Shenzhen Chuangwei Electronic Appliance Tech Co., Ltd.
4F & 6F, Overseas plant south, Skyworth Industrial Park, Shiyan Street, Bao'an District, Shenzhen, China

Date: 2022-01-23

SOFTWARESECURITYREQUIREMENTS FORU-NII DEVICES
(594280 D02 U-NII Device Security 1.3,11/12/15)

Company Name: Shenzhen Chuangwei Electronic Appliance Tech Co., Ltd.
FCC ID: 2AABK-SKYV3
Product Name: 10 inch WIFI Digital Photo Frame
Model: SKY-V3, D106, Skylight 3

SOFTWARE SECURITY DESCRIPTION	
GeneralDescription	
Q.	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.
A.	The end users can not change the device's RF parameters by OTA or firmware upgrade.
Q.	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?
A.	The RF parameters are written in IC,The power output can be changed by IC manufacture only.
Q.	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.
A.	We use keys to protect against modification. The keys embedded in the IC should match with the one in the firmware.
Q.	4. Describe in detail any encryption methods used to support the use of legitimate RF-related software/firmware.
A.	AES encryption keys
Q.	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?
A.	The compliance for each mode are controlled by Windows or Linux stack instruction. The device of any software or any software we own have no authority to place the adapter in these mode.

Third-PartyAccessControl	
Q.	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.
A.	There is no third party has these capability.
Q.	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.
A.	Only the IC Supplier encrypte key to load MAC address can add the firmware into the products.
Q.	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.
A.	The host manufacture OS capabilities are restrict through the IC hardware. Drivers are controlled by encrypted keys.

SOFTWARE CONFIGURATIONDESCRIPTION USER-CONFIGURATIONGUIDE	
Q.	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.	No transmitter configuration is controllable through Ui. The output power and modulation are restricted by radio and antenna design.
Q.	a. What parameters are viewable and configurable by different parties?[9]
A.	No parameters are viewable or configurable by different parties.
Q.	b. What parameters are accessible or modifiable by the professional installer or system integrators?
A.	No parameters is accessible by the professional installer.
Q.	(1) Are the parameters in some way limited, so that the installers will not enter parameters that exceed those authorized?
A.	Yes
Q.	(2) What controls exist that the user cannot operate the device outside its authorization in the U.S.?

A.	Before the product deliver out of the manufacture, the RF parameters, frequency, power, bandwidth, are set by initial software. And can not be changed by professional installer or system integrator
	c. What parameters are accessible or modifiable by the end-user?
	None
Q.	(1) Are the parameters in some way limited, so that the user or installers will not enter parameters that exceed those authorized?
A.	Yes
Q.	(2) What controls exist so that the user cannot operate the device outside its authorization in the U.S.?
A.	Before the product deliver out of the manufacture, the RF parameters, frequency, power, bandwidth, are set by initial software. And cannot be changed by end user.
Q.	d. Is the country code factory set? Can it be changed in the UI?
A.	Yes. The factory sets the country code. There is no country code on the system UI. so it can't be changed in the system UI.
Q.	(1) If it can be changed, what controls exist to ensure that the device can only operate within its authorization in the U.S.?
A.	No, It can't be changed.
Q.	e. What are the default parameters when the device is restarted?
A.	The default parameters are set by the stack in OS or connect to the network.
Q.	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.
A.	No.
Q.	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?
A.	A firmware key encryption is allowed to release such a parameter and it is only possible to be load at the factory. Our production will start after certification has been granted.
Q.	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.
A.	The device is not allowed to use different types of antenna.

Shenzhen Chuangwei Electronic Appliance Tech Co., Ltd.

Martin Wu

Martin Wu/Manager