Continental

FCC ID: LHJ:LNADVW, IC: 2807E-LNADVW

WiFi Security Attestation for LNADVW

As required by Document 594280 D02 U-NII Device Security v01r03, this document describes the measures implemented to ensure that the device cannot be modified by any RF-related SW changes by third parties to operate outside the authorized RF parameters.

SOFTWARE SECURITY DESCRIPTION

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.

1. LNADVW is an embedded module that will be integrated into automotive telematics device. RF parameters are part of the SW code resigning inside the LNADVW module. After the telematics device leaves Continental's factory, there are no updates made ever to the calibration parameters. The software Download is protected by a TCU request to a hard-coded server address (to avoid spoofing).

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?

2. WiFi RF parameters are located in the EEPROM data.bin file located on the LNADVW embedded module. These parameters are not modifiable outside of Continental's factory.

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.

3. To ensure that the source of the RF-related software/firmware is valid, the SW image download is protected by the host device request to a hard-coded address to avoid spoofing. Transport Security Layer (TLS) handshake is also implemented with protected certificates. Unique device log-in credentials, OMA-DM tree comparison and synch, and image download protected by TLS. The image can only be modified using proprietary development tool available within Continental.

4. Describe in detail any encryption methods used to support the use of legitimate RF-related software/firmware.

4. The target SW image is verified on the target device via a digital signature which was generated using the Continental or OEM key. Encryption of the image can also happen but not required.

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?

5. Only Hot Spot (Master) mode is enabled for the end user. There is no mechanism available to switch between Master and Client mode. The Device does not have User Interface.

Continental

FCC ID: LHJ:LNADVW, IC: 2807E-LNADVW

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.

1. The telematics device containing the LNADVW module will be installed in a vehicle sold in the U.S. market. If the vehicle travels to a region outside on the U.S., WiFi hotspot functionality will be discontinued by the telematics device.

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.

2. Device does not permit third-party software or firmware installations.

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.

3. For LNADVW, the host device is also Continental's product. The driver SW is loaded into the host telematics devices and are part of the application SW image. The drivers are controlled and managed as part of the overall application SW image and cannot be updated independently.

SOFTWARE CONFIGURATION DESCRIPTION
USER CONFIGURATION GUIDE

Because the LNADVW does not have any user interfaces, the requirements in this section are not applicable.

James Zhang

Engineering Manager
Continental Automotive Systems, Inc.
21440 W. Lake Cook Rd.
Deer Park, IL 60010