channel, bandwidth, modulation.

   (b) What parameters are accessible or modifiable by the professional installer or system integrators?

   Ans: This is not professional install device.

   (1) Are the parameters in some way limited, so that the installers will not enter parameters that exceed those authorized?

   Ans: This is not professional install or system integrate device.

   (2) What controls exist that the user cannot operate the device outside its authorization in the U.S.?

   Ans: This is not professional install or system integrate device.

   (c) What parameters are accessible or modifiable by the end-user?

   Ans:

   ☐ Antenna types ☐ Power settings ☐ Country code

   ☒ Other: Authorized channel, bandwidth, modulation.

   (1) Are the parameters in some way limited, so that the user or installers will not enter parameters that exceed those authorized?

   Ans: ☒ Yes ☐ No

   (2) What controls exist so that the user cannot operate the device outside its authorization in the U.S.?

   Ans: The RF parameters in Flash is Read-Only and is obtained by the factory.

RF parameters: power settings, antenna types or country code settings will be locked in this partition.

(d) Is the country code factory set?

Ans: ☒ Yes ☐ No

Can it be changed in the UI?

Ans: ☐ Yes ☒ No

(1) If it can be changed, what controls exist to ensure that the device can only operate within its authorization in the U.S.?

Ans: The country code settings in Flash is Read-Only and is obtained by the factory.

(e) What are the default parameters when the device is restarted?

Ans: Factory default is DEMO country that has commonly allowed channels and transmit power limit in all regulatory domains

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.

Ans: ☒ Yes, the device supports bridge. It could receive WiFi device signal as client device then transmit signal to other by Master device and it is compliant with FCC DFS specification.

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?

   Ans: This device cannot be configured as a master and client.

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))

   Ans: ☐ Yes ☒ No

   This device cannot be configured as different types of access points, such as point-to-point or point-to-multipoint, and use different types of antennas.