# HMD Global Oy

**Bertel Jungin aukio 9, 02600 Espoo, Finland**

**FCC ID:** 2AJOTTA-1500

Software Security Requirement Description for UNII Devices

**II. 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.<br><br>For users can update the software by OTA. Users can update SW through setting---system update. But upgrade methods only can upgrade the operating system and built-in application software, the radio frequency parameter will not change. |
| | 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?<br><br>The radio frequency parameter stored in non-volatile memory, and it cannot be modified by end user except our professional service engineer used special tools and drivers. |
| | 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.<br><br>The devices radio frequencies was controlled by the radio frequency parameter which store in non-volatile memory. And the radio frequency parameter need special tools and special drivers to re-flesh. |
| | 4. Describe in detail any encryption methods used to support the use of legitimate RF-related software/firmware.<br><br>The radio frequency parameter was produced by special software after calibrated. Software is provided with key encryption that is unknown to anyone else. And these information are differences in each country. If the radio frequency parameter is not matched with the devices, the upgrade process will be automatically forced stopped by devices upgrade software. |

| | |
|---|---|
| | 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?<br><br>The devices was design as a client without radar detection function. For the DFS compliance, please refer DFS test report. |

| | |
|---|---|
| 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.<br><br>Frequency parameter will be hidden in the system, no third-parties will get rights to modify system property and files. except our-self. |
| | 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<br><br>The radio frequency parameter is not easily be re-fresh by the third parties, it must be re-fresh by a special tools and special drivers, what more our devices upgrade software will compare the new parameter, if it's not correct the upgrade process will be automatically forced. |

| | |
|---|---|
| | 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.<br><br>Our devices is a end product not a modular devices, and its function cannot working as a modular devices. |

## III. SOFTWARE CONFIGURATION DESCRIPTION GUIDE

| | |
|---|---|
| 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.<br><br>There is no need a professional installer for our devices. The UI had same level for the all user. |
| | a) What parameters are viewable and configurable by different parties?<br><br>The end user only authorized tune on/off radios, and 2.4G band/ 5G band mode selection. |
| | b) What parameters are accessible or modifiable by the professional installer or system integrators?<br><br>There is no need a professional installer for our devices. |
| | (1) Are the parameters in some way limited, so that the installers will not enter parameters that exceed those authorized?<br><br>There is no need a professional installer for our devices. |
| | (2) What controls exist that the user cannot operate the device outside its authorization in the U.S.?<br><br>The RF parameters of each country code are set in factory and the country code cannot be modified selected by operator、installer、user. |

| | |
|---|---|
| | b) What parameters are accessible or modifiable to by the end-user?<br><br>The end user only authorized tune on/off radios, and 2.4G band/ 5G band mode selection, and cannot modify any radio parameters. |
| | (1) Are the parameters in some way limited, so that the installers will not enter parameters that exceed those authorized?<br>The end user only authorized tune on/off radios, and 2.4G band/ 5G band mode selection, and cannot modify any radio parameters. |
| | (2) What controls exist that the user cannot operate the device outside its authorization in the U.S.?<br><br>The RF parameters of each country code are set in factory and the country code cannot be modified selected by operator、installer、user. |
| | c) Is the country code factory set? Can it be changed in the UI?<br><br>The RF parameters of each country code are set in factory and the country code cannot be modified selected by operator、installer、user. There is no UI to change country code on the device.. |
| | (1) If so, what controls exist to ensure that the device can only operate within its authorization in the U.S.?<br><br>The RF parameters of each country code are set in factory and the country code cannot be modified selected by operator、installer、user. |
| | e) What are the default parameters when the device is restarted?<br><br>If devices restarted the built-in operating software will re-check his location and automatic import the correct RF parameter. |
| | 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.<br><br>No, this devices cannot be configured in bridge or mesh mode. |

| | |
|---|---|
| | 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?<br><br>This device was designed as a client without radar detection function. |
| | 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))<br><br>The device cannot be change to operate mobile hotspot in point-point/point-smultipoint modes. |