SOFTWARE SECURITY FOR U-NII DEVICES

FCC ID: SL4FF51

Pursuant to FCC Part 15E 15.407(i) and KDB 594280 D02 U-NII Device Security v01r03
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.
	Only Station application, will not switch to softtap, there will be no switching caused by the problem. The software/firmware of existing products cannot be updated on the device side. Since the software has been fixed to the product, the RF parameters of the device of the product will not be affected. The RF parameters can be changed only after changes are made at the bottom of the software or through the production and measurement tool.
	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?
	RF parameters cannot be changed in any other way
	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.
	The current software can be modified only by the production and test tool, which requires a user name and password
	4. Describe in detail any encryption methods used to support the use of legitimate RF-related software/firmware.
	A user name and password are required to log in to the production test tool
	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?
	RF drivers are compiled and packaged, and the user platform software does not have ROOT permission

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.

	No third party can operate equipment sold in the United States.
	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 firmware cannot be installed
	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.
	The LINUX driver software controls the load on the host. The RF parameter of WIFI is saved in the original code of the driver, and the user cannot modify it. RF parameters are written through the production tool, which is protected by user name and password.

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 existing devices do not have user configuration interface, no professional installation personnel, system integrators, only a common user interface
	a) What parameters are viewable and configurable by different parties?
	Only the WIFI/ hotspot function is configured to turn on and off and WIFI input name and password.
	b) What parameters are accessible or modifiable by the professional installer or system integrators?
	Only access WIFI/ hot spots on and off and WIFI input name and password parameters
	(1) Are the parameters in some way limited, so that the installers will not enter parameters that exceed those authorized?
	For the installer, there are restrictions on entering and changing parameters
	(2) What controls exist that the user cannot operate the device outside its authorization in the U.S.?
	The software sets permissions for common users and cannot perform operations that are not authorized

User Configuration guide	c) What parameters are accessible or modifiable to by the end-user?
	Only access WIFI/ hot spots on and off and WIFI input name and password parameters
	(1) Are the parameters in some way limited, so that the user or installers will not enter parameters that exceed those authorized?

	For the installer, there are restrictions on entering and changing parameters
	(2) What controls exist that the user cannot operate the device outside its authorization in the U.S.?
	The software sets permissions for common users and cannot perform operations that are not authorized
	d) Is the country code factory set? Can it be changed in the UI?
	Yes, depending on the country you choose
	(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 can only be controlled by choosing the country and cannot go beyond the mandate of the country
	e) What are the default parameters when the device is restarted?
	After the restart, it is the same as the initial setting and will not change
	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.
	Do not support
	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 is no frequency band configuration. After a user selects a country, the device is configured according to the authorization
	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))
	The device has only one antenna, one access point (point to point)

Name and surname of applicant (or authorized representative): TomTom International BV

Date: March 9, 2023 **Signature:** DocuSigned by: Barto Wijlens D0D84AF857A548A...