Speedata Group Ltd

SOFTWARE SECURITY DESCRIPTION

An applicant must describe the overall security measures and systems that ensure that only:

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

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

The device comply with KDB 594280D01 and D02

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.. The software updates are given to customer via official WEB page, and there will be a installed instruction on the webpage, and the related info and documents are open to public.
	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? All the parameter limitations are hard-coded into special permanent memory space to not exceed the authorized limits. Professional installer has no acces to change radio parameter limits.
	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. To protect software copywriting or modifications every device has a license which is bonded to a MAC address. Any software modification will end up with a voided license which in turn will prohibit further product usage.
	4. Describe in detail any encryption methods used to support the use of legitimate RF-related software/firmware.. All manufactured product have unique MAC address, unique license and a special product limitation parameters , WEP, WAP, WAP-2 encryption methods are 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? Since the software can work in both modes (Master and Client) software was developed to update limitations,during configuration, instantly to meet compliance in any operating mode. Only authorized operating bands are allowed to configure by the professional installer.
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.. No, the product can be operated in a non-US domain only if the non-US domain supports the US Band and US voltage.
	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. The product Radio Frequency (RF) calibration information is written in non-standard way, thus making impossible for the third party to develop a software manufactured devices.
	3. For Certified Transmitter modular devices, describe how the module grantee ensures that hosts 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 parameters are not modified outside the grant of authorization. Products, which are certified as End product are used only with original software as well. This way protecting illegal device configuration or use.

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 parameter, 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.

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 Professional installer
	a) What parameters are viewable to the professional installer/end-user? The software has access to below listed radio parameters: - Operating frequency - Channel width (e.g. 20MHz, 40MHz) - Modulation and coding rate - Transmitter power - Spacial streams number - Guard interval between transmitted symbols These parameters cannot exceed authorized parameters.
	b) What parameters are accessible or modifiable to the professional installer? The professional installer may change below listed parameters: - Operating frequency - Channel width (e.g. 20MHz, 40MHz) - Modulation and coding rate - Transmitter power - Spacial streams number - Guard interval between transmitted symbols These parameters cannot exceed authorized parameters.
	i. Are the parameters in some way limited, so that the installers will not enter parameters that exceed those authorized? Re:Yes
	ii. What controls exist that the user cannot operate the device outside its authorization in the U.S.? Each product is built specifically to meet region regulations (e.g. US). that product for US region are limited to US country code only. The professional installer can not change the country code.
	c) What parameters are accessible or modifiable by the end-user? Re: The end-user gets the service options.
	i. Are the parameters in some way limited, so that the installers will not enter parameters that exceed those authorized? YES

	ii. What controls exist that the user cannot operate the device outside its authorization in the U.S.? Each product is built specifically to meet region regulations (e.g. US). that product for US region are limited to US country code only. The professional installer can not change the country code.
	d) Is the country code factory set? Can it be changed in the UI? Yes, the country code is set by factory.it can not be changed in the 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.? Each product is built specifically to meet region regulations (e.g. US). that product for US region are limited to US country code only. The professional installer can not change the country code.
	e) What are the default parameters when the device is restarted? Country of USA, 802.n HT20, and channel of 5200MHz are the default parameters when device is restarted.
	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. The radio can be configured in bridge. we make sure our products comply with regulations KDB Publication 905462 D02. The product is restricted to not use the DFS band and the emissions are not fall into the DFS band.
	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? The device can be configured as a master, but this is not user configurable.
	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)) The device can be only configured with fixed integral point to point antennas, it can not be changed.

Sincerely,

Huang Jianning

Signature

[Name] Huang Jianning

[Title] Oversea Manager

[Company] Speedata Group Ltd

[Address] Room 2-308, building No. 25, No. 9 Anningzhuang Road West, Haidian district, Beijing, China