Software Security Description – KDB 594280 D02v01r03	
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. - The part to modify both 2.4GHz and 5GHz are stipulated by SSID, and controled by password, and modification control is done only by end-user administorator.
	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? - RF parameter is embedded in firmware and neither MORITEX and customers cannot modify them. It is restricted not exceed permitted RF characteristics.
	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. - The RF related source is stored and managed at MORITEX's developer company and locked inside. Thus, RF related modification is executed only at MORITEX's developer company.
	4. Describe in detail any encryption methods used to support the use of legitimate RF-related software/firmware. - The RF related source is written in binary code, and unable to modify them.
	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? - RF of the products has infrastructure mode and Soft AP mode. These are switchable by software.
Third-Party Access Control	1. Explain if 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 US. - Firmware which correspondence to even outside of Taiwan allows user to operate regulation domain of Wi-Fi module and frequency.
	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 its authorization for operation in the US. In the description include what controls and /or agreements are in place with providers of third-party functionality to ensure the device’s underlying RF parameters are unchanged and how the manufacturer verifies the functionality. - Only firmware of Wi-Fi module with Worldwide version is provided.
	3. For Certified Transmitter modular devices, describe how the module grantee ensures that host manufactures 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.

	- Since the module is not certified module, the security requirement for software as U-NII device is not related, even if it is related, no others can modify parameter except MORITEX's developer company.
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. - The part to modify both 2.4GHz and 5GHz are stipulated by SSID, and controlled by password, and modification control is done only by end-user administrator.
	a. What parameters are viewable and configurable by different parties? - They are no part related to RF.
	b. What parameters are accessible or modified by the professional installer or system integrators? - They are no part related to RF.
	(1) Are the parameters in some way limited, so that the installers will not enter parameters that exceed those authorized? - There are no parameters which can be executed by installer.
	(2) What controls exist that the user cannot operate the device outside its authorization in the US? - Not especially.
	c. What parameters are accessible or modifiable by the end-user? - SSID, password and encryption types.
	(1) Are the parameters in some way limited, so that the user or installers will not enter parameters that exceed those authorized? - This is managed by password.
	(2) What controls exist so that the user cannot operate the device outside its authorization in the US? - Remains blank, because the contents is duplicated with b (2)
	d. Is the country code factory set? Can it be changed in the UI? - Since only firmware of Wi-Fi module with Worldwide version is provided, there are no country codes.
	(1) If it can be changed, what controls exist to ensure that the device can only operate within its authorization in the US? - No
	e. What are the default parameters when the device is restarted? - No
	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

	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 exit, 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? - The setting of master and client is modifiable. Frequency channel can be settled as master.
	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)) - Antenna cannot be modified, because it is installed inside of the products and unable to disassemble.

Sincerely,

Hitoshi Yoshida

Name: Hitoshi Yoshida

Title: Senior Project Manager
Moritex Corporation

Date: May 17th, 2018