Huawei Technologies Co.,Ltd.

Statement

Federal Communications Commission
Oakland Mills Road
Columbia MD 21046

2015-12-11

Subject: Statement for 5G Wi-Fi™

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 Device Security v01r02.
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

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.	There are two methods of updating the software/firmware on the device and these are either Firmware Over the Air (FOTA) from the User's Service Provider or via a hardware connection to a computer supporting the download client. The download client is a software tool that has to be downloaded from the Huawei web site. Via OTA, the device has to be powered on and in Idle mode, registered with the Users Service provider. The User is informed that there is a new software/firmware version available, the option to update the software/firmware is selected then the download commences without any user intervention as all authentication is done directly between the device and the Service Provider. The user is then requested to power cycle the device to active the newly installed SW. Via the download client, the device is to be initially recognized by the download client as being an authentic device via the correct authentication certificates held on the device. The User is then advised of the Software/Firmware updates that are available for download to their device. The User requests the necessary updates and the Software/Firmware is

	downloaded to the device without any further User intervention as all authentications is carried out between the certificates held on the device and the download client. As part of the Software/Firmware update, the device power cycles so that is ready for the User to disconnect from the download Client and continue using.
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?	The Software/Firmware in the device, controls the following RF parameters: 1. Transmitter Frequency 2. Transmitter Output Power 3. Receiver Frequency 4. Channel Bandwidth 5. RSSI calibration The Software/Firmware controls the RF parameters listed above so as to comply with the specific set of regulatory limits in accordance with the FCC grants issued for this device. Yes. The RF parameters are limited to comply with FCC rules and requirements during calibration of the device in the factory. Security keys (certification certificates) are in place to ensure that these parameters cannot be access by the User and/or a 3rd party
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.	All software images are digitally signed with public key cryptography. Images are signed by private key stored in securely merged 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 the verification protocols in place to ensure that installed software/firmware is legitimate.	The same as General Description Q3
5. Describe in detail any encryption methods used to support the use of legitimate software/firmware.	Software/firmware is not encrypted.
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?	This handset will only operate as a master device in hot spot mode and in Wi-Fi direct mode, both of which are limited to the 2.4GHz band on channels 1 – 11 only. This device can only be configured as a client in all UNII bands where it operates using passive scanning techniques.
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.	3rd party does not have the capability

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.[6]	3rd party cannot access SW/FW
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.[7]	NA
SOFTWARE CONFIGURATION DESCRIPTION	
1. To whom is the UI accessible? (Professional installer, end user, other.)	NA
a) What parameters are viewable to the professional installer/end-user?[6]	NA
b) What parameters are accessible or modifiable to the professional installer?	NA
i) Are the parameters in some way limited, so that the installers will not enter parameters that exceed those authorized?	NA
ii) What controls exist that the user cannot operate the device outside its authorization in the U.S.?	NA
c) What configuration options are available to the end-user?	NA
i) Are the parameters in some way limited, so that the installers will not enter parameters that exceed those authorized?	NA
ii) What controls exist that the user cannot operate the device outside its authorization in the U.S.?	NA
d) Is the country code factory set? Can it be changed in the UI?	NA
i) If so, what controls exist to ensure that the device can only operatewithin its authorization in the U.S.?	NA
e) What are the default parameters when the device is restarted?	NA
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.	NA
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?	NA
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	NA

compliance with applicable limits and the proper antenna is used for each mode of operation. (See Section 15.407(a))	

Best Regards

Zhang Xinghai
EMC Laboratory Manager
Huawei Technologies Co., Ltd.
Address: Administration Building, Headquarters of Huawei Technologies Co., Ltd., Bantian, Longgang District, Shenzhen, 518129, P.R.C
E-mail: zhangxinghai@huawei.com
Tel: 0086-0755-28970299
Fax: 0086-0755-89650226

**Wi-Fi is a trademark of Wi-Fi Alliance