Date 2016-04-26

To: Federal Communications Commission,
Authorization & Evaluation Division,
7345 Oakland Mills Road
Columbia, MD 21046

And TUV SUD BABT TCB
Octagon House,
Segensworth Road,
Fareham,
Hampshire,
PO15 5RL

FCC ID: 2ACCJH043
This product only support slave mode on DFS channels,will not initiate any transmission on DFS frequencies without initiation by a master.

This product only support passive scanning on DFS channels(5150MHz-5250MHz and 5725MHz-5825MHz).

The following is the Software Security Description.

Software Security Description – KDB 594280 D02v01r01 Section II		
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. 1, Firmware Over the Air (FOTA) from the User’s Service Provider in the phone. 2, Via a hardware connection to a computer supporting the Mobile Upgrade tool download client. The Mobile Upgrade download client is a software tool that has to be downloaded from a web site used for SW download. Via FOTA, 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. And then the device

		will restart itfelf. Via the Mobile Upgrade download client, the device is to be initially recognized by the tool 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 Mobile Upgrade 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?	We can update the parameters though our own FOTA update. And all the update is authorized; customer cannot change it by themselves.
	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.	Same as Q3
	5. Describe in detail any encryption methods used to support the use of legitimate software/firmware.	We used efuse solution, which is a hardware solution in SW.
	6. For a device that can be configured as a master and client (with active or	When the device is configured as a client,it could stay in the slave mode in all UNII bands where it

	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?	operates using passive scanning techniques.
Third-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.	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.	Not applicable – this is not a modular device.

Your understanding will be highly appreciated
Thank you.
Regards,

黄正仙

Project Manager
TCL Communication Ltd.