The description of the software must address the following questions in the operational description for the device and clearly demonstrate how the device meets the security requirements.

Software Security Description

1. Describe how any software/firmware update will be obtained, downloaded and installed Description: There are two ways (network and USB disk) to update firmware a. USB disk firmware is read from a USB disk b. Network firmware is downloaded from operator's upgrade server If new firmware is available, it will be downloaded, verified and programmed into NAND flash chip.
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? Description: No any parameters could be modified by software/firmware without hardware changes.
3. Are there any authentication protocols in place to ensure that the source of the software/firmware is legitimate? If so, describe in detail; if not, explain how the software is secured from modification Description: There is no authentication, however: 1. Firmware consists of several blocks (kernel, rootfs, branding) merged into one file, and each block is signed with service provider's key. Key certificate is stored in a R/O section and is used to verify downloaded firmware. 2. If signature verification fails, firmware update will not be performed.
4. Are there any verification protocols in place to ensure that the software/firmware is legitimate? If so, describe in detail Description: Firmware blocks are signed with operator's key and key certificate is stored in the STB R/O memory. Signature is verified before firmware upgrade.
5. Describe, if any, encryption methods used Description: No.
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 Description: The device can work as master (WiFi Access Point) and client (device which connects to WiFi AP), but only one mode can be enabled at a time.
7. How are unauthorized software/firmware changes prevented? Description: 1. Firmware consists of several blocks (kernel, rootfs, branding) and each block is signed with service provider's key. Key certificate is stored in a R/O section and is used to verify downloaded firmware 2. If signature verification fails, firmware update will not be performed
8. 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 compliance? If so, describe procedures to ensure that only approved drivers are loaded. Description: It is not possible
9. 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.

Description:
It is not possible

10. What prevents third parties from loading non-US versions of the software/firmware on the device?
Description:
Software is released and signed by an operator (IPTV service provider). Only the firmware signed with this operator's private key can be loaded on the device. All other third-party versions of firmware need to be signed with operator's private key in order to be accepted by firmware update tool running on STB.

11. For modular devices, describe how authentication is achieved when used with different hosts.
Description:
This is a standalone device which does not need a host. It is solid and there are no replaceable 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 parameter, the following questions shall be answered by the applicant and the information included in the operational description.

USER CONFIGURATION GUIDE

1. To whom is the UI accessible? (Professional installer, end user, other.)
a) What parameters are viewable to the professional installer/end-user?
Description:
There are 2 different versions of firmware:
1. Factory firmware which is also shipped to the end-user.
All users of the factory firmware can disable/enable RF part of WiFi module. Factory firmware does not support different types of users.
2. Engineering firmware for FCC certification. This firmware is used only for certification and never shipped to customers. It allows to change many parameters: WiFi adapter mode (production or calibration, which is used for FCC tests), Tx power, RF channel, bandwidth, MCS Index, RF band (802.11a/n/ac), Tx packets size and count. All parameters have predefined list of possible values stored in ROM
b) What parameters are accessible or modifiable to the professional installer?
Description:
Factory firmware allows to disable/enable RF part of WiFi module from the GUI.
i) Are the parameters in some way limited, so that the installers will not enter parameters that exceed those authorized?
Description:
All parameters have a limited range of valid values. They are hard-coded in the firmware and any other value is not available from the UI.
ii) What controls exist that the user cannot operate the device outside its authorization in the U.S.?
Description:
Region settings are hard-coded and there is no way to change them from the GUI.
c) What configuration options are available to the end-user?
Description:
Disable/enable RF part of WiFi module
i) Are the parameters in some way limited, so that the installers will not enter parameters that exceed those authorized?
Description:
All parameters have a limited range of valid values. They are hard-coded in the firmware and any other value is not available from the UI.
ii) What controls exist that the user cannot operate the device outside its authorization in the U.S.?
Description:

Region settings are hard-coded and there is no way to change them from the GUI. d) Is the country code factory set? Can it be changed in the UI? Description: Region settings are hard-coded and there is no way to change them from the GUI. i) If so, what controls exist to ensure that the device can only operate within its authorization in the U.S.? Description: N/A e) What are the default parameters when the device is restarted? Description: For engineering firmware default parameters are the one that allowed to pass EMC test during development phase. That is, when STB is turned on it can be taken to the EMC laboratory and should pass EMI tests. In factory firmware, all settings are saved to NVRAM and read back after power off/on.
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. Description: 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? Description: The device can work as master (WiFi Access Point) and client (device which connects to WiFi AP), but only one mode can be enabled at a time.
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)) Description: Only point-to-multipoint mode is available. This is a most common case when WiFi client connects to WiFi access point by its SSID and password.

How the product complies 15.407(c)
Description: WIFI chip support automatically discontinue transmission in case of either absence of information to transmit or operational failure, if the chip detects absence of information to transmit or operational failure, it will be automatically shut off.