Software Security Description – KDB 594280 D02v01r03 Section II		
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.	Ericsson introduces new SW after a complete SW verification and validation process. The SW is delivered through an Ericsson SW delivery system integrated into the Ericsson operations, administration and management system controller. Ericsson uses proprietary radio that can only runs Ericsson SW. This is available through secure Ericsson technical support.
	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 parameter are transmit power, operating channel, carrier bandwidth, modulation type, frequency band edge. Some parameters are fixed after factory calibration, such as transmit power, frequency band edge. Only authorized parameters are available and can be set in software. These authorized parameters do not make device exceed the authorized RF characteristics.
	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 Ericsson SW runs a load validation during the SW upgrade process to ensure that the SW is legitimate, unaltered, and downloaded correctly. The software image contains a proprietary digital signature. The SW, radios, and load validation are proprietary. SW images and loads are only available through the Ericsson operations, administration and management system controller. If device be out of factory, transmit power, frequency band edge can not be modified any more.
	4. Describe in detail any encryption methods used to support the use of legitimate RF-related software/firmware.	Software images are compressed but not encrypted.

	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 is a master only.
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.	The hardware is intended for the worldwide market. The professional installer shall configure the device for use in the country of operation using the Mobile Country Code(MCC). The MCC then ensures that the device cannot be configured in any manner which would violate the authorization of the country in which it is operated. The device will not come into normal operation if the MCC is incorrectly entered.
	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 device does not permit third party SW or firmware installation. The SW, firmware and radios are Ericsson proprietary. The Ericsson SW runs a load validation procedure during the SW upgrade process to ensure that the SW is legitimate, unaltered, and downloaded correctly. The software image contains a proprietary digital signature and any SW image will be rejected if the digital signature is not correct. SW images and loads are only available through the Ericsson operations, administration and management system controller.
	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	This device is certified as Limited Single-Modular Transmitter. Ericsson Approved PSU and antennas with Radio 2205 are required for use in all installations with the listed

	the drivers are controlled and managed such that the modular transmitter RF parameters are not modified outside the grant of authorization.	module. No SW control between those modules.

In addition to the general security consideration, for devices which have "User Interfaces" (UI) to configure the device in a manner that may impact the operational RF parameters, the following questions shall be answered by the applicant and the information included in the operational description. The description must address if the device supports any of the country code configurations or peer-peer mode communications discussed in KDB 594280 Publication D01.[8]

Software Configuration Description – KDB 594280 D02v01r03 Section III **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 only accessible to the professional installer. Access to the device is password protected.
a. What parameters are viewable and configurable by different parties? The professional installer can change the RF channel and adjust Tx power level to a lower level.
b. What parameters are accessible or modifiable by the professional installer or system integrators? (1) Are the parameters in some way limited, so that the installers will not enter parameters that exceed those authorized? 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). The MCC determines the authorized valid range of values that the professional installer can configure.
(2) What controls exist that the user cannot operate the device outside its authorization in the U.S.? 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.
c. What parameters are accessible or modifiable by the end-user? (1) Are the parameters in some way limited, so that the installers will not enter parameters t exceed those authorized? The MCC determines the authorized valid range of values that the operator can configure
(2) What controls exist that the user cannot operate the device outside its authorization in the U.S.? 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.

d. Is the country code factory set? Can it 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.?

The country code can only be set by the operator professional installer.

e. What are the default parameters when the device is restarted?

The device cannot become operational until the professional installer configures the country code (MCC). 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.

No.

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?

The device is a master only.

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))

The device is a point-to-multi-point device.
External antennas may only be installed by professional installers.