

Date: January 28, 2016

SOFTWARE SECURITY REQUIREMENTS FOR U-NII DEVICES
(594280 D02 U-NII Device Security 1.3, 11/12/15)

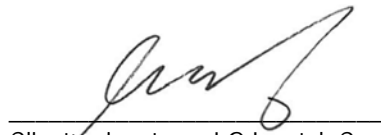
Company Name: LG Innotek Co., Ltd.
FCC ID: YZP-TWCMK007D
Product Name: Wi-Fi/BT Combo module

SOFTWARE SECURITY DESCRIPTION	
General Description	
Q.	1. Describe how any software/firmware updates for elements that 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.
A.	Module FW updated can only be done by grantee, update the FW via USB port on the engineering tool. The tool will check the firmware version, enable the update mode and install it.
Q.	2. Describe the RF 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?
A.	All RF parameter is hardcoded at factory, any future SW upgrade will not be able to modify any RF parameters.
Q.	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.
A.	This device has an 802.11a/b/g/n protocol. The FW on the device does not support writing to NVM(non-volatile memory) including FW, except through the use of our FW update tools. The FW update tool that has been provided by LG innotek permits programming of FW.
Q.	4. Describe in detail any encryption methods used to support the use of legitimate RF-related software/firmware.
A.	Same to answer #3.
Q.	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?
A.	No

Third-Party Access Control	
1. Explain if any third parties have the capability to operate a U.S.-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.	
No, Any 3 rd parties don't have capability to access and change this module. When US locked devices reach other countries, they have to be returned for replace non US locked devices. There is no method to alter or unlock them.	
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.	
There is only single USA version of SW . All US sold devices are locked to the US FCC rule and will never operate in manner that violates the FCC rule. The country lock is located in memory that unaffected by factory reset.	
3. For Certified Transmitter modular devices, describe how the module grantee ensures that host manufacturers 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 RF parameters are not modified outside the grant of authorization.	
All RF parameter was hardcoded at the factory , any OEM or system integrator will not able to modify , therefore, Radio module will remains compliance when used or installed into any system.	

SOFTWARE CONFIGURATION DESCRIPTION	
USER- CONFIGURATION GUIDE	
Q.	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.
A.	There is no UI for Installer / user configuration.
	a. What parameters are viewable and configurable by different parties? ⁹
	N/A
	b. What parameters are accessible or modifiable by the professional installer or system integrators?
	N/A
	(1) Are the parameters in some way limited, so that the installers will not enter parameters that exceed those authorized?
	N/A
	(2) What controls exist that the user cannot operate the device outside its authorization in the U.S.?
	N/A
	c. What parameters are accessible or modifiable by the end-user?
	N/A
	(1) Are the parameters in some way limited, so that the user or installers will not enter parameters that exceed those authorized?
	N/A
	(2) What controls exist so that the user cannot operate the device outside its authorization in the U.S.?
	N/A
	d. Is the country code factory set? Can it be changed in the UI?
	N/A
	(1) If it can be changed, what controls exist to ensure that the device can only operate within its authorization in the U.S.?
	N/A
	e. What are the default parameters when the device is restarted?
	N/A
Q.	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.
A.	This device cannot be configured in a bridge or mesh mode.

Q.	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?
A.	This device support only Wi-Fi client mode.
Q.	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.
A.	N/A



Client's signature : LG Innotek Co., Ltd.

Client's name / title : Jeong InChang / Director

Contact information / address : 978-1, Jangduk-dong, Gwangsan-gu, Gwangju, 506-731 Korea

Telephone: +82-62-950-0332

Fax No.: +82-62-950-0368

E-mail: ic.jeong@lginnotek.com