TomTom International BV.
De Ruijterkade 154, 1011 AC, Amsterdam The Netherlands

SOFTWARE SECURITY FOR U-NII DEVICES

Pursuant to FCC Part 15E 15.407(i) and KDB 594280 D02 U-NII Device Security, applicant must describe the overall security measures and systems that ensure that only:

1. Authenticated software is loaded and operating the device.
2. The device is not easily modified to operate with RF parameters outside of the authorization

The description of the software must address the following questions in the operational description for the device and clearly demonstrate how the device meets the security requirements.

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.
	Builds provided by TomTom can be installed using on-device SW. RF parameters are stored in the persist partition.
	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?
	The power limit of the wifi antenna is set in the nv memory, which is stored in the persist partition of the device. We never update the persist partition, it is set at time of manufacture and never updated.
	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.
	Packages to be installed are signed using TomTom key. Build itself is signed and signature is verified by the bootloader. Bootloader can only be modified using TomTom signed builds.
	4. Describe in detail any encryption methods used to support the use of legitimate RF-related software/firmware.
	Packages to be installed are signed using TomTom key. Build itself is signed and signature is verified by the bootloader. Bootloader can only be modified using TomTom signed builds.
	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?
	The power for each band is individually limited by configuration in the nv memory, furthermore each band can be disabled with settings in the nv memory.

3rd 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.
	Third party software or users cannot change the parameters.
	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.
	Third party software or users cannot change the parameters.
	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.
	Not applicable, this device is not a module.

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.
	a) What parameters are viewable and configurable by different parties?
	No RF parameters can be controlled via the UI. There is only a Wi-Fi on/off + regular network selection.
	b) What parameters are accessible or modifiable by the professional installer or system integrators?
	No RF parameters can be controlled via the UI.
	(1) Are the parameters in some way limited, so that the installers will not enter parameters that exceed those authorized?
	No RF parameters can be controlled via the UI.
	(2) What controls exist that the user cannot operate the device outside its authorization in the U.S.?
	No RF parameters can be controlled via the UI so this is not possible.

User Configuration guide	c) What parameters are accessible or modifiable to by the end-user?
	No parameters can be changed by the end user.
	(1) Are the parameters in some way limited, so that the user or installers will not enter parameters that exceed those authorized?
	No parameters can be changed by the end user.
	(2) What controls exist that the user cannot operate the device outside its authorization in the U.S.?
	No parameters can be changed by the end user so this is not possible.
	d) Is the country code factory set? Can it be changed in the UI?
	There is no county code set in the factory or in the UI.
	(1) If it can be changed, what controls exist to ensure that the device can only operate within its authorization in the U.S.?
	Country code cannot be changed.
	e) What are the default parameters when the device is restarted?
	See extra document : 5G_power_limit.xlsx
	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.
	It cannot be configured in bridge or mesh mode.
	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?
	There are no UI options to change any of the Wi-Fi parameters other than security type and password.
	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))
	There is only one Wi-Fi antenna that supports all Wi-Fi bands.

Product Name: Tablet
The applicant: TomTom International BV
FCC ID: S4L4FI722

David Cox / Project Manager / TomTom International B.V.