Amino Communications Ltd
1010 Cambourne Business Park, Cambourne, Cambridge, CB23 6DP, United Kingdom

Software Security Requirements for U-NII Devices

Date: 30 August 2024

FCC: XVG500107APBT

ISED: 6800A-500107APBT

Subject: Attestation Letter regarding UNII devices

Software security questions and answers per KDB 594280 D02v01R03:

Software Security Description – KDB 594280 D02v01r03 Section II	
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.
	Description: **Firmware is signed and encrypted by Amino's own key before releasing to operator or uploading to management server. Once new firmware is downloaded to the STB, STB will verify signature and then decrypt the image before upgrading the image to STB.**
	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?
	Description: **Radio frequency parameters are limited by US regulatory domain and country code to limit frequency and transmit power levels. All the Wi-Fi RF parameters are hardcoded in Amino signed firmware and cannot be changed.**
	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.
	Description: **Amino receives RF-related software from component vendors via a secure file transfer service hosted by Amino. Separate user accounts are issued to different vendors. Amino verifies updates from vendors before applying them in new firmware releases.**

	4. Describe in detail any encryption methods used to support the use of legitimate RF-related software/firmware.
	Description: **The SoC on the product is OTP fused to only allow booting from Amino signed bootloader. A chain of trust from the boot loader ensures that the box can only load and run Amino signed firmware packages. The RF-related software and parameters are packaged with the Amino firmware in a read-only partition. Amino strives to follow the best practice for software development cybersecurity in our processes to protect the signing keys and ensure only authorized firmware packages are released.**
	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?
	Description: **Compliance is verified during testing for FCC certification. The configuration required for compliance is then hardcoded in the firmware and cannot be modified by end user. The device is configured as a client without radar detection capability.**
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.
	Description: **Third parties do not have capability to change regulatory domain on the product. Units sold in the U.S. are factory configured for US.**
	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.
	Description: **No third-party firmware can be installed on the product. While third party applications can be installed, Amino firmware ensures that the underlying RF parameters and read-only and cannot be changed by applications.**

	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.
	Description: **N/A.**

Software Configuration Description – KDB 594280 D02v01r03 Section III **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? **Ans: There is no configuration interface for RF parameters. The country code is factory set. There are no different levels of access permitted for professional installers, system integrators or end-users.**
b. What parameters are accessible or modifiable by the professional installer or system integrators? (1) Are the parameters in some way limited, so that the installers will not enter parameters that exceed those authorized? **Ans: There is no configuration interface for RF parameters. The country code is factory set. There are no different levels of access permitted for professional installers, system integrators or end-users.**
(2) What controls exist that the user cannot operate the device outside its authorization in the U.S.? **Ans: There is no configuration interface for RF parameters. The country code is factory set. There are no different levels of access permitted for professional installers, system integrators or end-users.**
c. What parameters are accessible or modifiable by the end-user? (1) Are the parameters in some way limited, so that the installers will not enter parameters that exceed those authorized? **Ans: There is no configuration interface for RF parameters. The country code is factory set. There are no different levels of access permitted for professional installers, system integrators or end-users.**
(2) What controls exist that the user cannot operate the device outside its authorization in the U.S.? **Ans: There is no configuration interface for RF parameters. The country code is**

factory set. There are no different levels of access permitted for professional installers, system integrators or end-users.

d. Is the country code factory set? Can it be changed in the UI?

(1) If it can be changed, what controls exist to ensure that the device can only operate within its authorization in the U.S.?

Ans: There is no configuration interface for RF parameters. The country code is factory set. There are no different levels of access permitted for professional installers, system integrators or end-users.

e. What are the default parameters when the device is restarted?

Ans: Units sold in the US have factory set country code. The default parameters are certified for FCC compliance.

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.

Ans: Bridge or mesh mode are 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?

Ans: The device supports Wi-Fi Direct. The feature is enabled by default and not configurable. Compliance is verified during FCC testing.

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))

Ans: The device cannot be configured as different types of access points. Only one type of antenna is supplied.

Signature:

Name: Victor Tse

Title: VP, Development and Engineering

Company name: AMINO COMMUNICATIONS LTD.