Federal Communications Commission
Office of Engineering and Technology
Laboratory Division

April 30, 2014

Public Draft for Review

Laboratory Division Draft Publication Report

Title: Software Security and Configuration Control Requirements for Non-SDR Devices

Short Title: Software Security and Configuration Control

Reason: Adding attachment D02 to update KDB to address recently revised rules for U-NII devices.

Publication: 594280

Keyword/Subject: U-NII, DFS, 15 Subpart E, Software Configuration, Security

---

Question: What are the software security requirements for non-SDR devices and what limitations apply to software configuration control for such devices?

Answer:

See attachment below 594280 D01 Configuration Control v01r02 for guidance on restrictions on configuration controls for devices not approved as Software Defined Radios.

The Commission recently revised (FCC 14-30 in ET Docket 13-39) the rules for U-NII devices, effective June 2 2014, operating under Part 15 rules to require such devices to implement software security to ensure that the devices operate as authorized and cannot be modified. The attached draft document provides guidance on the information that must be provided in the application filing to show that proper security is implemented in the device.

The Commission has established a transition period as follows:

- New devices or permissive changes on previously approved devices will be permitted under the previous rules for one year after the effective date (June 2 2015).
- Devices approved under the new rules after the effective date must apply all the appropriate test procedures for such devices and provide software security documentation discussed in this guidance. This applies to all new devices and application for permissive changes of previously approved devices.
- All devices approved under previous rules cannot be marketed after two years from the effective rules.
- After two years from the effective date, no permissive changes will be permitted under for devices approved under the previous rules unless they meet the requirements of the new rules.

A previous draft of document software configuration control (594280 Software Configuration Control DR04-41649) was previously published and while it has expired, it may be used for software configuration control.

This draft KDB for the attachment 594280 D02 U-NII Device Security v01 can be used after the effective date (June 2 2014) of the rules.

Attachment List:

594280 D01 Configuration Control v02

594280 D02 U-NII Device Security v01

Attachment: 594280 D02 U-NII Device Security v01

Federal Communications Commission
Office of Engineering and Technology
Laboratory Division

SOFTWARE SECURITY REQUIREMENTS FOR U-NII DEVICES

I. INTRODUCTION

On March 31, 2014, the Commission revised the rules in Part 15 that permits U-NII devices in the 5 GHz Band.[1] As part of that revision, the Commission required that all U-NII device software be secured to prevent its modification to ensure that the device operates as authorized thus reducing the potential for harmful interference to authorized users. Although, the Commission refused to set specific security protocols, the methods used by manufacturers to implement the security requirements must be well documented in the application for equipment authorization. In this document, we provide general guidance on the type of information that should be submitted in the equipment authorization application. The security description provided in the application must cover software security, configuration, and authentication protocols descriptions, as appropriate. This guidance applies to master and client devices. Special circumstances that apply only to client devices are also addressed.

II. SOFTWARE SECURITY DESCRIPTION GUIDE

An applicant must describe the overall security measures and systems that ensure that only:

1. Authenticated software is loaded and operating the device.
2. The device is not easily modified to operate with RF parameters outside of the authorization.

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. While the Commission did not adopt any specific standards, it is suggested that the manufacturers may consider applying existing industry standards.[2] Also, this guide is not intended to be exhaustive and may be modified in the future. There may be follow-up questions based on the responses provide by the applicant for authorization.

[1] See *Revision of Part 15 of the Commission's Rules to Permit Unlicensed National Information Infrastructure (U-NII) Devices in the 5 GHz Band, First Report and Order*, ET Docket No. 13-49 (2014) (1st R&O).

[2] It is suggested that manufacturers follow existing security standards and definitions: X.800, RFC 2828, and IEEE 802.11i.

General Description

- Describe how any software/firmware update will be obtained, downloaded, and installed.
- 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?
- Are there any authentication protocols in place to ensure that the source of the software/firmware is legitimate? If so, describe in details; if not, explain how the software is secured from modification.
- Are there any verification protocols in place to ensure that the software/firmware is legitimate? If so, describe in details.
- Describe, if any, encryption methods used?

Third-Party Access Control

- How is any unauthorized software/firmware change prevented?
- 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.
- 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.
- What prevents third parties from loading non-US versions of the software/firmware on the device?
- For modular devices, describe how authentication is achieved when used with different hosts.

III. SOFTWARE CONFIGURATION DESCRIPTION GUIDE

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. The description must address if the device supports any of the country code configurations or peer-peer mode communications discussed in KDB Publication 594280.[3]

- To whom is the UI accessible? Professional installer? End user?
    - What parameters are viewable to the professional installer/end-user?[4]
    - What parameters are accessible / modifiable to the professional installer?
        - Are the parameters in some way limited, so that the installers will not enter parameters that exceed those authorized?

[3] See KDB Publication 594280 D01 – Software Configuration Control for Devices. The document provides some guidance for devices permitting device configurations and limitations on configuration parameters accessible to the third parties.

[4] The specific parameters of interest for this purpose are those that may impact the compliance of the device. These typically include frequency of operation, power settings, antenna types, DFS settings, receiver thresholds, or country code settings which indirectly programs the operational parameters.

        - What controls exist that the user cannot operate the device outside its authorization in the U.S.?
    - What configuration options are available to the end-user?
        - Are the parameters in some way limited, so that the installers will not enter parameters that exceed those authorized?
        - What controls exist that the user cannot operate the device outside its authorization in the U.S.?
    - Is the country code factory set? Can it be changed in the UI?
        - If so, what controls exist to ensure that the device can only operate within its authorization in the U.S.?
    - What are the default parameters when the device is restarted?
- 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.
- For a device that can be configured as a master and client, please explain how does the device ensure 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? If this is user configurable, describe what controls exist to ensure compliance?