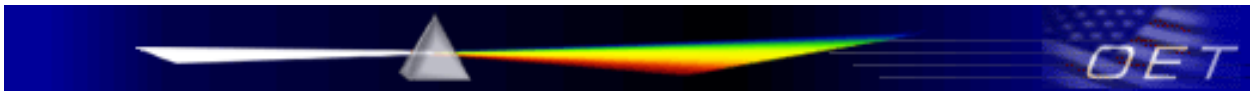

Federal Communications Commission
Office of Engineering and Technology
Laboratory Division

July 17, 2014

SOFTWARE DEFINED RADIO APPLICATION GUIDE

I. INTRODUCTION

This publication is a guide to help applicants provide the software operational and security description for a Software Defined Radio (SDR) for an initial certification or permissive change application. The guide also explains the procedure when submitting information needed in a Permit but Ask (PBA) procedure for approval by a Telecommunications Certification Body (TCB).

- Section I is an introduction to SDR
- Section II describes a template for providing the required operational and security description for equipment authorization application review.
- Section III describes the support information for permissive changes for SDRs.
- Section IV describes specific security requirements for U-NII devices
- Section V provides direction for submitting a PBA request.

The FCC rules[1] require that any radio, in which the software[2] is designed or expected to be modified by a party other than the manufacturer that would affect the operating parameters of frequency range, modulation type, maximum output power or other radio frequency parameters outside the range under which the transmitter has been approved in accordance with the Commission rules, must comply with the requirements in Section 2.944 (a) and must be certified as a software defined radio. In many other cases where such software is under complete control of a manufacturer, the rules allow the manufacturer to choose if they want to have the device approved as an SDR.[3] An SDR grant has the advantages of allowing a manufacturer to (1) market the same transmitter with the intrinsic capability of operating in other regulatory domains and/or (2) permit third parties including their customers, professional

[1] *See* Section 2.944.

[2] Software is code, configuration settings or machine instructions that form the elements that when put in place, affect, modify or change the features, performance that operates the transmitter with operating frequencies, output power, modulation types or other radio frequency parameters that are approved or modified as permitted under Section 2.1043 changes in certified equipment. This includes configuration capabilities, command language controls, operating systems, browser based controls, application code, firmware, code for fixed read only memories or field programmable gate arrays, etc.

[3] The Commission also has adopted rules for split-modular transmitters which permit the manufacturer to have certain control software reside outside the front-end RF transmitter (Section 15.212). In such cases the software must have certain authentication support to ensure security. The following guidance for software for SDRs may also be applied to split- modular transmitters.

installers to add software to modify its operating parameters (rule parts, additional frequency bands, new modulation types, change bandwidth).

Non-SDR(s) are fixed to only operate on approved frequencies, are limited to all applicable conditions of the certification and cannot be generally modified in the field outside the grant conditions. For non-SDR(s), third parties[4] (end users, professional installers,[5] and distributors) cannot have any ability to configure or operate transmitters on non-US frequencies, or in any way[6] that violates the approved certification. The Commission may allow grantees to permit specific parties, such as operating system providers, service providers or parties under direct control of the grantee to enable software upgrades for field deployed non-SDR devices. Such upgrades can be permitted with connection to the grantee or related parties' website. The details of such arrangements including the procedures to maintain control of the software uploads must be included in the original filing or Class II permissive change filings and is subject to Permit-but-ask procedures for TCB processing.[7]

Certain types of non-SDR Client devices[8] may be permitted to be enabled on other frequency bands outside of the grant condition, if the device only operates in these bands under control of a master device. In this way, compliance is ensured when operating in the US under control of a FCC granted master device

To obtain an SDR grant the responsible party must demonstrate and maintain an acceptable software security process that ensures full compliance to the FCC certification when marketed, sold, operated or updated in the U.S.

---

[4] Third parties include end users, professional installers, repair shops etc., essentially all parties except the grantee or any party legally contracted to the grantee when the grantee remains liable by the contracted relationship for any actions of the contracted party.

[5] Some specific rules permit professional installers limited additional configuration adjustments over what is permitted by end-users or license holders. In this case the specific configuration adjustments are within the granted conditions for this specific equipment such as power adjustment to compensate for cable feeder loss or antenna gain or limited frequencies, but within the granted frequencies, set by professional installers for licensed operators.

[6] Operating the device on any other regulatory frequency bands, modulation types, bandwidth, power, etc. that is not permitted by the rules, and/or not in compliance with the certification as granted.

[7] *See* KDB Publication 388624 for Permit-but-ask and KDB Publication 178919 regarding restrictions on permissive changes through software or any exceptions.

[8] A device is the embodiment of the host hardware and software to be certified that defines the operating conditions. The host hardware is the physical non programmable elements of a service targeted as a licensed or unlicensed certified device in the U.S., other legal applications or any other regulatory domain. Client devices defined in Section 15.202 that operate under control of a master device may be marketed with the ability to be enabled in other frequency bands not permitted in the grant. Some licensed Client devices (*i.e.*, Parts 22 and 24 Cell Phones) enabled by master devices (base stations) may also qualify as client devices. Note: some devices commonly sold or known as client devices for IEEE 802.11 Wi-Fi operate in Ad Hoc, peer-to peer or mesh network mode. These devices will initiate transmissions not under control of a master device and do not qualify as a Section 15.202 client device. Other IEEE 802.11 Wi-Fi client devices that actively scan only on U.S. frequencies and only operate in Ad Hoc mode on U.S. frequencies but passively scan on other than U.S. frequencies may qualify as a Section 15.202 client device. (*See* KDB 594280 for further discussion on software configuration control and master – client devices). In all cases, the client devices must always be fully compliant with all the applicable rules for operation in the authorized bands.

SDR rules under Section 2.944 require that SDR applicants:

- Take steps to ensure that only approved software operates the radio;
- Ensure that any radio where third parties can operate outside of the grant is an SDR;
- Provide an operational description with the application for certification.

The following five questions (illustrated in figure 1) can be used for determining if a radio can elect to be,[9] or must be an SDR:[10]

1. Can the RF parameters of the device be altered through software?

   Yes, go to question 2.
   No, not an SDR.

2. Can third parties not permitted by the Commission through specific filings modify, configure, or load different software, or make configuration settings to operate the device or host hardware radio frequency parameters (frequency range, modulation type, maximum output power or other radio parameters) in any other way than granted (or expected to be granted)?

   Yes, must be an SDR.
   No, go to question 3.

3. Is the device capable of operating in any other in any other way than granted, or will be, granted?

   Yes, go to question 4.
   No, go to question 5.

4. Is this a Part 15 client device as defined in Section 15.202 (as opposed to a master device)?

   Yes, qualifies as a Part 15 client device, go to question 5.
   No, must be an SDR.

5. Does the manufacturer elect SDR?

   Yes, elects to be an SDR.
   No, not an SDR.

[9] When the host hardware cannot operate in any way other then what is granted, an applicant may still elect to be an SDR to take advantage of Class III permissive changes

[10] If third parties can operate a device through software outside of the granted conditions then the device can only be approved as an SDR if the manufacturer demonstrates a software security process to ensure only approved software operates the radio when in the US and within the granted parameters. The only exception is for devices that qualify as a Part 15 client device (*see* footnote 8).

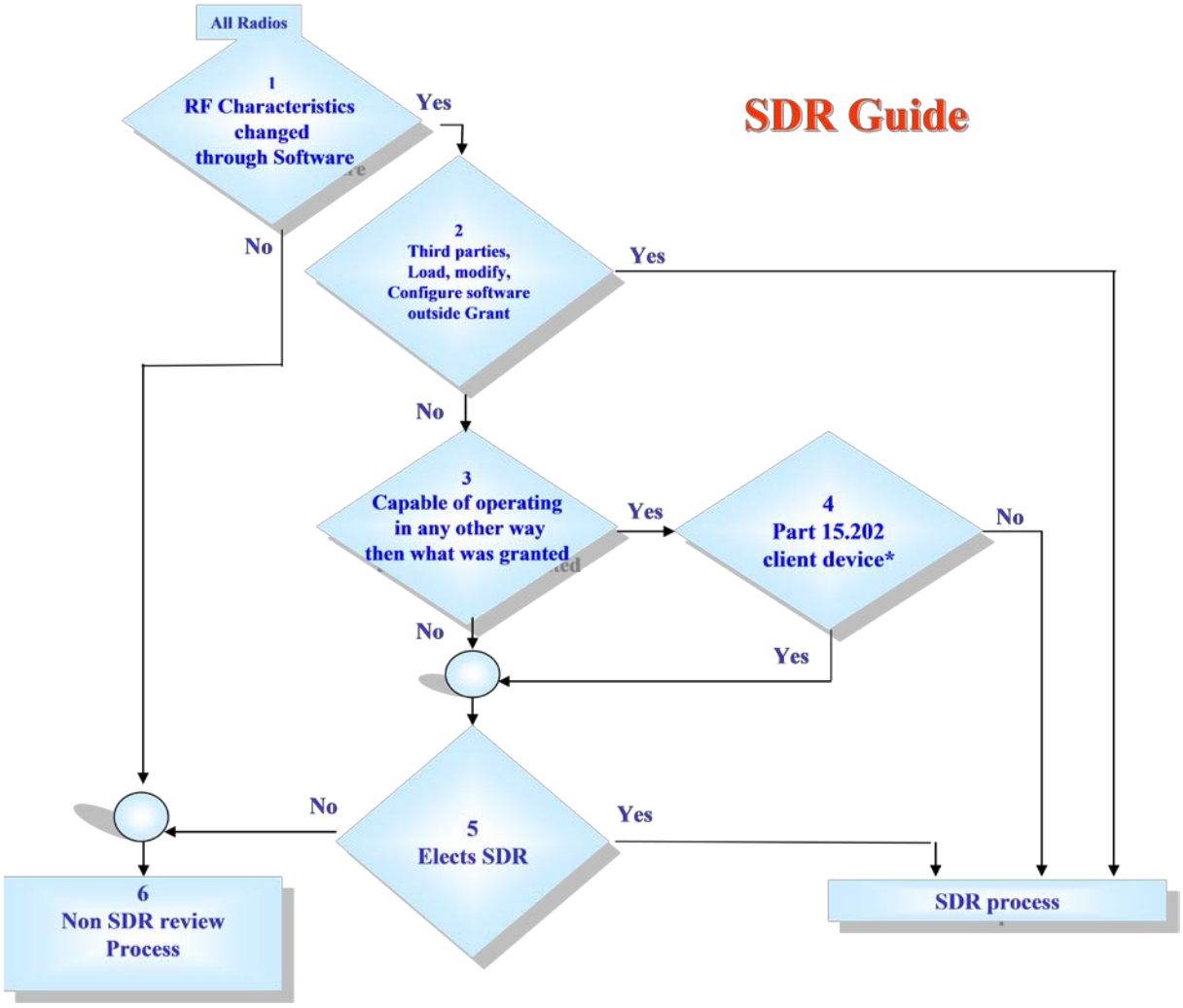
All Radios
1
RF Characteristics changed through Software
Yes
No
SDR Guide
2
Third parties, Load, modify, Configure software outside Grant
Yes
No
3
Capable of operating in any other way then what was granted
Yes
4
Part 15.202 client device*
No
No
Yes
No
5
Elects SDR
Yes
6
Non SDR review Process
SDR process

FIGURE 1

II. SOFTWARE DEFINED RADIO SECURITY DESCRIPTION GUIDE

The following table can be used as a reference guide by the applicant to describe how their system meets the security requirements for Section 2.944 Software Defined Radios. An applicant must describe the security measures and systems that ensure that only authenticated, legal (as granted) software is loaded and operating the device.

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. An applicant may select to copy the table and replace the examples in the applicant response column to provide answers and reference attachments.

The security description shall be considered confidential. The Form 731 SDR exhibit folder will not be available for public view and remains confidential.

1	Description Software (Section 2.944 (c))	1.1	General software operational description.
		1.2	Describe all the radio frequency parameters that are modified by the software without any hardware changes.
		1.3	High level (simplified) block diagram of the software architecture.
2	Labelling	2.1	How is the device to be labeled? Will the device have a single label or will it use an electronic label per Section 2.925 (e)?
		2.2	How can the FCC verify, in the field, that the correct version of the software is running in the device? Submit a description of this capability and instructions for the FCC to use in the field to verify that proper software is operating in the device.
		2.3	Describe the means by which software version numbers can be related to any future Class III permissive changes. For example: v01.01 was the software version for the Initial grant. Version v17.01 was for the first Class III Change. Any Version betweenV01.001 to V16.99 is assumed to be representative of the equipment exhibits in the initial grant. Version V22.15 would represent the version as modified by the Class III change.
3	Security	3.1	Describe the procedure that ensures that third parties (Professional installers, qualified personnel, authorized certified technicians, end users, etc. – not direct employees) cannot operate US sold devices on any other regulatory domain frequencies, or in any manner that is in violation of the certification.
		3.2	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.
		3.3	Describe how the software updates are distributed for all regulatory domains and what procedures ensures that a product sold in the US can only operate as granted on US frequencies and at authorized radio parameters.
		3.4	If the product cannot be modified by third parties and can only operate as granted on US frequencies and with authorized radio parameters, explain how this is achieved.
		3.5	What stops third parties from loading non-US versions of software onto products intended for US sale?
		3.6	Can third parties make factory level changes to reload non-US domain codes, etc.

4	Unauthorized changes (hack) to the software	4.1	Describe how open source is the operating code for granted RF properties. Describe the difficulty and proprietary nature of the code that controls the RF parameters as granted.

III. PERMISSIVE CHANGES FOR SDR OR CHANGES IN FCC ID

Class I:

- Changes in the equipment that does not degrade the characteristics reported.
- SDR is no different than non-SDR grant.

Class II:

- Changes in the host hardware equipment that affect the characteristics.
- Any Class II change (even for adding new antenna types) will prevent the grantee from making future Class III changes.

Class III:

If there are no host hardware changes or previous Class II changes, there is no limit to the number of Class III changes:

- Modifications to software that affect RF parameters that degrade original reported RF parameters, but still meet the rules for original equipment class. Submit test documentation similar to the Class II requirements for non-SDR.
- Adding new technical rule part and/or equipment class. For example, an SDR first granted as a Section 15.247 DTS device could later add Part 15 Subpart E, U-NII. Submit a complete set of new test documentation for a new equipment class, similar to the procedures for a non-SDR.
- Major changes in Software Distribution and Security (SDS) that materially change the descriptions provided on the initial grant require a Class III permissive change. Do not submit only the changes. A full description is required. The Class III documentation in effect, replaces the original description in its entirety.

A Class III change should also include a statement:

- To identify all versions of software that are approved in the original grant, and all other granted Class III permissive changes including the requested Class III change.
- That confirms that there is no change to the Software Distribution and Security documentation. If there is such a change, then a Class III resubmission of SDS security documentation is also required.

Changes in FCC ID under Section 2.933 require a new application be filed. This new application requires an initial grant PBA procedure (see section IV below) with a description explaining how the new applicant responsible for the change in FCC ID meets the security requirements for Section 2.944 for a Software Defined Radio.

IV. U-NII DEVICES CERTIFIED AS SDR

In addition to providing a security description as stated in this publication, U-NII devices seeking certification as SDR must address additional security aspects related to U-NII devices.[11] To supplement the software security description, these questions from KDB Publication 594280 D02 must be answered[12]:

- Section II - Software Security Description/General Description – Questions 3 to 6.
- Section II - Software Security Description/Third-Party Access Control – Questions 1 and 2
- All of Section III – User Configuration Guide

V. PERMIT BUT ASK PROCEDURE

TCBs are permitted to approve SDR(s) subject to a Permit-But-Ask (PBA)[13] procedure prior to an initial or a Class III permissive change application. The TCB must submit the following with the PBA request:

1. State if the PBA is an initial grant or permissive change.
2. For an initial grant or permissive change to the Software, Distribution and Security Documentation provide:
    a. Manuals and operational descriptions to allow the reviewer to understand the product and its operation.
    b. Provide the software security description information requested organized in the format defined in Section II of this guide.
3. If there is no change in the original granted security procedure, a PBA for a permissive change is still required. The permissive change request must state that there is (1) no Class II hardware change and (2) no change to the original Software, Distribution and Security procedure.

Guidance found in KDB Publication 388624 must be followed to submit the PBA. The TCB is responsible for ensuring that all the requirements for all the applicable rule parts have been met. The checkbox for SDR on the initial Form 731 must be marked and the software description must be uploaded as specific exhibit. (Note that the software description is automatically marked confidential). After a review of the Form 731, the KDB Inquiry, and all uploaded exhibits, the FCC reviewer will modify the application to permit the grant to be issued, and inform the TCB through the KDB (under the same PBA KDB Inquiry number) that the grant can be issued.

[11] *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). Devices may be approved under the U-NII rules effective prior to June 2, 2014 during a transition period of one year for new applications and two years for permissive change application without providing additional security requirements. *See* KDB Publication 926956.

[12] *See* KDB Publication 594280 D02 U-NII Device Security.

[13] The Commission has established a "Permit but Ask (PBA)" procedure (*See* KDB Publication 388624) for certain devices prior to an equipment authorization.

Change Notice:

12/02/2009: 442812 D01 SDR Apps Guide v01, original publication.

02/24/2011: 442812 D01 SDR Apps Guide v01 has been changed to 442812 D01 SDR Apps Guide v02. Item I Introduction: paragraph 3 and note 6 have been added to permit specific third parties permission to upgrade non SDR grants.

10/24/2012: 442812 D01 SDR Apps Guide v02 has been changed to 442812 D01 SDR Apps Guide v02r01. Removed the requirement for non-SDR to file a Class II permissive change directly with the Commission.

10/31/2013: 442812 D01 SDR Apps Guide v02r01 has been changed to 442812 D01 SDR Apps Guide v02r02. Clarified Section IV Permit But Ask Procedure, that a PBA is required for an initial or Class III application.

07/17/2014: 442812 D01 SDR Apps Guide v02r02 has been changed to 442812 D01 SDR Apps Guide v02r03. Added Section IV for U-NII device security requirements subject to new rules effective June 2, 2014.