SONY
Sony Mobile Communications

Confidential 1(1)

Document number

Revisio
PA7

Prepared by
SEM/CGVFDA SHIMIZU KOICHI

Date
2016-3-21

Contents responsible if other than preparer

Remarks
This document is managed in metaDoc.

Approved by
SEM/CGVFDA SHIMIZU KOICHI

Suzu Technical Description for WLAN Security

1 SOFTWARE SECURITY REQUIREMENTS FOR U-NII DEVICES KDB 594280 D02 U-NII Device Security v01

The information within this section of the Operational Description is to show compliance against the Software Security Requirements laid out within KDB 594280 D02 U-NII Security v01 r03.

The information below describes how we maintain the overall security measures and systems so that only:

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

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.*	Some models have operator-specific OMA DM client. For DM session HTTPS is used to provide confidentiality and to prevent tampering, and OMA DM protocol is used to prevent spoofing which means client and server must be authenticated to each other. For FOTA package download, HTTPS is used and the device makes a request only to the server informed by the server during DM session. The other models have SOMC download client. To obtain information of available update, HTTPS is used to provide confidentiality and to prevent tampering, and the manifest has a SOMC signature to confirm legitimacy of the information carried in the manifest. Before the installation process begins, the device checks the authenticity and integrity of the FOTA package, and checks the update is applicable to the device. SW signing verification is also performed at every device boot up as well. FOTA package consists of deltas which cannot be analyzed and is signed with a SOMC signature. User data is left untouched by the installation.

General Description	
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 any other software/firmware changes will not allow the device to exceed the authorized RF characteristics?	The product in market uses different type of software, which have mechanism which only a licensed driver or FW can be updated. Thus, any compliance related parameters can't be changed by end-users.
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*.	All SW images are digitally signed with public key cryptography. Images are signed by private key stored in securely manged server, and verified by public key stored in a device when they are flashed into the device. Some SW images are verified with the public key when they are executed.
4. Describe, ***in detail***, any encryption methods *used to support the use of legitimate RF-related software/firmware.*	Software/firmware is not encrypted.
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?	'- The device is evaluated in each band as a client and as a master and complies with all applicable rules. - Maximum output power is the same regardless of whether it functions as master or client. - The operation mode is as follow. Please refer to technical description page#9 for detail. 2.4G : Master mode operation / Hotspot, Wi-Fi Direct(GO/GC) W52/58 : Master mode operation / Hotspot, Wi-Fi Direct(GO/GC) W53/56 : Client mode operation / Wi-Fi Direct (GO※/GC) ※If an AP beacon is in those Bands, DUT could work as Wi-Fi Direct GO mode. (listen only mode)

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 may allow the device to operate in violation of the device's authorization if activated in the U.S..*	SW update can be done by over the air or PC tool. All SW images are digitally signed with public key cryptography. Images are signed by private key stored in securely manged server, and verified by public key stored in a device when they are flashed into the device.
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.	The device does not permit third-party to install a software or firmware. SW signing verification is performed at every device boot up.
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*[1]	Not applicable

[1] Note that Certified transmitter modules must have sufficient level of security to ensure that when integrated into a permissible host the device's RF parameters are not modified outside those approved in the grant of authorization. (See, KDB Publication 99639). This requirement includes any driver software related to RF output that may be installed in the host, as well as, any third party software that may be permitted to control the module. **A full description of the process for managing this should be included in the filing**.

SOFTWARE CONFIGURATION DESCRIPTION – USER CONFIGURATION GUIDE[2]	
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.	None
a) What parameters are viewable and configurable by different parties[3]	None
b) What parameters are accessible or modifiableby the professional installer or system integrators?	None
i) Are the parameters in some way limited, so that the installers will not enter parameters that exceed those authorized?	None
ii) What controls exist that the user cannot operate the device outside its authorization in the U.S.?	Not applicable
c) What configuration options are accessible or modifiable to the end-user?	None
i) Are the parameters in some way limited, so that the user or installers will not enter parameters that exceed those authorized?	Not applicable
ii) What controls exist that the user cannot operate the device outside its authorization in the U.S.?	Not applicable
d) Is the country code factory set? Can it be changed in the UI?	No country code setting
i) If it can be changed, what controls exist to ensure that the device can only operate within its authorization in the U.S.?	Not applicable
e) What are the default parameters when the device is restarted?	Target Power setting, Supported channel table, regulatory limit/scan-type table
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.	The device doesn't provide configured controls of master/client mode to users.
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?	The device doesn't provide configured controls of master/client mode to users.

[2] This section is required for devices which have a "User Interfaces" (UI) to configure the device in a manner that may impact the operational parameter. Supporting information is required in the operational description. The operational description must address if the device supports any of the country code configurations or peer-peer mode communications discussed in KDB 594280 Publication D01.

[3] The specific parameters of interest for this purpose are those that may impact the compliance of the device (which would be those parameters determining the RF output of the device). These typically include frequency of operation, power settings, antenna types, DFS settings, receiver thresholds, or country code settings which indirectly programs the operational parameters.

SOFTWARE CONFIGURATION DESCRIPTION – USER CONFIGURATION GUIDE[2]	
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))	For Wi-Fi Direct operation, there are not available to select master or client mode by user. For Wi-Fi Direct and Hotspot operation, the device can be only activated/deactivated from UI. Only for Hotspot mode, channel selection is available (TBD).