

Software Security Description – KDB 594280 D02v01r01 Section II

<p>General Description</p>	<p>1. Describe how any software/firmware update will be obtained, downloaded, and installed.</p> <p>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.</p> <p>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.</p>
	<p>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?</p> <p>The Software/Firmware in the device, controls the following RF parameters:</p> <ol style="list-style-type: none"> 1. Transmitter Frequency 2. Transmitter Output Power 3. Receiver Frequency 4. Channel Bandwidth 5. RSSI calibration <p>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.</p> <p>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</p>
	<p>3. Are there any authentication protocols in place to ensure that the source of the software/firmware is legitimate? If so, describe in details; if not, explain how the software is secured from modification</p> <p>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.</p>
	<p>4. Are there any verification protocols in place to ensure that the software/firmware is legitimate? If so, describe in details.</p> <p>The same as General Description Q3</p>
	<p>5. Describe, if any, encryption methods used.</p> <p>Software/firmware is not encrypted.</p>
	<p>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?</p> <p>This device 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.</p>

	This device can only be configured as a client in all UNII bands where it operates using passive scanning techniques.
Third-Party Access Control	1. How are unauthorized software/firmware changes prevented? The same as General Description Q3
	2. Is it possible for third parties to load device drivers that could modify the RF parameters, country of operation or other parameters which impact device compliance? If so, describe procedures to ensure that only approved drivers are loaded. No
	3. 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
	4. What prevents third parties from loading non-US versions of the software/firmware on the device? All software images are signed by private key. The device will check version number of software and verify its images by public key when software are flashed into the device.
	5. For modular devices, describe how authentication is achieved when used with different hosts. Not applicable – this is not a modular device