

Declaration of Software Security

Federal Communication Commission

Equipment Authorization Division, Application Processing Branch
7435 Oakland Mills Road
Columbia, MD 21048

Innovation, Science and Economic Development Canada

Spectrum Engineering Branch
3701 Carling Avenue, Building 94
Ottawa, Ontario K2H 8S2

SOFTWARE SECURITY REQUIREMENTS FOR U-NII DEVICES acc. to KDB 594280

We, Mitsubishi Electric Corporation, declare on our sole responsibility that the requirements of KDB 594280 for the device:

Model: R1LOW-R	with FCC ID:	UHJ-R1LOW-R
HVIN: R1LOW-R	and IC ID:	662K-R1LOWR

are followed as described below:

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:

*Software update package has authenticated signature and encrypted when it is shipped.
Device checks if the software update package is not modified after shipment by signature verification.
Device installs update package only when verification success.*

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:

*Frequency setting (with or without 5GHz), WLAN mode, output Power, ANT configuration (SISO/MIMO) and RF related parameters can be set in the hardware configuration file. Additionally, the regulatory database for each country and DFS sensitivity parameter are coded in WLAN host driver statically. Both the hardware configuration file and the host driver are hard-coded and it can be updated by software/firmware update.
But software/firmware update package has authenticated signature and encrypted and it is secure.*

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:

*Device verifies software before execution.
Only when device confirm the software is not modified after install, software can be executed.*

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

Description:

It is not encrypted but cannot be accessed by third parties or users. Furthermore, the software is validated before start up. If it is falsified, it cannot be booted up.

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:

WLAN mode is used singly and it has no effect as it is used singly. The RF of master mode and client mode are switched by time division in the chip internally and don't affect each other. This is the same behavior regardless of band.

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:

The 3rd Party doesn't have any capability to configure the setting of frequency and/or regulatory domain.

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:

The installation of third-party software is not permitted. It is accomplished by digitalized signature using certificate, and verify boot and SELinux.

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:

The regulatory information is hard-coded into the host driver, and WLAN can work only in the frequency band allowed by the country code. This database cannot be changed arbitrarily by the user.

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:

There is no viewable and configurable parameter by different parties.

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

Description:

Country code which decide frequency.

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

Description:

The country code can be changed only by vehicle configuration, and it can be modified by a specific tool.

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

Description:

The RF-related software/firmware is under the access control by verify boot, and it cannot be changed by user.

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

Description:

There is no parameter accessible or modifiable by the 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:

N/A

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

Description:

N/A

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

Description:

YES the country code is set in the factory. And it cannot 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:

N/A

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

Description:

The default parameters are depends on the country code parameter which is stored in the device, and to change country code parameter, authenticated tool only.

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. Bridge mode and mesh mode cannot be configured.

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:

The parameter that can be configured by user is enabling or disabling master mode.


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:

The software complies with Wi-Fi Alliance specifications, and the compliance to MIMO or SISO operation is guaranteed by Wi-Fi Alliance certification. The antenna settings are shared during the connection process, and set to properly.

Please do not hesitate to contact us for further explanations or comments.

Sincerely,

DocuSigned by:

4D06A291D81B402...

Signature

March 7, 2022

Date

Printed Name of Signee: Ryuji Yoshinaga
Title: Senior Manager, Design-A Section
Car Multimedia Design Dept.
Company: Mitsubishi Electric Corporation
Address: 2-3-33, Miwa, Sanda-city, Hyogo 669-1513 Japan
Phone: +81-79-559-4813
Fax: N/A
Email: Yoshinaga.Ryuji@db.MitsubishiElectric.co.jp