The information within this section of the Operational Description is to show compliance against the Software Security Requirements laid out within KDB 594280 D02 U-NII Security v01 r03.

The information below describes how we maintain the overall security measures and systems so that only:

1. Authenticated software is loaded and operating on the device
2. The device is not easily modified to operate with RF parameters outside of the authorization

| **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. | Kyocera provide the software to Mobile Network Operator, and only OTA(Over the Air) download is available for the software/firmware update. |
| 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? | The following parameters are configured by NV(Non-Volatile) file in the file system.<br>- frequency and bandwidth<br>- scan method (active/passive)<br>- maximum power level at each frequency<br>- power level at each rate<br>- RSSI offset<br>This is binary formats, and the user cannot access nor modify it.<br><br>Kyocera choose the frequencies for each products from the list below:<br>4920-4980MHz<br>5040-5080MHz<br>5180-5320MHz<br>5500-5700MHz<br>Active channel setting example:<br>setting parameter<br>0: disable<br>1: enable with active scanning<br>2: enable with passive scanning<br><br>In the case of EA34, the following frequencies/ band width are selected as passive scanning: 2 to use in US or US territories<br>Other frequencies/ band width are prohibited as disable: 0 to ensure the compliance.<br><br>5180-5240 (20MHz step/ 20MHz BW)<br>5260-5320 (20MHz step/ 20MHz BW)<br>5500-5700 (20MHz step/ 20MHz BW)<br>5190-5310 (40MHz step/ 40MHz BW)<br>5510-5670 (40MHz step/ 40MHz BW)<br>5210, 5290, 5530, 5610 (80MHz BW) |

| General Description | |
|---|---|
| 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. | "Qualcomm Secure Boot" is used for authentication protocol and only legitimate software/firmware can be installed. |
| 4. **Describe *in detail*** any encryption methods used to support the use of legitimate RF-related software/firmware. | No encryption methods used for the software/firmware update. |
| 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? | For EA34, only client mode is available in U-NII bands. The master mode is not permitted. |

| 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. | EA34 is release to Japanese market only. For US and US territories, the device operates as item 2 in "General Description". Thus, no violation happens. |
| 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. | 3rd Party does not have a capability to load the software/firmware. In addition, EA34 is released to Japanese market only, and non-US version software/firmware does not exist. |
| 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[1] | EA34 is not modular device. |

[1] Note that Certified Transmitter Modules must have sufficient level of security to ensure that when integrated into a permissible host the device's RF parameters are not modified outside those approved in the grant of authorization. (See, KDB Publication 99639). This requirement includes any driver software related to RF output that may be installed in the host, as well as, any third-party software that may be permitted to control the module. A full description of the process for managing this should be included in the filing.

| SOFTWARE CONFIGURATION DESCRIPTION GUIDE – USER CONFIGURATION GUIDE[2] | |
|---|---|
| 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. | The professional installers, system integrators and end-users can access UI such as Wi-Fi turn on, Wi-Fi scan on. However, professional installers, system integrators , end-users cannot view, nor access, nor modify the parameters that is related with compliance (frequency of operation, power settings, DFS settings, receiver thresholds, or country code settings. etc) |
| a) What parameters are viewable and configurable by different parties?[3] | The compliance related parameters are not viewable to the professional installer/end-user. |
| b) What parameters are accessible or modifiable by the professional installer or system integrators? | The compliance related parameters are not accessible/ modifiable to the professional installer/system integrators. |
| i) Are the parameters in some way limited, so that the installers will not enter parameters that exceed those authorized? | The compliance related parameters cannot be modified. |
| ii) What controls exist that the user cannot operate the device outside its authorization in the U.S.? | EA34 has only one configuration for US and US territories, and it cannot be modified by the user. |
| c) What parameters are accessible or modifiable by the end-user? | The end-user cannot access nor modify the compliance related parameters. |
| i) Are the parameters in some way limited, so that the user or installers will not enter parameters that exceed those authorized? | The compliance related parameters cannot be modified. |
| ii) What controls exist so that the user cannot operate the device outside its authorization in the U.S.? | EA34 has only one configuration for US and US territories, and it cannot be modified by user. |
| d) Is the country code factory set? Can it be changed in the UI? | EA34 is released to Japanese market only. Thus, the country code does not set in the factory. The configuration is defined by NV file and it cannot be modified by UI. |
| i) If it can be changed, what controls exist to ensure that the device can only operate within its authorization in the U.S.? | It cannot be changed. |
| e) What are the default parameters when the device is restarted? | The default parameters are defined by NV files that are described item 2 in “General Description”. |
| 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. | EA34 does not support bridge nor 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? | EA34 supports only single Client mode in U-NII band. The end-user cannot modify the mode settings. |

[2] See KDB Publication 594280 D01Software Configuration Control for Devices. The document provides guidance for devices permitting device configurations and limitations on configuration parameters accessible to the third-parties in which the software is designed or expected to be modified by a party other than the manufacturer and would affect the RF parameters of the Software Defined Radio (SDR).

[3] The specific parameters of interest for this purpose are those that may impact the compliance of the device (which would be those parameters determining the RF output of the device). These typically include frequency of operation, power settings, antenna types, DFS settings, receiver thresholds, or country code settings which indirectly programs the operational parameters.

| **SOFTWARE CONFIGURATION DESCRIPTION GUIDE – USER CONFIGURATION GUIDE[2]** | |
|---|---|
| 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)) | EA34 does not operate as Access Point in U-NII band. |