Software security for UNII Devices

Neutrik AG

Im alten Riet 143

9494 Schaan, Liechtenstein

To Whom It May Concern:

Product/Model/HVIN: XIRIUM PRO / NXP2TX / NXP2TX-C

FCC ID: 2ABA7XPT

IC ID: 11536A-XPT

SOFTWARE SECURITY REQUIREMENTS FOR U-NII DEVICES acc. to KDB 594280

SOFTWARE CONFIGURATION 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 initial software and firmware are flashed during the manufacturing process of the device. Subsequent firmware update are downloaded from the manufacturer's website onto a PC and flashed onto the device by connecting the device to the PC by using a USB cable.
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? Change of WLAN radio frequency channels are done through the software/firmware. The transmission power is also managed by software such that it does not exceed the authorized power values.
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 can only be downloaded from the manufacturer's website. The firmware update software ensures and checks the version and type of firmware in the existing device and the version and type of firmware to be updated and allows the update only when these checks are successful. A GUI application that can connect to the device reads back and verifies that the firmware is proper.
4	Describe in detail any encryption methods used to support the use of legitimate RF-related software/firmware. No encryption methods.
5	For a device that can be configured as a master and client (with active orpassive 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? The device cannot be configured as a client. A master device always acts as master in all operating bands.
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. The customer can choose only between FCC approved channels according to the device's authorization. The transmission power is limited to the maximum authorized level.
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 firmware can be flashed only by a legitimate firmware updater provided by the manufacturer. The firmware updater ensures that only US firmware versions can be flashed onto the device.
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. No modular transmitter parameters are accessible or being controlled

	by the host.
	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. The device is intended for use in professional applications only, with users ranging from professional installers to professional audio technicians. Therefore different levels of user access are not implemented.
1.a	What parameters are viewable and configurable by different parties? RSSI signal strength, battery status, delay status, device name, RF channel, transmission power
1.b	What parameters are accessible or modifiable by the professional installer or system integrators? delay time, device name, RF channel, transmission power (within permissible limits)
1.b(1)	Are the parameters in some way limited, so that the installers will not enter parameters that exceed those authorized? Yes, on all available and permissible channels the power is limited to the authorized value.
1.b(2)	What controls exist that the user cannot operate the device outside its authorization in the U.S.? The customer can choose only between FCC approved channels according to the device's authorization. The transmission power can only be set to the maximum authorized level.
1.c	What parameters are accessible or modifiable by the end-user? Same as under 1.b
1.c(1)	Are the parameters in some way limited, so that the user or installers will not enter parameters that exceed those authorized? Same as under 1.b(1)
1.c(2)	What controls exist so that the user cannot operate the device outside its authorization in the U.S.? Same as under 1.b(2)
1.d	Is the country code factory set? Can it be changed in the UI? Yes, factory set by default. It can be changed in the UI.

1.d(1)	If it can be changed, what controls exist to ensure that the device can only operate within its authorization in the U.S.? The alternative country setting for Europe requires limited choice of channels and reduced power levels. Changing the country code would not violate U.S. authorization.
1.e	What are the default parameters when the device is restarted? Radio frequency channel is channel 48. Power level is restored from saved value and does not exceed what is allowed on that channel.
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 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? Device operates as master only. UI software cannot control this.
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)) Authorization is based on use of antennas with gain of 9 dBi at the maximum conducted power level. Additionally provided antennas exhibit lower antenna gain and therefore compliance with power limits is guaranteed.

M. Natter

Markus Natter, Senior Standards Engineer

Neutrik AG

Im alten Riet 143

9494 Schaan, Liechtenstein

Phone: 00423 / 237 2424