AIRTAME
December 10th, 2018

SOFTWARE SECURITY REQUIREMENTS FOR U-NII DEVICES
(594280 D02 U-NII Device Security 1.3, 11/12/15)

Company Name: Airtame ApS
FCC ID: 2ADEFAT-DG2
Product Model: AT-DG2

SOFTWARE SECURITY DESCRIPTION	
General Description	
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 Software can only be upgraded to versions provided by Airtame through the official update mechanism. An emergency update for the software is also possible through USB. The Software running on Airtame provides the firmware for our Cypress WiFi chip. This binary firmware is provided by Cypress at request, so it cannot be modified without official request to Cypress' team. This firmware includes vital WiFi configurations, such as available channels, TX power levels and so on.
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 set in the binary firmware that's used by the Cypress WiFi chip. This firmware is generated by Cypress for Airtame, based on the measured parameters during certification, to be within the regulations. There is no way to update this firmware without going through an official request with Cypress for a modification.
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.	As per request to Cypress, Airtame receives a binary firmware used for the Cypress wifi chip. This firmware contains the restrictions for allowed channel use, tx power and so on. The way this firmware is created is only known by Cypress, thus neither Airtame nor any other third party can go and change the configurations within. The Cypress WiFi chip firmware is the bundled into the Airtame update, and shipped through our official firmware update mechanism to the devices. The firmware on the device is read-only, and does not support any modification of these configurations without a firmware update. The device receives updates through HTTP(S).
Q.	*4. Describe in detail any encryption methods used to support the use of legitimate RF-related software/firmware.*
A.	The user does not have any access to the legitimate RF-related software/firmware.
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.	As mentioned before, the parameters that describe the RF behaviour of the WiFi chip are hardcoded in an official firmware provided by Cypress to Airtame. These parameters can't be changed by the product configuration. In the case of Airtame acting as both an AP (master) and a STA (client) on the same band, it will align it's AP behaviour to the STA, meaning that it will inherit settings used for the client (channel, power strength, etc), all based on the regulatory domain. Regardless of which bands and which modes Airtame operates in, it will respect the RF parameters set up in the WiFi chip's firmware.

Third-Party Access Control	
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.	Given that the regulatory domain is set at the factory, and the device doesn't have localization capabilities. it is a possibility that a third party could take a US device to another regulatory domain and use it there. Airtame has no method of preventing this, and this is at the third party's own risk.
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.	The Airtame device does not allow third party modifications to the software or the firmware of the device.
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.	All vital RF parameters are contained within the binary blob firmware provided by Cypress. Any modification to the binary firmware needs to go through Cypress as an official request for change. This request needs to be originating from Airtame's personnel. No user modifications of these settings are possible.

SOFTWARE CONFIGURATION DESCRIPTION	
USER CONFIGURATION GUIDE	
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.	*a. What parameters are viewable and configurable by different parties?*
	SSID, Channel (within permitted regulatory domain), Encryption method
	b. What parameters are accessible or modifiable by the professional installer or system integrators?
	SSID, Channel (within permitted regulatory domain), Encryption method
	(1) Are the parameters in some way limited, so that the installers will not enter parameters that exceed those authorized?
	They are limited by the Cypress wifi firmware. There are no configuration options exposed that would allow the device to be outside the permitted limits.
	(2) What controls exist that the user cannot operate the device outside its authorization in the U.S.?
	There are no configurations exposed to the system integrator that would allow the device to operate outside its authorization.
	c. What parameters are accessible or modifiable by the end-user?
	SSID, Channel (within permitted regulatory domain), Encryption method
	(1) Are the parameters in some way limited, so that the user or installers will not enter parameters that exceed those authorized?
	They are limited by the Cypress wifi firmware. There are no configuration options exposed that would allow the device to be outside the permitted limits.
	(2) What controls exist so that the user cannot operate the device outside its authorization in the U.S.?
	There are no configurations exposed to the user that would allow the device to operate outside its authorization.

	d. Is the country code factory set? Can it be changed in the UI?
	Yes, it's factory set. Can't 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.?
	It can't be changed in the UI. So it doesn't apply.
	e. What are the default parameters when the device is restarted?
	When restarted, it will set the previous settings. When factory resetting, it will default back to original settings as it was from the factory.
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.	The radio cannot be operated in bridge or mesh mode.
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.	The user can configure the operational mode of the device (master and client, master or client, just master or just client), however they cannot change any of the RF parameters. These RF parameters are hardcoded in the binary firmware provided by Cypress. This firmware makes sure that regardless of operational modes, the WiFi chip is compliant.
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. (See Section 15.407(a))*
A.	The device can only be used in one access point mode.

	The device has two antennas, one 5Ghz only, and another with a dual band 2.4+5Ghz. The usage of these antennas are controlled by the Cypress WiFi chip. The limits were measured for both antennas and are hardcoded in the Cypress provided WiFi firmware.

Name: Attila Sükösd
Title: CTO
Company: Airtame Aps
Address: Kuglegårdsvej 1, 1434 Copenhagen, Denmark

Signature