FCC ID: PD97262WW

Software Security Description – KDB 594280	
General Description	
1. Describe how any software/firmware update will be obtained, downloaded, and installed.	Firmware is loaded in factory and update (bug fixing for example) can only be obtained on vendor site. Driver (USB) is pre-loaded on Notebook host where the card is installed.
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 (Tx Power, Bandwidth) are stored in Firmware and loaded in NVM. Secured boot will only allow authorized Firmware to start and authorized RF parameters to be used and not exceeded.
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.	Firmware updater can only handle Firmware from vendor site. Then Secured boot will only allow authorized Firmware to start. USB driver is only used to establish a digital link between data modem card and a notebook host.
4. Are there any verification protocols in place to ensure that the software/firmware is legitimate? If so, describe in details.	Firmware updater can only handle Firmware from vendor site. Then Secured boot will only allow authorized Firmware to start. Non authorized or modified Firmware will just not start
5. Describe any encryption methods used.	N/A
6. For a device that can be configured as a master and a client (with active or passive scanning), explain how the device ensures compliance for each mode? In particular if the device acts as a master in some band of operation and client in another; how is compliance ensured in each band of operation?	N/A
Third-Party Access Control	
1. How are unauthorized software changes /firmware changes prevented?	Secured boot will only allow authorized Firmware to start.
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 that only approved drivers are loaded.	No

3. 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 is violation of the certification.	This cellular device has capability to operate in Europe or other Geos. This is transparent to end-user as device will look for available bands in passive scan.
4. What prevents third parties from loading non-U.S. versions of the software/firmware on the device?	There is no alternate non US version of Firmware and Secured boot will only allow authorized FW to start.
5. For modular devices, describe how authentication is achieved when used with different hosts.	Module is already installed on host when sold
Software Configuration Description	
1. To whom is the UI accessible?	
a) What parameters are viewable to the professional installer/end user?	No parameters accessible
b) What parameters are accessible or modifiable to the professional installer?	No parameters accessible
i) Are the parameters in some way limited, so that the installers will not enter parameters that exceed those authorized?	No parameters accessible
ii) What controls exist that the user cannot operate the device outside it's authorization in the U.S.?	No parameters accessible
c) What configuration options are available to the end user?	No parameters accessible
i) Are the parameters in some way limited, so that the installers will not enter parameters that exceed those authorized?	No parameters accessible
ii) What controls exist that the user cannot operate the device outside it's authorization in the U.S.?	N/A
d) Is the country code factory set? Can it be changed in the UI?	No country code
i) If so, 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 restarted?	Device is by default in passive scan
2. Can the radio be configured in bridge or	No

mesh mode? If yes, an attestation may be required. Further information is available in KDB 905462 D02.	
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 to ensure compliance.	N/A

Name of applicant (or authorized agent)

Date: June 23, 2015 Signature: _____

Name: Steven C. Hackett

Product Regulations Engineer

Intel Mobile Communications