Alcatel-Lucent Shanghai Bell Co., Ltd.

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, including those that may affect the device's RF parameters can be downloaded via three methods:
	    The uplink OLT device from the network service provider.
	    Network Management devices from the network service provider.
	    Local Webpage from LAN port via https & super user authentication.

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 software is able to modify the Mode, Bandwidth, working channel, transmit Power. The unit includes radio parameters to limit to its power output and channels it operates on to match the authorized RF characteristics in the regulatory domain that it was originally shipped in regardless of what is set through the UI, and the UI also does not show settings which would violate the authorized 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 software is encrypted with integrity check to ensure the validity of its content. Without passing the firmware integrity check, no upgrade will be performed.
4	Describe in detail any encryption methods used to support the use of legitimate RF-related software/firmware. These encryption & security methods were implemented in the SW to protect against modification of software by unauthorized parties: SSL/SSH/HTTPS/Image digital signature base on DSA algorithm.
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? This device can only be configured as master mode. User can only configure the parameters for GUI within ROM pre-set authorized range, so user has no way to break compliance on our device.

Alcatel-Lucent Shanghai Bell Co., Ltd.

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. Not possible.
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. Not possible.
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. Not possible.

Alcatel-Lucent Shanghai Bell Co., Ltd.

SOFTWARE CONFIGURATION DESCRIPTION

USER CONFIGURATION GUIDE

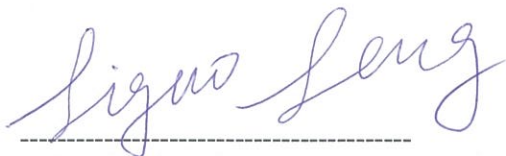|	
1	Describe the user configurations permitted through the UI. If different levels of access are permitted for professional installers, system integrators or end-users, describe the differences. a. What parameters are viewable and configurable by different parties? Mode, Bandwidth, Channel, Transmit Power, SSID, Security Type, but only within ROM pre-set authorized range. b. What parameters are accessible or modifiable by the professional installer or system integrators? Same as above. (1) Are the parameters in some way limited, so that the installers will not enter parameters that exceed those authorized? All above parameters have pre-defined range according to the certification test result. They are stored in the ROM flash and shown in UI, which no allow user to adjust beyond the pre-set value. (2) What controls exist that the user cannot operate the device outside its authorization in the U.S.? All parameters indicating different countries are permanent setting in the ROM, so if a device is a product for US, it cannot be changed for another region. c. What parameters are accessible or modifiable by the end-user? Mode, Bandwidth, Channel, Transmit Power, SSID, Security Type, but only within ROM pre-set authorized range. (1) Are the parameters in some way limited, so that the user or installers will not enter parameters that exceed those authorized? All above parameters have pre-defined range according to the certification test result. They are stored in the ROM flash and shown in GUI, which no allow user to adjust beyond the pre-set value. (2) What controls exist so that the user cannot operate the device outside its authorization in the U.S.? All parameters indicating different countries are permanent setting in the ROM, so if a device is a product for US, it cannot be changed for another region. d. Is the country code factory set? Can it be changed in the UI?

	It is factory set and cannot be changed in the GUI. (1) If it can be changed, what controls exist to ensure that the device can only operate within its authorization in the U.S.? N/A. e. What are the default parameters when the device is restarted? Mode, Bandwidth, Channel, Transmit Power, SSID, Security Type, but only within ROM pre-set authorized range.
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 cannot be configured in bridge or 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? This device can only be configured as master mode. User can only configure the parameters for GUI within ROM pre-set authorized range, 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)) The device does not support point-to-point & point-to-multipoint operation, and does not support use different types of antennas.

Date: May 27, 2017

Liguo Leng

Liguo Leng / HW Consultant Engineer

Alcatel-Lucent Shanghai Bell Co., Ltd.
Tel: 86-21-38434963
Email: Liguo.Leng@alcatel-sbell.com.cn