Software Security Declaration

Product:	Neratec Wireless Module
Model Name	DT60M
FCC ID:	2AEJD-103678-DT60M
Version:	Version 2.0 / 2015.06.22
Confidentiality:	Confidential

This device is fully compliant with the requirement of KDB 594280D02 version to V01r01

	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 nonvolatile 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 openSSL encryption and the firmware updates can only be stored in nonvolatile memory when the firmware is authenticated. The encryption key is known by the module manufacturer only.
4.	Describe in detail the verification protocols in place to ensure that installed software/firmware is legitimate.	The firmware binary is encrypted. The process to flash a new firmware is using a secret key to decrypt the firmware, only correct decrypted firmware is stored in nonvolatile memory (see #3).
5.	Describe in detail any encryption methods used to support the use of legitimate software/firmware.	Standard openSSL encryption is used (see #3).

Neratec Solutions AG
Rosswiesstrasse 29
CH-8608 Bubikon
Switzerland

Tel +41 55 253 2000
Fax +41 55 253 2070
info@neratec.com
www.neratec.com

6.	For a device that can be configured as 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.	How is unauthorized software/firmware changes prevented?	Unauthorized firmware is not accepted by the firmware update process. See General Description #5, #3
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 embedded software is protected via the measures explained in the previous section. Distributions of host operating software are encrypted with a key.
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, third parties don't have the capability to access and change radio parameters. US sold modules are factory configured to US.
4.	What prevents third parties from loading non -US versions of the software/firmware on the device?	Only encrypted and verified firmware is applied and stored in the nonvolatile memory.
5.	For modular devices, describe how authentication is achieved when used with different hosts.	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.	To whom is the UI accessible? (Professional installer, end user, other.)	The UI is accessible to anyone using the device.
a.	What parameters are viewable to the professional installer/end user?	Various device status information is made available like log information, connection status, operation mode, operation frequency, etc. Radio parameters are described in c.i

b.	What parameters are accessible or modifiable to the **professional installer**?	This device is not subject to professional installation
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**?	The end user is able to configure the operation frequency, modulation, reduce the output power levels etc. The end user cannot change the antenna gain and country code, those settings are programmed at factory production time.
i.	Are the parameters in some way limited, so that the installers will not enter parameters that exceed those authorized?	Yes, the parameters can only be changed within the limits of country code US.
ii.	What controls exist that the user cannot operate the device outside its authorization in the U.S.?	The country code and regulatory domain control do limit all the parameters set by UI
d.	Is the country code factory set? Can it be changed in the UI?	The country code is factory set and is never changed by 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
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 nonvolatile 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 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?	No end user controls or user interface operation to change master/client operation.
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	The device does not support these modes/features.

	antenna is used for each mode of operation. See Section 15.407(a).