Date: 2019-11-13

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	**Manufacuter:** Telit Communications S.p.A., Via Stazione di Prosecco, 5/B. 34010 Sgonico, Trieste (Italy),

Related to product:

Type of equipment:	Radio module
Brand name:	Telit
FCC ID:	RI7WL865E4
IC:	5131A-WL865E4

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

5GHz Band,

- Frequency center Range **5.170 – 5.240 GHz, 5.260 – 5.320 GHz, 5.500 – 5.700 GHz, 5.735 – 5.835 GHz**
  - Channels 36-165 (BW 20 MHz)
    - 36,40,44,48,52,56,60,64,100,104,108,112,116,132,136,140
- In Canada, the device won't operate in the frequency range 5600 – 5650 MHz (channels within this range won't be used)"

Operation modes, DFS and TPC

DFS Operational Mode: Slave without Radar detection.

TPC Function: Not Supported

In the frequency band below, this product can only be used as a client, since the RF chip has no hardware radar detection capability and uses passive scanning in these channels.

- 5250-5350 MHz
- 5470 – 5725 MHz

Whereas the product can operate as both client and master in the following frequency bands

- 5170 – 5250MHz
- 5735 – 5835 MHz

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.	RF parameters are part of OTP and programmed in production line. This cannot be over-written in the field by a firmware upgrade. Firmware is downloaded through HTTPS (secured tunnel) from the server and is protected with the Hash to make sure the firmware is not tampered. A secured boot, would further validate the firmware image before execution.
	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?	No RF parameters are modified by software without hardware 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.	Firmware is downloaded through HTTPS (secured tunnel) from the server and is protected with the Hash to make sure the firmware is not tampered. A secured-boot, would further validate the firmware image before execution.

	4. Describe in detail any encryption methods used to support the use of legitimate RF-related software/firmware.	Hashing mechanism is used to ensure that the firmware is not tampered with.
	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?	Firmware restricts users from configuring the device to act as master in restricted bands and the same applies for active scanning in client mode. Also user doesn't have option to overwrite these configuration.
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.	Not applicable, since the module isn't an end product.
	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.	Not applicable

	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 module firmware doesn't expose any functionality that can alter the RF parameters to the host.

Sincerely,

Ken Bednasz
Title: VP Application Engineer
Company: Telit Communications S.p.A.
Telephone: 1-919-415-1517
e-mail: Ken.Bednasz@telit.com