Company: Sahara Presentation Systems Ltd

Address: Europa House, Littlebrook DC1, Shield Road, Dartford, Kent, United Kingdom

Product Name: Clevershare Hub, CleverHub

Model Number(s): Clevershare Hub, CleverHub

FCC ID: 2APKO-WB05

SOFTWARE SECURITY REQUIREMENTS FOR U-NII DEVICES REF KDB 594280 D02 U-NII Device Security v01r03		
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.	We do not release the firmware on our website for downloading. Our direct host manufacturer (OEM) can request the firmware from us and it will be made available via secure server.
	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 nay other software/firmware changes will not allow the device to exceed the authorized RF characteristics?	The configuration file can modify the transmit power and frequency offset; but configuration files can only be modified in the factory.
	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 firmware binary is encrypted. The process to flash a new firmware is using a secret key to decrypt the firmware, only correct decrypted firmware is stored in non-volatile memory.
	4. Describe in detail any encryption methods used to support the use of legitimate RF-related software/firmware.	Standard openSSL encryption is used (see #3).
	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?	The device ensures compliance by checking the configured parameter and operation values according to the regulatory domain and country code in each band. Working in band U-NII-1, and U-NII-3, the device complies with both passive and active scanning, while in band UNII-2A, UNII-2C complies only with passive scanning, which

		would be configured in the manufacturer's firmware.
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, third parties don't have the capability to access and change radio parameters. US sold modules are factory configured to 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.	The embedded software is protected via the measures explained in the previous section. Distributions of host operating software are encrypted with a key.
	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.	N/A. The device doesn't contain Certified Transmitter modular.

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 UI is accessible to anyone using the device.
	a) What parameters are viewable and configurable by different parties?	None of the RF parameters are viewable or configurable by different parties.
	b) What parameters are accessible or modifiable by the professional installer or system integrators?	This device is not subject to professional installation.
	(1) Are the parameters in some way limited, so that the installers will not enter parameters that exceed those authorized?	
	(2) What controls exist that the user cannot operate the device outside its authorization in the U.S.?	

	c. What parameters are accessible or modifiable by the end-user?	The end user cannot modify any RF options.
	(1) Are the parameters in some way limited, so that the user or installers will not enter parameters that exceed those authorized?	The built in regulatory settings cannot be changed by the end-user.
	(2) What controls exist so that the user cannot operate the device outside its authorization in the U.S.?	The authorization will be obtained and set well in the firmware before shipped.
	d. Is the country code factory set? Can it be changed in the UI?	All parameters (Power, Frequencies, etc.) apply to different countries and are permanent settings in the ROM. If it's a device selling to the US, it cannot be changed to another region 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.?	N/A
	e. What are the default parameters when the device is restarted?	At each start, the factory-configured country code and antenna gain are read from non-volatile 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.	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?	Not user configurable in the UI.
	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)	Not supported. There is only one type of AP.

Sincerely,

Name: Robert Xenos Robert Xenos

Date: August 21, 2023