Software security for UNII Devices

beyerdynamic GmbH & Co. KG

Theresienstrasse 8, 74072 Heilbronn, Germany

To Whom It May Concern:

Product/Model/HVIN: QUINTA TB

FCC ID: OSDQUINTATB

IC ID: 3628A-QUINTATB

SOFTWARE SECURITY REQUIREMENTS FOR U-NII DEVICES acc. to KDB 594280

SOFTWARE CONFIGURATION DESCRIPTION	
General Description	
1	Describe how any software/firmware updates for elements than 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. *The software that can be downloaded from the internet cannot change the RF performance. The RF module uses a separate microcontroller which cannot be field-updated. The system uses a proprietary protocol and cannot be operate as WLAN device according to IEEE 802.11.*
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? *As said above, there is no way to change any RF parameter or RF protocol via 3rd party accessible software*
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. *As said above, there is no way to change any RF parameter or RF protocol via 3rd party accessible software*
4	Describe in detail any encryption methods used to support the use of legitimate RF-related software/firmware.

	As said above, there is no way to change any RF parameter or RF protocol via 3rd party accessible software
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? *This is not applicable here*
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. *There is now way that any 3rd party device can communicate with the system*
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 now way that any 3rd party device can communicate with the system*
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. *There is no way that any 3rd party device can communicate with the system*
	SOFTWARE CONFIGURATION DESCRIPTION
USER CONFIGURATION GUIDE	
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. *The uses can only determine the RF band where the system operates by GUI or by external IP commands. There are three bands: High, Mid & Low*

1.a	What parameters are viewable and configurable by different parties? *Only the transmission frequency can be changed by external software*
1.b	What parameters are accessible or modifiable by the professional installer or system integrators? *There is no difference between end user and professional installer. The professional installer can also only change the frequency.*
1.b(1)	Are the parameters in some way limited, so that the installers will not enter parameters that exceed those authorized? *The installer has no additional means to change anything than just the frequency*
1.b(2)	What controls exist that the user cannot operate the device outside its authorization in the U.S.? *There is no way that any 3rd party device can communicate with the system. The RF parameters cannot be changed via user software*
1.c	What parameters are accessible or modifiable by the end-user? *Only frequency*
1.c(1)	Are the parameters in some way limited, so that the user or installers will not enter parameters that exceed those authorized? *The parameters are fixed using internal commands*
1.c(2)	What controls exist so that the user cannot operate the device outside its authorization in the U.S.? *There is no way that any 3rd party device can communicate with the system. The RF parameters cannot be changed via user software*
1.d	Is the country code factory set? Can it be changed in the UI? *The country settings (RF levels) are factory set and cannot be altered by installer or user*
1.d(1)	If it can be changed, what controls exist to ensure that the device can only operate within its authorization in the U.S.? *It cannot be changed*
1.e	What are the default parameters when the device is restarted? *The default settings are according to the RF emission test report: 16dBm e.i.r.p. at 5.2GHz*
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, it can't
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? *This is not applicable here since the system is proprietary*
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)) *This is not applicable here since the system is proprietary*

i.V.

Name: Ulrich Roth

Company: beyerdynamic GmbH & Co. KG

Address: Theresienstrasse 8, 74072 Heilbronn, Germany

Phone: +49 7131 617 155

Fax: +49 7131 617 215

Email: roth@beyerdynamic.de