

AACS RED LASER RECORDER ROBUSTNESS RULES APPLICABLE TO 4C HIGHLY CONFIDENTIAL INFORMATION (4C CPRM DEVICE KEYS) AND 4C CONFIDENTIAL INFORMATION (4C SECRET CONSTANTS)

1. CONSTRUCTION

- 1.1 **Generally.** These Robustness Rules shall be applicable to AACS Red Laser Recorders implementing the 4C Media Verification Specification and shall specifically apply to the portions of AACS Red Laser Recorders with respect to the treatment of 4C Highly Confidential Information in the form of 4C CPRM Device Keys and 4C Confidential Information in the form of 4C Secret Constants. In that regard, an AACS Red Laser Recorder shall meet these Robustness Rules as shipped and be designed and manufactured so as to resist attempts to modify such products so as to defeat the requirements set forth below.
- 1.2 **Keep Secrets.** AACS Red Laser Recorders shall be designed and manufactured such that they shall resist attempts to discover or reveal Device Keys, other 4C Highly Confidential Information, or secret intermediate calculated cryptographic values used in the 4C Technology.
- 1.3 **Keep Confidential.** AACS Red Laser Recorders shall be designed and manufactured such that they shall resist attempts to discover 4C Confidential Information in the form of 4C Secret Constants. Adopter's compliance with these Robustness Rules with regard to 4C Confidential Information shall be fulfilled by compliance with this Section 1.4 and Sections 3.2, 3.3 and 4 of these Robustness Rules.

2. METHODS OF MAKING FUNCTIONS ROBUST

AACS Red Laser Recorders shall use at least the following techniques to be designed to effectively frustrate efforts to circumvent or defeat the functions and protections in the following manner:

- 2.1 **Robustness Requirements Applicable to Software Implementations.** Any portion of an AACS Red Laser Recorder that implements the 4C Media Verification Specification in software shall include all of the characteristics set forth in Section 1 of these Robustness Rules. In addition, such implementations shall –

2.1.1 Comply with Section 1.2 of these Robustness Rules by reasonable methods, which may include, but shall not be limited to: encryption, execution of a portion of the implementation in ring zero or supervisor mode, and/or embodiment in a secure physical implementation; and in every case of implementation of software, using techniques of obfuscation to disguise and hamper attempts to discover the approaches used.

2.1.2 Be designed so as to perform self-checking of the integrity of its component parts and be designed to result in a failure of the implementation to provide the authorized Security Functions in the event of unauthorized modification. For these purposes, a "modification" includes any change in, or disturbance or invasion of features or characteristics, or interruption of processing, relevant to Section 1 of these Robustness Rules. This provision requires at a minimum the use of "signed code" or other means of tagging or operating throughout the code which are equivalent or more robust.

2.2 **Robustness Requirements Applicable to Hardware Implementations.**

Any portion of the AACS Red Laser Recorder that implements the 4C Media Verification Specification in hardware shall include all of the characteristics set forth in Section 1 of these Robustness Rules. The fact that a software implementation operates on a hardware computing platform shall not, in and of itself, cause such hardware computer platform to be subject to the requirements set forth in Sections 2.2 and 2.3. If, however, the software implementation relies on hardware or any hardware component to satisfy these Robustness Rules, then such hardware or hardware component shall be governed by the robustness rules set forth herein for hardware implementations. In addition, such Implementation shall:

2.2.1 Comply with Section 1.3 of these Robustness Rules by reasonable means including, but not limited to: embedding 4C CPRM Device Keys and other Highly Confidential information in silicon circuitry or firmware which cannot reasonably be read, or the techniques described above for software.

2.2.2 Be designed such that attempts to remove or replace hardware elements in a way that would compromise the content protection features of the 4C technology would pose a serious risk of damaging the AACS Red Laser Recorder so that it would no longer be able to execute the Security Functions. By way of example, a component which is soldered rather than socketed may be appropriate for these means.

2.2.3 Be designed such that the failure of a Security Function would cause the product to no longer be able to receive, playback, or record AACS Content.

2.3 **Robustness Requirements Applicable to Hybrid Implementations.**

The interfaces between hardware and software portions of a Participating Device shall be designed so that the hardware portions comply with the level of protection that would be provided by a pure hardware

implementation, and the software portions comply with the level of protection which would be provided by a pure software implementation.

3. REQUIRED LEVELS OF ROBUSTNESS

- 3.1 The Security Functions and the characteristics set forth in Section 1.2 shall be implemented so that it is reasonably certain that they:
 - 3.1.1 Cannot be defeated or circumvented using Widely Available Tools (Section 3.3) or Specialized Tools (Section 3.4) and
 - 3.1.2 Can only with difficulty be defeated or circumvented using Professional Tools (Section 3.5).
- 3.2 The characteristics set forth in Section 1.3 shall be implemented so that it is reasonably certain that they:
 - 3.2.1 Can only with difficulty be defeated or circumvented using Widely Available Tools (Section 3.3).
- 3.3 “Widely Available Tools” shall mean general-purpose tools or equipment that are widely available at a reasonable price, such as screwdrivers, jumpers, clips, file editors, and soldering irons.
- 3.4 “Specialized Tools” shall mean specialized electronic tools that are widely available at a reasonable price, such as memory readers and writers, debuggers, decompilers, or similar software development products other than devices or technologies that are designed and made available for the specific purpose of bypassing or circumventing the protection technologies that are required by the 4C Media Verification Specification, i.e., "Circumvention Devices".
- 3.5 “Professional Tools” shall mean professional tools or equipment, such as logic analyzers, chip disassembly systems, or in circuit emulators, but not including either professional tools or equipment that are made available on the basis of a non-disclosure agreement or Circumvention Devices.
- 3.6 “Security Functions” shall mean the authentication and cryptographic functions used for media verification as set forth in the 4C Media Verification Specification.

4. NEW CIRCUMSTANCES

If a particular implementation of an AACS Red Laser Recorder when designed and shipped complies with the requirements set forth above, but at any time

thereafter circumstances arise which — had they been existing at the time of design — would have caused such implementation to fail to comply with these Robustness Rules ("New Circumstances"), then upon having reasonable notice of such New Circumstances, the developer of such implementation shall promptly redesign affected product(s) or make available upgrades to its affected product(s), and, as soon as reasonably practicable, consistent with ordinary product cycles and taking into account the level of threat to content under the New Circumstances, shall incorporate such redesign or replacement into its affected product(s), cease manufacturing such affected product(s) and cease selling such affected product(s).

5. EXAMINATION/INSPECTION

Adopter agrees that, under reasonable terms and upon notice given by any Eligible Content Participant (as that term is defined in the AACS Content Participant Agreement) that such Eligible Content Participant reasonably and in good faith believes that a particular model or version of an AACS Red Laser Recorder designed or manufactured by Adopter does not comply with these Robustness Rules, such Eligible Content Participant may designate an independent expert acceptable to Adopter (which acceptance shall not be unreasonably withheld) to inspect the details necessary and sufficient to determine whether Adopter's AACS Red Laser Recorder is in compliance with these Robustness Rules. Such inspection shall be at the Eligible Content Participant's expense and shall be conducted at mutually convenient times. By way of example, "details necessary and sufficient" (as used in the sentence above) include the executable object code, functional design diagrams, examples of the product, or block diagrams but shall not include the source code, the Verilog Hardware Description Language ("VHDL") or similar highly confidential information. Beyond providing access to the aforementioned details, Adopter's active participation in such inspection shall be voluntary. Adopter shall not be precluded or estopped from challenging the opinion of such expert in any forum. Nothing in this paragraph shall limit the role or testimony of such expert, if any, in a judicial proceeding under such protective orders as a court may impose. This provision may not be invoked more than once per implementation, model or version, except to the extent that one or more Eligible Content Participants are re-inspecting such implementation, model, or version that has been revised in an effort to cure any alleged failure of compliance. For purposes of this Section 6, "reasonable terms" shall include, at a minimum, execution of non-disclosure agreements that (x) are applicable to Eligible Content Participant and any independent expert retained by Eligible Content Participant pursuant to this Section, (y) are acceptable to Adopter and Eligible Content Participant, and (z) provide protections for Confidential and Highly Confidential Information relating to the 4C Technology that are no less stringent than those provided for in this Agreement.