Software Security Declaration

FCC ID :2AAWQ-CAPRICA2XL

SOFTWARE SECURITY 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.	Phorus provides software updates via a secure storefront. A comprehensive security systemties software directly to a particular hardware device via an encrypted digital certificate.
	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?	All the radio frequency parameters are Transmit power, operating channel, modulation type. Only authorized parameters are available and can be set in software which are only calibrated at time of manufacture.
	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 update files are digitally signed at the time of creation. The certificates are checked against unique codes that are programmed into hardware at time of manufacture. Software that has not been authenticated with the proper digital certificates cannot be loaded or executed on the hardware.
	4. Describe in detail any encryption methods used to support the use of legitimate RF-related software/firmware.	Related source code is not shared with customers, therefore only Phorus can modify it and release official firmware.
	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	The device has been tested in client modes. The software has been validated and is controlled via our release process ensuring correct functionality.

	each band of operation?	

SOFTWARE SECURITY DESCRIPTION		
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.	There is no capability to change any parameter that would make the device violate the certification. No interface for third parties to set parameters.
	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. *Note : See*, for example, www.XXXXX.com/	There are not non-US versions of the software for third parties and in any case all software loads are securely controlled as indicated above.
	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.	Module is controlled through driver loaded in the host, which is packed into the released software to manufacture properly with device, and there is no way to modify transmitter parameters from software outside the grant of authorization.

	Note that Certified Transmitter Modules must have sufficient level of security to ensure that when integrated into a permissible host the device's RF parameters are not modified outside those approved in the grant of authorization. (See, KDB Publication 99639). This requirement includes any driver software related to RF output that may be installed in the host, as well as, any third-party software that may be permitted to control the module. A full description of the process for managing this should be included in the filing.	

SOFTWARE SECURITY 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 end user can only select a band.
	a. What parameters are viewable and configurable by different parties? *Note: The specific parameters of interest for this purpose are those that may impact the compliance of the device (which would be those parameters determining the RF output of the device). These typically include frequency of operation, power settings, antenna types, DFS settings, receiver thresholds, or country code settings which indirectly programs the operational parameters.*	The end user can only select a band.
	b. What parameters are accessible or modifiable by the professional installer or system integrators?	The end user can only select a band.
	(1) Are the parameters in some way limited, so that the installers will not enter parameters that exceed those authorized?	No parameters are available for adjustment.
	(2) What controls exist that the user cannot operate the device outside its authorization in the U.S.?	No Ul is available for this access.
	c. What parameters are accessible or modifiable by the end-user?	Band selection.
	(1) What parameters are accessible or modifiable by the end-user?	Band selection.
	(2) What controls exist so that the user cannot operate the device outside its authorization in the U.S.?	No Ul is available for this access.
	d. Is the country code factory set? Can it be changed in the UI?	Yes, country code is set by factory via a region code setting which cannot 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.?	
	e. What are the default parameters when the device is restarted?	The device goes to a default (approved) Tx channel and power level based on factory setting which is set as authorization in the U.S.

SOFTWARE SECURITY DESCRIPTION		
USER CONFIGURATION GUIDE	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 applicable for a client module level device.
	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?	This device is just a client, the user cannot arbitrarily change themselves.
	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 applicable for a client module level device.