Model 3e-523E-900
3e Technologies international, Inc.

1. **Describe how any software/firmware update will be obtained, downloaded, and installed. Software that is accessed through manufacturer's website or device's management system, must describe the different levels of security.**

   Obtaining and downloading firmware updates for the model 3e-523E-900 is a manual process. Customers can obtain firmware updates only by request to or on the advice of 3eTI's Technical Support Department. Firmware update files are then made available for user download on password protected, temporary ftp site.

   Firmware installation: there are two management account levels on the 3e-523E-900 device: CryptoOfficer and Administrator. Of these two, only the CryptoOfficer account has rights to perform firmware updates.

   Firmware installation is done trough the Graphical User Interface (GUI) on the device. Once authenticated, the user navigates to the System Upgrade menu option, on this page the operator selects the update file on local PC and loads it to the device. The device will verify the newly loaded firmware, upon successful update, the device will reboot.

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?**

   There are no configuration options available to the user to modify the frequency parameters; these are locked in by firmware. Installers/operators can only change transmitter's operation (On/Off), and signal power level.

3. **Describe in detail the authentication protocols that are in place to ensure that the source of the software/firmware is legitimate. Describe in detail how the software is protected against modification.**

   As described in item #1, the firmware is not available for automatic download over a network. 3eTI has a manual process in place for obtaining and downloading firmware which guarantees that the customer receives legitimate firmware updates. The firmware is signed with ECDSA private key, and digest hash safeguards firmware from modifications.

4. **Describe in detail the verification protocols in place to ensure that installed software/firmware is legitimate.**

   Firmware legitimacy is verified by the device with ECDSA public key.

5. **Describe in detail any encryption methods used to support the use of legitimate software/firmware.**
   No encryption on software/firmware

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 3e-523E-900 can be configured either as a master or as a client. In both modes, the device radio is locked by firmware to operate only in the permitted frequency band, and no option is available to Installer/operator to change this configuration.

Third Party Access Control

1. **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.**

   Third parties cannot change the device's regulatory domain configuration (locked in at factory), frequencies or any other parameter that are in violation of the certification.

2. **What prevents third parties from loading non-US versions of the software/firmware on the device? Describe in detail how the device is protected from "flashing" and the installation of third-party firmware such as DD-WRT.6**

   Third parties cannot obtain non US versions of the firmware; all firmware upgrade distribution must be authorized by 3eTI's Technical Support department. The devices' proprietary bootloader does not allow flashing of third party firmware.

3. **For Certified Transmitter modular devices, describe how the module grantee ensures that hosts manufactures 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 parameters are not modified outside the grant of authorization.7**

   The radio card used in this system was approved previous to this requirement. However, the card itself is just a hardware device under the command of the 3e-523-3 software developed by 3eTI. As explained in previous numerals, the software offers no configuration option for the user to modify operation of the device outside of its authorization.

SOFTWARE CONFIGURATION DESCRIPTION

1. **To whom is the UI accessible? (Professional installer, end user, other.)**
   The UI is accessible to professional installers or operators with the right log in credentials. .

   a) **What parameters are viewable to the professional installer/end-user?9**
   If installer/end user has login credentials viewable radio parameters are: SSID, transmitter operation status and power level.

   b) **What parameters are accessible or modifiable by the professional installer?**
   If installer has login credentials it can change parameters such as: SSID, transmitter operation (on/off), and power level.

(1) **Are the parameters in some way limited, so that the installers will not enter parameters that exceed those authorized?**

The parameters are limited, transmitter options are: on/off, power level options: 4 to 8

(2) **What controls exist that the user cannot operate the device outside its authorization in the U.S.?**
The firmware in the 3e-523E-900 is locked in at factory to operate within its authorization in the U.S., there are no configuration options in the device for the user to change device's parameters outside authorization.

c) **What parameters are accessible or modifiable to by the end-user?**
End user, in the case of the 3e-523-900E, is typically a network administrator/network security officer; the device therefore will have limited access. An end user, as understood here, can have one of two privilege levels; CryptoOfficer or Administrator. The Crypto Officer can view and change most settings permitted by firmware. The Admistrator role has reduced privileges – among others, it cannot perform firmware upgrades.

(1) **Are the parameters in some way limited, so that the installers will not enter parameters that exceed those authorized?**
The parameters are limited, for example transmitter options are: on/off, power level options: 4 to 8

(2) **What controls exist that the user cannot operate the device outside its authorization in the U.S.?**
The firmware in the 3e-523E-900 is locked in at factory to operate within its authorization in the U.S; there are no configuration options in the device for the user to operate the device outside its authorization.

d) **Is the country code factory set? Can it be changed in the UI?**
The country code is factory set; the user has no configuration option to change it trough UI.

(1) **If so, what controls exist to ensure that the device can only operate within its authorization in the U.S.?**
Device is locked in by firmware to operate within its authorization in the U.S., user has no option to change it.

e) **What are the default parameters when the device is restarted?**
Radio Region: United States
Mode: AP and Bridge.
Frequency: 20MHz channel centered at 2.452GHz and translated to 916 MHz for transmission.
Transmitter power: OFF

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.**

Device is not capable of transmitting in the UNII Bands.
The radio can be configured as bridge; however, the radio is limited to operate only in the 2.4GHz band which is then fed internally to a frequency converter which converts the 2.4GHz frequency to a frequency in the 900MHz band and transmitted into the air.

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?**

   Device is not capable of transmitting in the UNII Bands.

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 FCC test report does not limit the device to use a particular antenna for a particular application. To insure compliance, the 3e-523E-900 User Guide states that this product is required to be installed by a professional installer.