| | |
|---|---|
| Shanghai EFIX Geomatics Co., Ltd<br>Room 1137, Area D, 11th Floor, Building<br>1, No. 158, Shuanglian Road, Qingpu<br>District, Shanghai<br><br>Date: June 28, 2025<br><br>FCC ID: 2A3MU-F61W<br>Model Number : Geodetic GNSS Receiver | |
| **Software Security Description – KDB 594280 D02v01r03 Section II** | |
| **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>Software/firmware will be obtained by the factory, downloaded from the ODM website, and installed by the end user.<br>Software is accessed through Web UI when computer is connected. |
| | 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>The RF parameters cannot be modified by software.<br>All these parameters will not exceed the authorized parameters. The firmware has been complied as binary file. It couldn't change the setting RF parameter through this binary file. It is read-only without change. |
| | 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>No any authentication protocol is used. The RF Parameters is put in read-only partition of EUT's flash and are only installed in the factory. RF parameters including frequency of operation, power setting, modulation type, antenna types or country code setting will be locked in this partition. |
| | 4. Describe in detail any encryption methods used to support the use of legitimate RF-related software/firmware.<br>No encryption methods used. |
| | 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>This is a client device without Radar detection. |
| **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>No any third parties have the capability to operate a US 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. |

| | |
|---|---|
| | 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>The RF Parameters is put in read-only partition of EUT's flash and are only installed in the factory. RF parameters including frequency of operation, power setting, modulation type, antenna types or country code setting will be locked in this partition. |
| | 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>User couldn't change channel for UI, so user has no way to break compliance on our device. |

**Software Configuration Description – KDB 594280 D02v01r03 Section III**
**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.

a. What parameters are viewable and configurable by different parties?

b. What parameters are accessible or modifiable by the professional installer or system integrators?

(1) Are the parameters in some way limited, so that the installers will not enter parameters that exceed those authorized?

Yes.

(2) What controls exist that the user cannot operate the device outside its authorization in the U.S.?

The RF Parameters is put in read-only partition of EUT's flash and are only installed in the factory. RF parameters including frequency of operation, power setting, modulation type, antenna types or country code setting will be locked in this partition.

c. What parameters are accessible or modifiable by the end-user?

(1) Are the parameters in some way limited, so that the installers will not enter parameters that exceed those authorized?

Yes.

(2) What controls exist that the user cannot operate the device outside its authorization in the U.S.?

Authorized channel, bandwidth, and modulation.

d. Is the country code factory set? Can it be changed in the UI?

(1) If it can be changed, what controls exist to ensure that the device can only operate within

its authorization in the U.S.?
Yes, the country code is set by factory. It cannot be changed in the UI.

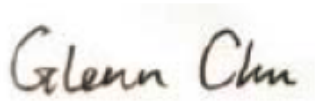
e. What are the default parameters when the device is restarted?
Factory setting.

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.
No, this device cannot be configured in both bridge and 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?
User couldn't change channel for UI, so user has no way to break compliance on our device.

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))
This device cannot be configured as Different types of access points.

(Signature)



**June 28, 2025**



| | |
|---|---|
| Name | Glenn Chu |
| Position | Certificate Manager |
| Company Name | Shanghai EFIX Geomatics Co., Ltd |
| Address | Room 1137, Area D, 11th Floor, Building 1, No. 158, Shuanglian Road, Qingpu District, Shanghai |
| Tel | +8675529766001 |
| Fax | / |
| Email | 359662367@qq.com |