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

Date: Dezember 14, 2017

FCC ID: S4L4FIC00

To the attention of
Federal Communications Commission
Authorization and Evaluation Division

Permanent Confidentiality Request

Pursuant to Sections 0.457 and 0.459 of the Commission's Rules, the Applicant hereby requests confidential treatment of information accompanying this Application as outlined below:

Schematics
Block Diagram
Operational Description
Software Operational Description
Part list
Tune-up Procedure

The above materials contain trade secrets and proprietary information not customarily released to the public. The public disclosure of these matters might be harmful to the Applicant and provide unjustified benefits to its competitors.

The Applicant understands that pursuant to Rule 0.457, disclosure of this Application and all accompanying documentation will not be made before the date of the Grant for this application.

Sincerely yours,

Signature: 

David Cox – TomTom BRIDGE Product Unit Leader – TomTom International B.V.

David.Cox@tomtom.com

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

Date: December 14, 2017

FCC ID: S4L4FIC00

To the attention of
Federal Communications Commission
Authorization and Evaluation Division

Confidentiality Request

Pursuant to Sections 0.457 and 0.459 of the commission's rules, we request **short-term confidential** treatment for the following information until 120 days after the Grant Date of Equipment Authorization in order to ensure sensitive business information remains confidential until the actual marketing of the device:

External photos
Test Setup photos
User's manual
Internal Photos

Sincerely yours,

Signature: 

David Cox – TomTom BRIDGE Product Unit Leader – TomTom International B.V.
David.Cox@tomtom.com

TomTom International B.V.

De Ruijterkade 154, 1011 AC, Amsterdam The Netherlands

DFS client device channel plan and software operational declaration

Date: December 14, 2017

We, TomTom International B.V., declare that the device, FCC ID: S4L4FIC00 Model Name: 4FIC00, does not have "Ad Hoc on non-US frequencies" and/or "on DFS frequencies. Also, the client software and associated drivers will not initiate any transmission on DFS frequencies without initiation by a master. This includes restriction on transmissions for beacons and support for ad-hoc peer-to-peer modes.

Below is the channel / frequency plan for the device

CH	1	2	3	4	5	6	7	8	9	10	11
Frequency (MHz)	2412	2417	2422	2427	2432	2437	2442	2447	2452	2457	2462
Scan Type	Active	Active	Active	Active	Active	Active	Active	Active	Active	Active	Active

5G band 1 (if without 80MHz, please delete CH 42)

CH	36	38	40	42	44	46	48				
Frequency (MHz)	5180	5190	5200	5210	5220	5230	5240				
Scan Type	Active	Active	Active	Active	Active	Active	Active				

5G band 2 (if without 80MHz, please delete CH 58)

CH	52	54	56	58	60	62	64
Frequency (MHz)	5260	5270	5280	5290	5300	5310	5320
Scan Type	Passive	Passive	Passive	Passive	Passive	Passive	Passive

5G band 3 (if without 80MHz, please delete CH106)

CH	100	102	104	106	108	110	112	116			
Frequency (MHz)	5500	5510	5520	5530	5540	5550	5560	5580			
Scan Type	Passive	Passive	Passive	Passive	Passive	Passive	Passive	Passive			
CH	132	134	136	140							
Frequency (MHz)	5660	5670	5680	5700							
Scan Type	Passive	Passive	Passive	Passive							

5G band 4 (if without 80MHz, please delete CH155)

CH	149	151	153	155	157	159	161	165
Frequency (MHz)	5745	5755	5765	5775	5785	5795	5805	5825
Scan Type	Active	Active	Active	Active	Active	Active	Active	Active

Also, on DFS channels, the WLAN driver in the device operates under the control of an AP at all times, except when in ad-hoc mode, on US non-DFS channels. The device passively scans DFS frequencies until a master device is detected. The control of this functionality is not accessible to anyone under any conditions. Furthermore, the firmware is protected by special signature and CRC checksum. Signature and CRC checksum will be calculated and verified before firmware upgrade. Unauthorized modification to firmware will lead the failure of verification thus firmware upgrade is not allowed.

Sincerely yours,

Signature:

David Cox – TomTom BRIDGE Product Unit Leader – TomTom International B.V.
David.Cox@tomtom.com

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

Attestation for FCC Declaration of Conformity

Date: November 14, 2017
FCC ID: S4L4FIC00

To whom it may concern:

We, the undersigned **TomTom International B.V.**, hereby attest to the fact that we will apply the Declaration of Conformity procedure to the class B computer peripheral portion of this composite filing.

Thank you for your attention

Sincerely yours,

Signature: _____

David Cox – TomTom BRIDGE Product Unit Leader – TomTom International B.V.
David.Cox@tomtom.com

TomTom International B.V.

De Ruijterkade 154, 1011 AC, Amsterdam The Netherlands

Date: December 14, 2017

FCC ID: S4L4FIC00

Tune-up procedure

Calibration equipment consists of an RF signal generator, power supply, power meter, spectrum analyzer and a radio communication test set. A mechanical fixture holds the DUT in place and is responsible for reliably mating the RF connector of the jig to the DUT. The entire fixture is enclosed in an RF shield box whose purpose is to prevent external RF signals from interfering or contributing to measurements of the DUT's RF. RF shielded cabling connecting the instrumentation to the jig is used for the same reason. All of this equipment is mounted in a rack and is known as a Calibration test station.

The Calibration process is automated, with a host PC controlling both the test equipment and EUT. The Calibration program measures individual EUT's RF power and key RF parameters and writes the proper calibration value back into EUT's internal register (proprietary and not user changeable) and re-measures RF parameters again to insure that all required parameters are within the limit. As described above, every EUT will be tested individually to make sure that the output power and RF characteristic will not exceed the level documented in the EMC/RF compliance test report(s).

Signature:

David Cox – TomTom BRIDGE Product Unit Leader – TomTom International B.V.

David.Cox@tomtom.com

TomTom International B.V.

De Ruijterkade 154, 1011 AC, Amsterdam The Netherlands

Date: December 14, 2017
FCC ID: S4L4FIC00

Software Operational Description

We, **TomTom International B.V.** hereby declare that requirements of KDB 594280 D02 U-NII Device Security v01r03 have been met and shown on the following question. Further we declare that the info listed below are correct and represent the product in consideration under this filing.

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.

Description: 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?

Description: 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.

Description: Packages to be installed are signed using TomTom key. The 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.

Description: Packages to be installed are signed using TomTom key. The 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?

Description: 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.

6. 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.

Description: Third party software or users cannot change the parameters.

7. 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.

Description: Third party software or users cannot change the parameters.

8. 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.

Description: Not applicable, this device is not a module.

9. 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?

Description: No RF parameters can be controlled via the UI. There is only a wifi on/off + regular network selection.

b) What parameters are accessible or modifiable by the professional installer or system integrators?

Description: No RF parameters can be controlled via the UI.

i) Are the parameters in some way limited, so that the installers will not enter parameters that exceed those authorized?

Description: No RF parameters can be controlled via the UI.

ii) What controls exist that the user cannot operate the device outside its authorization in the U.S.?

Description: No RF parameters can be controlled via the UI so this is not possible.

c) What parameters are accessible or modifiable by the end-user?

Description: No parameters can be changed by the end user.

i) Are the parameters in some way limited, so that the user or installers will not enter parameters that exceed those authorized?

Description: No parameters can be changed by the end user.

ii) What controls exist so that the user cannot operate the device outside its authorization in the U.S.?

Description: 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?

Description: There is no country code set in the factory or in the UI.

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

i) If it can be changed, what controls exist to ensure that the device can only operate within its authorization in the U.S.?

Description: Country code cannot be changed

e) What are the default parameters when the device is restarted?

Description: See extra document : 5G_power_limit.xlsx

10. 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.

Description: It cannot be configured in bridge or mesh mode.

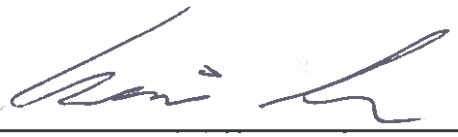
11. For a device that can be configured as a master and client (with active or passive scanning),if this is user configurable, describe what controls exist, within the UI, to ensure compliance for each mode. If the device acts as a master in some bands and client in others, how is this configured to ensure compliance?

Description: There are no UI options to change any of the wifi parameters other than security type and password.

12. 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))

Description: There is only one wifi antenna that supports all wifi bands.

If you should have any question(s) regarding this declaration, please don't hesitate to contact us. Thank you!

Signature: 

David Cox – TomTom BRIDGE Product Unit Leader – TomTom International B V

David.Cox@tomtom.com