

SOFTWARE SECURITY DESCRIPTION

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.

An applicant must describe the overall security measures implemented in the device that ensure that the device cannot be modified by any RF-related software changes by third parties to operate outside the authorized RF parameters without further approval from the FCC.

The description of the RF-related software must address the following questions in the operational description for the device and clearly demonstrate how the device meets the RF-security requirements.⁵ While the Commission did not adopt any specific standards, it is suggested that the manufacturers may consider applying existing industry standards for security.⁶

This guide is not intended to be exhaustive and may be modified in the future. There may be follow-up questions based on the responses provide by the applicant for authorization.

SOFTWARE SECURITY DESCRIPTION	
General Description	1. Describe how any software/firmware updates for elements that 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. <i>Re: It is bundled as part of a Software update, where user or installer cannot modify the content. All Installation & update proceeds automatically once user accepts to update and install through Samsung website or device management system.</i>
	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? <i>RF parameters are fixed and not altered in FW update.</i>
	3. Describe in detail the authentication protocols that are in place to ensure that source of the RF-related software/firmware is valid. Describe in detail how the RF-related software is protected against modification. <i>The software version is distributed to the host integrators as a pre-built binary driver preventing any end user modifications. The Firmware/Flash is released to the host integrator /wireless module CM so it is a controlled release.</i>
	4. Describe in detail any encryption methods used to support the use of legitimate RF-related software/firmware. <i>No encryption, but module firmware is a binary code.</i>
	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? <i>A single Firmware is provided to the Module Manufacturer for Client and a single Firmware is provided for Master. There are no modes in which Client FW will / can act as Master and there are no modes in which the Master can act as Client.</i>
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. <i>There is no operation by third parties. Driver FW is created by Avnera Corporation, released to module manufacturer and completed module is installed into end product.</i>
	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 device's underlying RF parameters are unchanged and how the manufacturer verifies the

	functionality. Re: It is impossible. All the manufactured products do not support any third party firmware upgrade. All FW is created by Avnera nd Released to the module manufacturer. Third party development company or organizations are not supported
	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. All drivers are included in the module. No drivers are located external to the module.

SOFTWARE CONFIGURATION DESCRIPTION GUIDE

In addition to the general security consideration, for devices which have “User Interfaces” (UI) to configure the device in a manner that may impact the operational RF parameters, the following questions shall be answered by the applicant and the information included in the operational description. The description must address if the device supports any of the country code configurations or peer-peer mode communications discussed in KDB 594280 Publication D01.⁸

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. Re: There is not any UI to access RF parameter / protocol setting.
	a) What parameters are viewable and configurable by different parties? Re: No RF parameters or protocols are accessible by a third party.
	b) What parameters are accessible or modifiable by the professional installer or system integrators? Re: There is not any RF parameter which is accessible or modifiable to the professional installer.
	(1) Are the parameters in some way limited, so that the installers will not enter parameters that exceed those authorized? Re: Parameters are not accessible.
	(2) What controls exist that the user cannot operate the device outside its authorization in the U.S.? Re: There is no user control of RF parameters.
	C) What parameters are accessible or modifiable by the end-user? Re: None
	(1) Are the parameters in some way limited, so that the user or installers will not enter parameters that exceed those authorized? Re: RF Parameters may not be modified.
	(2) What controls exist so that the user cannot operated the device outside its authorization in the U.S.? Re : RF parameters may not be modified
	D) Is the country code factory set? Can it be changed in the UI? Re: There is a single Firmware Driver, there is no country code.
	(1) If it can be changed, what controls exist to ensure that the device can only operate within its authorization in the U.S.? Re : N/A
	E) What are the default parameters when the device is restarted? Re: All default parameters are programmed in the single binary or in both driver and firmware which would be embedded in system firmware. The system firmware is programmed and protected in flash memory. The professional installer/end-user cannot access the flash memory.
	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. Re: Not supported
	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? Re: No. End-use cannot configure the device to be as a master or client.
	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)) Re: This product is not an access point.