Software Security Declaration

Model: AP 511X (AP 5115, AP 5116, AP 5117, AP 5118)

This device is fully compliant with the requirement of KDB 594280 D02 U-NII Device Security v01.

SOFTWARE SECURITY DESCRIPTION		
General Description	1. Describe how any software/firmware update will be obtained, downloaded, and installed.	*Ericsson introduces new SW through an EC process after a complete SW validation process. Ericsson uses proprietary radio that can only runs Ericsson SW. This is available through secure Ericsson technical support.*
	2. Describe all the radio frequency parameters that are modified by any software/firmware without any hardware changes. Are these parameters in some way limited, such that, it will not exceed the authorized parameters?	*All the radio frequency parameters are Transmit power, operating channel, modulation type.* *Only authorized parameters are available and can be set in software.*
	3. Are there any authentication protocols in place to ensure that the source of the software/firmware is legitimate? If so, describe in details; if not, explain how the software is secured from modification.	*The Ericsson SW runs a load validation during the SW upgrade process to ensure that the SW is legitimate, unaltered, and downloaded correctly.* *The SW, radios, and load validation are proprietary.*
	4. Are there any verification protocols in place to ensure that the software/firmware is legitimate? If so, describe in details.	*Software image contains 'MD5' signature and contains platform type imbedded in header.*
	5. Describe, if any, encryption methods used.	*Software images are not encrypted but are compressed.*
	6. 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 is only a master.*
Third Party Access Control	1. How are unauthorized software/firmware changes prevented?	*The SW and radios are Ericsson proprietary. The SW is updated through an Ericsson controller (a closed system).*
	2. Is it possible for third parties to load device drivers that could modify the RF parameters, country of operation or other parameters which impact device	*No, the APs are password protected. The device drivers that set channels and country are embedded into the SW load build and not accessible to any user.*

	compliance? If so, describe procedures to ensure that only approved drivers are loaded.	*It is a proprietary system. The memory maps, SW algorithms are not published.*
	3. Explain if any third parties have the capability to operate a US sold device on any other regulatory domain, frequencies, or in any manner that is in violation of the certification	*The access points sold to the US cannot be operated on any other country or domains. This is locked into the manufacturing data and cannot be changed.*
	4. What prevents third parties from loading non-US versions of the software/firmware on the device?	*The devices are HW configured to only accept US SW loads only at the time of manufacture, and not changeable.*
	5. For modular devices, describe how authentication is achieved when used with different hosts.	*This is not a modular device.*
SOFTWARE CONFIGURATION DESCRIPTION		
User Configuration Guide	1. To whom is the UI accessible? (Professional installer, end user, other.)	*The UI is accessible to the professional installer.*
	a) What parameters are viewable to the professional installer/end-user?	*The professional installer can change the RF channel and Tx power levels.*
	b) What parameters are accessible or modifiable to the professional installer?	*The RF channel can only be set to FCC approved channels. The TX power level can be set up to the approved RF power levels (or less).*
	i) Are the parameters in some way limited, so that the installers will not enter parameters that exceed those authorized?	*Yes, all radio parameters are limited by SW settings pre-determine by the FCC radio regulatory approval process. These parameters are in a drop-down list in the GUI and cannot go outside of these approved values.*
	ii) What controls exist that the user cannot operate the device outside its authorization in the U.S.?	*The radios are configured at manufacturing to be US only and only Ericsson US SW loads can be installed. These loads control the limits of the operation of the radio.*
	c) What configuration options are available to the end-user?	*Not available to the end user.*
	i) Are the parameters in some way limited, so that the installers will not enter parameters that exceed those authorized?	*Yes, all radio parameters are limited by SW settings pre-determine by the FCC radio regulatory approval process. These parameters are in a drop-down list in the GUI and cannot go outside of these approved values.*
	ii) What controls exist that the user cannot operate the device outside its authorization in the U.S.?	*The radios are configured at manufacturing to be US only and only Ericsson US SW loads can be installed. These loads control the limits of the operation of the radio.*
	d) Is the country code factory set? Can it	*Yes the country code is factory set. It*

	be changed in the UI?	*cannot be changed in the UI.*
	i) If so, what controls exist to ensure that the device can only operate within its authorization in the U.S.?	*The radios are configured at manufacturing to be US only and only Ericsson US SW loads can be installed.*
	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 country setting.*
	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.	*This approval is for UNII-3 band and this KDB applies only to UNII-2A and UNII-2C.*
	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 to ensure compliance.	*The AP is a Master only.*