< TCL Technoly Electronics (Huizhou) Co., Ltd.>

Federal Communication Commission
Equipment Authorization Division, Application Processing Branch
7435 Oakland Mills Road
Columbia, MD 21048

<2016-08-01>

Attn: Office of Engineering and Technology
Subject: Attestation Letter regarding UNII devices

FCC ID: ZVA09

Software security questions and answers per KDB 594280 D02:

Software Security description – 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.	We do not release the firmware on our website for downloading. Our direct host manufacturer (OEM) can request the firmware from us and it will be made available via secure server.
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?	Radio frequency parameters are limited by US regulatory domain and country code to limit frequency and transmit power levels. These limits are stored in non-volatile memory by the module manufacturer at the time of production. They will not exceed the authorized values.
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	The firmware is installed on each single module during manufacturing process. The correct firmware is verified and installed by the module manufacturer. In addition, the firmware binary is encrypted using open SSL encryption and the firmware updates can only be stored in non-volatile memory when the firmware is authenticated. The encryption key is known by the module manufacturer only.
4	Describe in detail the verification protocols in	The firmware binary is encrypted.

	place to ensure that installed software/firmware is legitimate	The process to flash a new firmware is using a secret key to decrypt the firmware, only correct decrypted firmware is stored in non-volatile memory (see #3).
5	Describe in detail the verification protocols in place to ensure that installed software/firmware is legitimate	Standard open SSL encryption is used (see #3).
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?	The device ensures the compliance by checking the configured parameter and operation values according to the regulatory domain and country code in each band.
Software Security description – 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.	No, third parties don't have the capability to access and change radio parameters. US sold modules are factory configured to US.
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.	The embedded software is protected via the measures explained in the previous section. Distributions of host operating software are encrypted with a key.
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.	The module is not available for sale or installation outside of company licensing agreements. Modules are always installed in host systems in a factory by end integrators (OEM) responsible for loading authorized software.
Software Security description – USER CONFIGURATION GUID		
1	Describe the user configurations permitted through the UI. If different levels of access are	There is no user configuration GUI.

	permitted for professional installers, system integrators or end-users, describe the differences.	
	a. What parameters are viewable and configurable by different parties?	There is no user configuration GUI.
	b. What parameters are accessible or modifiable to the professional installer? i. Are the parameters in some way limited, so that the installers will not enter parameters that exceed those authorized? ii. What controls exist that the user cannot operate the device outside its authorization in the U.S.?	This device is not subject to professional installation
	c. What configuration options are available to the end-user? i. Are the parameters in some way limited, so that the installers will not enter parameters that exceed those authorized? ii. What controls exist that the user cannot operate the device outside its authorization in the U.S.?	The end user is not able to configure any parameters related to the devices radio The parameters can only be changed remotely within the limits of country code US. The country code and regulatory domain control do limit all the parameters set
	d. Is the country code factory set? Can it be changed in the UI? i. If so, what controls exist to ensure that the device can only operate within its authorization in the U.S.?	The country code is factory set and is never changed by UI. The country code is factory set and is never changed by UI
	e. What are the default parameters when the device is restarted?	At each boot up the country code and the antenna gain are read from the non-volatile memory, those values are configured during module production.
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.	Not supported
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	No end user controls or user interface operation to change master/client operation.

	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?	
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. See Section 15.407(a).	The device does not support these modes/features.

Sincerely

Peng Weirun

(Signed)
Name / Title: Weirun Peng / Approbation Engineer
Company: TCL Technoly Electronics (Huizhou) Co., Ltd.
Address: Section 37, Zhongkai High-tech development Zone Huizhou 516006, China
Phone: 86-752-2606710
Fax: 86-752-2625162
Email: pengwr@tcl.com