Lemobile Information Technology (Beijing) Co., Ltd

Software Security Description – KDB 594280 D02v01r01 Section II	
General Description	
1. Describe how any software/firmware update will be obtained, downloaded, and installed.	The system will message the user that new software is available. The user will have the option to update the system via OTA.
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?	Frequency/channel. Modulation (according to 802.11x standards). These parameters cannot exceed authorized parameters.
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	Yes. Platform goes through a secure boot process every time it is powered. System verifies the root of trust to verify all the software components are signed with right set of keys.
4. Are there any verification protocols in place to ensure that the software/firmware is legitimate? If so, describe in details.	Yes, System Control Unit the software which runs first when the device boots up verifies all the software components are signed with the right keys. If the component is signed with a wrong key or altered, system will not boot.
5. Describe, if any, encryption methods used.	Header of each firmware component is encrypted with an RSA private key
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?	N/A
Third-Party Access Control	
1. How are unauthorized software/firmware changes prevented?	The bootloader is locked. No unauthorized software/firmware is accepted by the system.
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.	The end user has no access to parameter settings. The device automatically adjusts to the appropriate authorized bands for each country managed by the AP or Network infrastructure based on IEEE 802.11d standard protocols. The country code is set in the initial OS setup, once the user chooses the country of preference there is no way to change the country code settings unless the system is “reset” to default factory settings. End users do not have any access to country code settings post initial setup. Access to these settings are non-existent to the user within the UI.
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.	Parameters for settings in “Settings” menu are controlled/ checked by Android OS and SW Apps. The end user has no access to parameter settings. The device automatically adjusts to the appropriate authorized bands for each country managed by the AP or Network infrastructure based on IEEE 802.11d standard protocols.
4. What prevents third parties from loading non-US versions of the software/firmware on the device?	No prevention present today to load non-U.S. version of software/firmware on a U.S. version of the same device
5. For modular devices, describe how authentication is achieved when used with	N/A

different hosts.	

Xu kunpeng

Company Officer:	Xu kunpeng
Telephone Number:	+86 010-50962938
Email:	xukunpeng@letv.com