



Date: 2016-09-29

FCC ID: **VW3FAST3486**

Software Operational Description

We, **SAGEMCOM BROADBAND SAS** hereby declare that requirements of KDB594280 have been met and shown on the following question. Further we declare that the info listed below are correct and represent the product in consideration under this filing.

Useful acronyms:

MSO : Multi-System Operator

CM : Cable Modem

BSP : Base System Package

1. Describe how any software/firmware updates for elements that 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.

Description:

The software/firmware is signed binaries that will be loaded by multi-system operator (MSO) via cable modem (CM) configuration file only.

There's no WEB GUI page available to download and install new software/firmware versions. All interfaces as GUI, serial console, SSH, telnet and SNMP are closed to the end-user by default. After new signed software/firmware is silently downloaded in background through the CM interface, it is copied in flash memory without any end-user action.

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?

Description:

The Wi-Fi default parameters are set from the base system package (BSP) / Wi-Fi driver, adapted in order to comply with FCC regulation. They are written into the non-volatile memory section of the device.

Those parameters set in non-volatile memory are restricted to the authorized ones and they comply with FCC rules.

By default those parameters are not accessible by any user interface (UI) for reading or modification.

Only MSO can activate access to a UI for the end-user. In that case, only 2 parameters can be set: channel and bandwidth. The UI for end-user always limits modifications of parameters so that channels can only be set to US channels and bandwidth in all operational modes.

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.

Description:

The product is compliant with DOCSIS Baseline Privacy Plus Interface specification concerning the protection and verification of the software/firmware download.

The manufacturer (Sagemcom) of the CM software/firmware always applies a digital signature to the code file; a signature that is verified with a certificate chain that extends up to the DOCSIS root. The manufacturer's signature authenticates the source and integrity of the code file to the CM. Additional control parameters are included in the code file to control access to the CM.

Though the manufacturer always signs their code file, an MSO may later apply their code signature in addition to the manufacturer's signature. The CM must verify both signatures with a certificate chain that extends up to the DOCSIS root before accepting a code file.

4. Describe in detail any encryption methods used to support the use of legitimate RF-related software/firmware.

Description:

The image is not encrypted only signed (RSA protected).

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?

Description:

Not relevant, the device is only master.

6. 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.

Description:

Only the MSO can change the parameter via CM configuration file. This configuration file is not visible to the end-user and it is downloaded through the CM interface.

The only UI that can be available is a WEB GUI.

If WEB GUI pages are available, which is not the case by default and it can only be activated by MSO.

The WEB UI for end-user only contains authorized parameters

7. 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.

Description:

Not relevant. Only the MSO can change the parameter via CM configuration file.

8. 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.

Description:

Not relevant, the device does not have modular device.

9. 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.

- a) What parameters are viewable and configurable by different parties?

Description:

The UI always limits the modifications of parameters: only SSID, channel, bandwidth can be viewable and configurable. And the channels can only be set to US channels and bandwidth in all operational modes.

- b) What parameters are accessible or modifiable by the professional installer or system integrators?

Description:

The UI always limits the modifications of parameters: only SSID, channel, bandwidth can be viewable and configurable. And the channels can only be set to US channels and bandwidth in all operational modes.

- i) Are the parameters in some way limited, so that the installers will not enter parameters that exceed those authorized?

Description:

Only SSID, channel, bandwidth can be viewable and configurable. And the channels can only be set to

US channels and bandwidth in all operational modes.

- ii) What controls exist that the user cannot operate the device outside its authorization in the U.S.?

Description:

The UI is not activated by default. It can only be activated by MSO. In that case installer access UI there is no proposed parameters to configure the device outside its authorization in the US.

- c) What parameters are accessible or modifiable by the end-user?

Description:

The UI is not activated by default. It can only be activated by MSO. It is not meant for end-user.

- i) Are the parameters in some way limited, so that the user or installers will not enter parameters that exceed those authorized?

Description:

The UI is not activated by default. It can only be activated by MSO. In that case installer access UI, he can only modify the SSID, channel and channel bandwidth only. Those parameters are restricted through list box selection to US channels and bandwidth in all operational modes.

- ii) What controls exist so that the user cannot operate the device outside its authorization in the U.S.?

Description:

The UI is not activated by default. It can only be activated by MSO. In that case installer access UI, there is no proposed parameters to configure the device outside its authorization in the US.

- d) Is the country code factory set? Can it be changed in the UI?

Description:

The country code is factory set and can-not be changed in the UI.

- i) If it can be changed, what controls exist to ensure that the device can only operate within its authorization in the U.S.?

Description:

NA. All parameters (RF, Frequencies and etc.) indicating different countries are permanent settings in ROM. So if a device is a product for US, it cannot be changed for another region.

- e) What are the default parameters when the device is restarted?

Description:

Default parameters at boot are the one configured for the device. If reset to default, parameters are the one from factory defaults.

10. 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 support for bridge or mesh mode, there is no option in the UI to do so.

11. 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:

Not relevant, the device is only master.

12. 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:

WDS is not enabled.

If you should have any question(s) regarding this declaration, please don't hesitate to contact us.
Thank you!

Name: Jacques LE ROUX

Title: R&D General Methods Department

Tel: + 33 1 57 61 25 72

Fax: + 33 1 57 61 38 99

E-mail: jacques.leroux@sagemcom.fr

