TQ–Systems GmbH | Gut Delling | 82229 Seefeld | Germany

7layers GmbH

Carsten Steinröder

Borsigstrasse 11
40880 Ratingen, Germany

Date: 2016-01-22

Contact person: Kotowsky Pia
Department: TQ PM DU
Phone: +49 831 690-683
Fax: +49 831 690-44683
E-mail: PIA.KOTOWSKY@tq-group.com

Software Security Requirement

Dear Mr. Steinröder,

Please find below the required information regarding “Software Security”

	Question	**Answer**
General Description	1. Describe how any software/firmware update will be obtained, downloaded, and installed.	The intelligence of the system is based on embedded RTOS on a microcontroller. The only way to update the firmware is by opening the case of the product and plugging-in a programming-cable with USB-connector. Furthermore a confidential software programming tool with its own data-transmission protocol is needed to configure the RF-Chip configuration which is stored into the microcontrollers flash memory. It is provided by AMIMON Ltd. - the WHDI-Chip manufacture to program the factory set of the RF-chip and cannot be obtained by third-parties.
	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?	There are several fixed configuration tables (including frequency, DFS setting, output power) depending on different country rules and norms. Due to encryption it is not possible to change these tables. During production the appropriate operating region / configuration table is selected.

	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.	FW authentication is done by using encrypted RC4 mechanism. For FW installation, FW must be encrypted with Unique Factory key to enable the installation. RF parameters are protected against modification by enabling setting the RF-related parameters in OTP-like mechanism (one time programmable) only at the factory.
	4. Are there any verification protocols in place to ensure that the software/firmware is legitimate? If so, describe in details.	HW verification protocol ensure that only Authentic FW will operate on Hardware. This is done by verifying that installed FW is encrypted with the Factory Key.
	5. Describe, if any, encryption methods used.	Factory authenticate FW uses RC4 encryption method with a 256 bit key to encrypt /decrypt the software. For installation, FW must be encrypted with Unique Factory key to enable the installation of legitimate SW.
	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 master role is dedicated to the Rx-Device.
Third-Party Access Control	1. How are unauthorized software/firmware changes prevented?	A third party has no access to any FW source code and drivers in general or to the RF driver in particular and therefore FW cannot be changed, and this is on top of the factory authentication encrypted key.

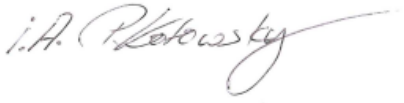
	2. Is it possible for third parties to load device drivers that could modify the RF parameters, country of operation or other parameters which impact device compliance? If so, describe procedures to ensure that only approved drivers are loaded.	There is no possibility to load drivers or create them, because the register set of RF-chip is confidential.
	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.	No such option is provided for third parties. Customers are explicitly advised that it is prohibited to operate the device outside the region for which it is sold.
	4. What prevents third parties from loading non-US versions of the software/firmware on the device?	Based on a RTOS there is no possibility to reconfigure or change the microcontrollers software.
	5. For modular devices, describe how authentication is achieved when used with different hosts.	The modular device is a black box from host view. Host only provides video data to Tx device and gets video data from Rx device. Therefore no authentication between host and device is necessary.
USER CONFIGURATION GUIDE	1. To whom is the UI accessible? (Professional installer, end user, other.)	The end user and the professional installer can initiate a link between transmitter and receiver by pressing a push button and the link status can be observed LEDs. Furthermore a system-reset can be initiated.
	a) What parameters are viewable to the professional installer/end-user?6	Neither the end user nor the installer can view any parameters.
	b) What parameters are accessible or modifiable to the professional installer?	Neither the end user nor the installer can change the parameters.
	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.?	-
	c) What configuration options are available to the end-user?	None.
	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.?	-
	d) Is the country code factory set? Can it be changed in the UI?	Yes the country code is factory set and cannot 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.?	-
	e) What are the default parameters when the device is restarted?	The default parameters are the factory reset and don´t change over the system lifetime.
	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.	No.
	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?	The device operates as a video-data streaming interface with a peer-to-peer connection according to the WHDI specification. It is a fixed configuration (peer-to-peer only).

	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.	

Best regards,

TQ-Systems Durach GmbH



i.A. Pia Kotowsky