Date:29/01/2020

to:	from:
Regulatory Certification Body DEKRA Testing and Certification, S.A.U. Parque Tecnológico de Andalucía C/ Severo Ochoa 2 & 6 29590 Campanillas Málaga, España	**Bittium Wireless Ltd.** Ritaharjuntie 1, 90590 Oulu, Finland

Related to product:

Type of equipment:	Secure Smartphone
Brand name:	Bittium
FCC ID:	V27SD-61
IC:	3282B-SD61

To whom it may concern,

We hereby declare that this device is programmed to operate only in the following frequencies:

2.4 GHz Band,

Frequency Range **2.401 - 2.482 GHz**

- Channels 1-11 (BW 22 MHz)
- Channels 1-11 (BW 20 MHz)
- Channels 3 and 11 (BW 40 MHz)

5GHz Band,

In Canada, the device won't operate in the frequency range **5.6 – 5.65 GHz** (channels within this range won't be used)

- Frequency Range **5.170 – 5.330 GHz**
  - Channels 36-64 (BW 20 MHz)
  - Channels 38-62 (BW 40 MHz)
  - Channels 42 and 58 (BW 80 MHz)

- Frequency Range **5.490 – 5.730 GHz**
  - Channels 100-144 (BW 20 MHz) (Except 120, 124, 128 in Canada)
  - Channels 102-142 (BW 40 MHz) (Except channels 118 and 126 in Canada)
  - Channels 106 and 138 (BW 80 MHz) (not in channel 122 in Canada)

Operation modes, DFS and TPC

This device does not support Ad-Hoc / Wi-Fi hotspot mode in 5 GHz frequency band where the device operates in both Master and Slave DFS functional modes.

Ad-hoc / Wi-Fi hotspot feature is limited to 11 channels available in 2.4 GHz frequency band.

As client device, this product does not initiate transmission of any probes, beacons and does not initiate Ad-Hoc operations when not associated with and under the control of a certified master device, according to Section 15.202 of FCC rules.

Future changes in this device will not change theses operational characteristics, in any mode of operation.

Software security description per KDB 594280 D02:

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.	There are three ways to provision software to the device: - Software is initially provisioned to the devices in Bittium's subcontractor factory. - Software is updated over the air, via HTTPS connection - Software is post-factory flashed via USB flashing method, binaries are obtained from Bittium Extranet In all of these cases, the software integrity is verified so that unauthorized firmware cannot be executed. Bittium Trusted Boot verifies the complete chain from bootloader up to Android OS. The strength of verification algorithms are at least RSA 2048 at all phases of SW bring-up. Over-the-Air SW packages signatures have been generated using ECC-256 key. Tough Mobile 2 firmware is built within secure offline environment where the build servers and key servers are located. It is an isolated network for the sole purpose of generating signed firmware images for the devices. Physical access to the firmware generation environment is limited only to Bittium IM personnel and members of Special Device Platform security team and all the servers have at least AES-256 strength disk encryption applied and are kept offline when inactive.

	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 are incorporated within the firmware image as pre-set tuning files and cannot be changed by end-user nor by pure SW changes.
	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.	Secure boot authenticates the firmware. Authentication starts by MSM670 SOC internal ROM bootloader which validates the 2nd stage bootloader XBL against factory-provisioned public key root hash (2k RSA). Then execution is passed to the XBL. XBL starts boot sequence which validates the modem signature against the same root key hash and loads it. It also authenticates firmware images for WLAN and DSPs (2k RSA). Linux kernel integrity is authenticated against a public RSA key located within bootloader binary (2k RSA). After that the execution passes to Linux kernel. Kernel authenticates all kernel modules that are loaded against signatures (4k RSA). Kernel also authenticates the Android OS system image integrity using kernel feature “dm-verity” where all the system binaries are compared against a signed (2k RSA) hash-table created during SW build-time. Any failure on signature check due to modification to AndroidOS root file system causes device to fall to non-usable state.

	4. Describe in detail any encryption methods used to support the use of legitimate RF-related software/firmware.	See chapter 3.
	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?	On client-mode, the DFS channels are not available; scanning of these bands is disabled. On DFS mode phone does not actively scan channels, but waits for channel configuration from access point. On master mode, WLAN 2.4GHz channels 12-13 are always disabled by checking if regional or country code is U.S. Configuration files cannot be changed as they are integrity-protected by secure boot chain.
Third-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.	Tough Mobile 2 SW configuration is world-compatible, ie there are no separate SW variants for regional markets. WLAN 2.4GHz channels 12-13 are always disabled by checking if regional or country code is U.S. After the airplane mode is turned off, WLAN is on world domain and in this mode WLAN 2.4GHz channels 12-13 are always disabled.
	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.	Device permits 3rd party application installation but not firmware installation. See chapter 3 from General description and chapter 1 from Third-Party Access Control

	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 for Tough Mobile 2 device. It is not a WIFI module.

Sincerely,

_____

By: Mikko Miettinen
Title: Senior Manager
Company: Bittium Wireless Ltd.
Telephone: +3583442000
e-mail: mikko.miettinen@bittium.com