

**DFAST TECHNOLOGY LICENSE AGREEMENT
FOR UNIDIRECTIONAL DIGITAL CABLE PRODUCTS
Jan 2014**

THIS LICENSE AGREEMENT (the “**Agreement**”) is made as of _____ (the “Effective Date”), by and between _____, having a place of business at _____ (“**Licensee**”), and **CABLE TELEVISION LABORATORIES, INC.**, having a place of business at 858 Coal Creek Circle, Louisville, Colorado, USA 80027-9750 (“**CableLabs**”).

WHEREAS, CableLabs is a research and development company funded by the cable television industry;

WHEREAS, CableLabs has acquired the rights to the DFAST scrambling technology, portions of which are embodied in a U.S. patent;

WHEREAS, Licensee is in the business of, among other things, designing, developing, manufacturing and distributing products related to digital television; and

WHEREAS, this Agreement provides a right to use the DFAST scrambling technology;

NOW, THEREFORE, in consideration of the foregoing and of the mutual covenants and agreements set forth herein, the parties hereby agree as follows:

1. DEFINITIONS. In addition to terms defined elsewhere in this Agreement, the following terms shall have the following meanings. All definitions herein shall apply equally to their singular and plural forms, all pronouns shall apply without regard to gender, and all references to Sections and Exhibits shall be deemed to be references to Sections of, and Exhibit to, this Agreement unless the context shall otherwise require.

1.1 “Cable Operator” means any cable operator that CableLabs identifies on its <www.cablelabs.com> website as a member and any other cable operator that provides POD Modules to customers in connection with the provision of cable services in North America.

1.2 “Compliance Rules” mean the rules described in Exhibit B hereto, as such rules may be amended from time to time pursuant to Section 6.2.

1.3 “Compliant” refers to a product that is in compliance with all applicable Compliance Rules and Robustness Rules.

1.4 “Controlled Content” means content that has been transmitted from the POD Module with the encryption mode indicator (“EMI”) bits set to a value other than zero, zero (0,0), or with copy control information (“CCI”) otherwise marked to indicate restrictions on access, copying, distribution, or usage rights.

1.5 “Derivative Work” means any work that is based upon DFAST Technology, other than the Referenced Technology, such as a revision, improvement, enhancement, modification, translation, abridgment, condensation, expansion, collection, compilation or other form in which such DFAST Technology may be recast, transformed, ported or adapted and that, if prepared without authorization of CableLabs, would constitute infringement of the DFAST Technology.

1.6 “DFAST Technology” means the Licensed Patents collectively with the Licensed Know-How.

1.7 “Documentation” means user manuals and other written materials (whether in print or electronic form) that relate to the DFAST Technology that have been provided by CableLabs hereunder, including materials for design (for example, flow charts and principles of installation, configuration, administration, and operation) and machine readable text or graphic files subject to display or print-out.

1.8 “Encoding Rules” means the rules of the United States Federal Communications Commission applicable to use of the Compliance Rules.

1.9 “Essential Patent Claim(s)” means claims of a patent or patent application pending on the effective date of this Agreement, issued now or in the future, that are necessarily infringed by those portions of Unidirectional Digital Cable Products that implement inventions claimed in US Patent 4,860,353. Without limiting the foregoing, Essential Patent Claims shall not include (a) any claims relating to semiconductor manufacturing technology; (b) claims relating to aspects of any technology or standard that is not itself part of the Referenced Technology (including by way of example, CSS, MPEG, IEEE 1394, DES, NRSS and smart card technology) even if such standard may otherwise be mentioned or required by the Referenced Technology; (c) claims which, if licensed, would require a payment of royalties by the licensor to unaffiliated third parties; (d) claims relating to any technology introduced into the Referenced Technology, the Compliance Rules or the Robustness Rules pursuant to changes made in accordance with Section 6; or (e) any claims other than those that are necessarily infringed by those portions of Unidirectional Digital Cable Products that implement the inventions claimed in US Patent 4,860,353, even if contained in the same patent as such claim(s).

1.10 “Intellectual Property Rights” means all intellectual property rights arising under statutory law, common law or by contract, and whether or not perfected, including, without limitation, all (a) patents, patent applications and patent rights, (b) rights associated with works of authorship including copyrights, copyright applications, copyright registrations, mask work rights, mask work applications, mask work registrations, and derivative works of the foregoing, (c) rights relating to the protection of trade secrets and confidential information, (d) trademarks, trade dress, trade name, design patent and service mark rights, whether or not registered and (e) divisions, continuations, continuations in part, renewals, reissues and extensions of the foregoing (as and to the extent applicable) now existing, hereafter filed, issued or acquired.

1.11 “Licensed Components” means component products which utilize the DFAST Technology and are designed for incorporation into Unidirectional Digital Cable Products.

1.12 “Licensed Know-How” means all know-how, associated technology, trade secrets, copyrighted works, reference source code implementations, shared secret keys, Diffie-Hellman system parameters, encryption and decryption keys, software development tools, methodologies, processes, technologies or algorithms, test data sets and test cases and other implementations of technology that CableLabs shall deliver to Licensee to assist in incorporating the DFAST Technology into Licensed Components, Prototypes, or Unidirectional Digital Cable Products.

1.13 “Licensed Patents” means U.S. Patent 4,860,353, any application, division, continuation or continuation in part of the foregoing patent, any patent reissuing on or reissuing pursuant to a reexamination of the foregoing patent and all foreign equivalents that CableLabs owns or has the rights to license.

1.14 “Prototype” means a pre-production model of a Unidirectional Digital Cable Product that is not sold commercially.

1.15 “POD Module” means an individual addressable device for authorizing and de-authorizing the decryption or descrambling of services and individual programs and events delivered through the Unidirectional Digital Cable Product on a service by service or individual program or event basis.

1.16 “Referenced Technology” means those standards set forth on Exhibits A and A1 hereto; provided however, Referenced Technology does not include any third party proprietary technology referenced in or required by such standards, such as DES, DTCP, or MPEG-2.

1.17 “Robustness Rules” mean the rules described in Exhibit C hereto, as such rules may be amended from time to time in accordance with Section 6.2.

1.18 “Test Tools” means devices that (a) utilize the DFAST Technology and have as their purpose the testing or verification of the performance of, or (b) are specifically designed for the purpose of testing or verification of the performance of, Unidirectional Digital Cable Products and Prototypes.

1.19 “Unidirectional Digital Cable Products” means unidirectional (“one-way”) digital television products (including without limitation, televisions, set-top-boxes and recording devices) that use the DFAST Technology. Unidirectional Digital Cable Products shall not include interactive (“two-way”) digital television products, including, without limitation, products that are capable of obtaining access to video-on-demand or impulse pay-per-view services, of using the return path of the cable system, or of using electronic program guide services provisioned by the Cable Operator.

2. SCOPE

2.1 License for Unidirectional Digital Cable Products. A license is granted herein only for Compliant Unidirectional Digital Cable Products, Licensed Components and Prototypes and Test Tools. No license is granted hereunder for manufacture, sale or distribution of advanced interactive (two-way) digital cable products.

2.2 Unidirectional Digital Cable Products. Unidirectional Digital Cable Products at the time of manufacture shall be Compliant and shall conform to the Referenced Technology as required by this Agreement. No feature or functionality of a Unidirectional Digital Cable Product, as manufactured and distributed, shall (a) technically disrupt, impede or impair the delivery of services to a cable customer; (b) cause physical harm to the network or the POD; (c) facilitate theft of service or otherwise interfere with reasonable actions taken by Cable Operators to prevent theft of service; (d) jeopardize the security of any services offered over the cable system; or (e) interfere with or disable the ability of a Cable Operator to communicate with or disable a POD Module or to disable services being transmitted through a POD Module.

3. LICENSE GRANTS AND RESTRICTIONS.

3.1 License for DFAST Technology. Subject to the terms and conditions set forth herein, CableLabs hereby grants to Licensee, and Licensee hereby accepts from CableLabs, a non-exclusive, non-transferable (except as set forth in Sections 3.2, 3.3 and 12.6 hereof) worldwide license under Intellectual Property Rights owned or licensable by CableLabs in the DFAST Technology to:

- (a) possess and use the DFAST Technology to develop and test Prototypes, Test Tools, and Licensed Components;
- (b) distribute the Test Tools and Licensed Components only to entities who have obtained a license from CableLabs for the use of the DFAST Technology (including, without limitation, entities that have obtained such license under PHILA or otherwise) (collectively, “**CableLabs Licensees**”) and have made parties;
- (c) distribute Prototypes to Cable Operators and other entities for the purpose of field trials and technology evaluation and not for retail;
- (d) make, have made, use, sell, offer to sell, import and otherwise distribute in North America Unidirectional Digital Cable Products;
- (e) practice any method or process under the DFAST Technology solely as necessary for the manufacture or use of products using the DFAST Technology in accordance with the terms and conditions of this Agreement;
- (f) Any right granted hereunder to the DFAST Technology is also granted with respect to the DFAST Technology as implemented in a Derivative Work, provided that the

rights granted under this section 3.1(f) shall be subject to all of the limitations set forth in this Agreement with respect to the DFAST Technology;

(g) use and reproduce the Documentation in order to modify the Documentation as reasonably required in connection with Licensee's creation of Derivative Works in accordance with this Agreement; and

(h) distribute the modified Documentation to customers in connection with the distribution of Unidirectional Digital Cable Products in accordance with this Agreement, provided that such modified Documentation shall not reveal any confidential information contained in the DFAST Technology.

3.2 Limited Right for Test Tools. In addition to the rights granted under Section 3.1(a) and 3.1(b), Licensee shall have the limited right to make, have made, use, sell, offer to sell and otherwise distribute Test Tools, subject to the following limitations:

(a) Licensee shall distribute the Test Tools containing the DFAST Technology only to other CableLabs Licensees or have made parties. Licensee must separately maintain records of sales of Test Tools, and Licensee shall provide the names and contact information of each purchaser to CableLabs.

(b) Licensee shall limit the use of Test Tools for the purposes of ensuring proper operation, testing, debugging, integration and tuning. For the purposes of this Section 3.2(b): (i) "testing" shall mean a process of evaluating a Prototype or Unidirectional Digital Cable Product to ensure proper operation; (ii) "debugging" shall mean a process of finding the cause of an error in a Prototype or Unidirectional Digital Cable Product, including analysis for the purpose of exposing possible design flaws; (iii) "integration" shall mean a process of evaluating the performance of a Prototype or a Unidirectional Digital Cable Product with a POD Module to ensure that they properly operate together; and (iv) "tuning" shall mean a process of evaluating and improving a Prototype or Unidirectional Digital Cable Product to work more efficiently with a POD Module.

3.3 Limited Right for Licensed Components. Licensee shall have the limited right to make, have made, use, sell, offer to sell, import and otherwise distribute Licensed Components provided, however, that Licensee shall distribute the Licensed Components only to other CableLabs Licensees or have made parties; and provided further that Licensee must separately maintain records of sales of Licensed Components, and Licensee shall certify, upon request of CableLabs, that Licensed Components have been distributed only to other CableLabs Licensees that are listed on the CableLabs website (www.opencable.com) or to have made parties.

3.4 No Other Licenses Granted. Except as provided herein, no license is granted by CableLabs, either directly or by implication, estoppel, or otherwise, and any rights not expressly granted to Licensee hereunder are reserved by CableLabs. No license is granted for any products (other than Licensed Components, Test Tools and Prototypes) that are not Compliant. All Intellectual Property Rights (except for Derivative Works made by Licensee which shall be

owned by Licensee) in the DFAST Technology shall be and remain the sole property of CableLabs or such companies that have licensed the DFAST Technology to CableLabs, and Licensee shall have no rights or interest in such DFAST Technology other than the rights granted to Licensee under this Agreement. CableLabs retains all right, title and interest in and to the Licensed Know-How used in connection with the DFAST Technology that are trade secrets or proprietary information of CableLabs or its licensors, members or affiliates or are otherwise owned or licensed by CableLabs.

3.5 Availability of Essential Patent Claims on Fair, Reasonable, and Non-Discriminatory Terms. With respect to all Essential Patent Claims owned or controlled by Licensee, Licensee agrees to make licenses, or cause licenses to be made, available for such Essential Patent Claims on terms that are fair, reasonable, and non-discriminatory to any third party that desires to implement or has implemented the DFAST Technology in Unidirectional Digital Cable Products or Licensed Components. Such license may be limited to products or services that are made, sold, or offered for sale in accordance with the terms of such third party's DFAST Technology License Agreement for Unidirectional Digital Cable Products. In addition, Licensee shall only be bound by this Section 3.5 to the extent such third parties submit to an equivalent undertaking with respect to any Essential Patent Claims owned or controlled by such third party.

3.6 Joint Defense of Intellectual Property Claims. If CableLabs on the one hand and/or Licensee on the other hand (each, a "**Defendant**"), should be sued on a single claim or related claims that the DFAST Technology necessarily infringes the patent or other rights of another party (a "**Suit**"), then the Defendants shall, subject to reasonable non-disclosure conditions, provide to each other reasonable non-privileged information and cooperation relating to their Suits, and CableLabs shall (subject to advice of litigation counsel) permit participation in the Suit by a Licensee that is not a Defendant at its own expense. Further, unless Licensee elects to independently defend the Suit, CableLabs and Licensee shall endeavor to negotiate in good faith a joint defense agreement whereby common claims against all Defendants may be defended in a coordinated and efficient manner. Provided that Licensee is a Defendant and is not exercising its right to pursue an independent defense of a Suit, CableLabs and Licensee shall establish a joint steering committee to negotiate in good faith allocations of joint defense costs where possible. Licensee shall have the right, in its sole discretion and at its sole expense, to pursue an independent defense of any Suit.

3.7 Technology Substitution in the Event of a Claim of Infringement. If CableLabs on the one hand or Licensee on the other hand receives notice that the DFAST Technology allegedly infringes a patent of a third party, then CableLabs may, at its sole option and expense, obtain for Licensee the right to use technology that is substantially equivalent to the DFAST Technology and does not infringe such patent.

4. DELIVERY OF LICENSED KNOW HOW; PRODUCTION FORECASTS.

4.1 Digital Certificates. At any time after Licensee has paid the License Fee (as defined in Section 5.1), Licensee may execute the Digital Certificate Authorization Agreement

(DCAA) in order to obtain associated digital certificates. Prior to paying the fees required under the DCAA, Licensee is not licensed to distribute any products or components hereunder, and the provisions of Sections 3.1, 3.2, and 3.3 and 3.5, 3.6 and 3.7 shall only be applicable after such DCAA fees are paid.

4.2 Delivery of Licensed Know-How. CableLabs agrees to deliver to Licensee one copy of the Licensed Know-How within ten days of the receipt by CableLabs of the DCAA Fees. Upon the request of such Licensee, CableLabs shall supply such Licensee with one or more additional copies of the Licensed Know-How as may be required for Licensee's operations. CableLabs reserves the right to charge a reasonable administrative fee in connection with such additional copies. Except as provided in Section 3.1(h), Licensee shall not make further copies of any Licensed Know-How provided pursuant to this Section 4, and shall treat all such information strictly in accordance with the provisions of Sections 7.1 through 7.3.

4.3 Production Forecasts. Licensee, together with other persons who are licensees under a DFAST Technology License Agreement for Unidirectional Digital Cable Products, shall provide to the Consumer Electronics Association ("CEA") confidential production forecasts of the number of Unidirectional Digital Cable Products that are expected to be entering the marketplace. Such monthly forecasts shall be provided to CEA for a rolling five-month period for five years from the month that the first Unidirectional Digital Cable Product is self-certified. This information shall be provided to CEA with the understanding that CEA shall aggregate such information, and provide the aggregate information to CableLabs on a monthly basis. CableLabs will issue only aggregate unit volume reports to Cable Operators for use in their planning. Except as specifically provided herein, CableLabs and Cable Operators shall not use or disclose information provided under this Section 4.3 in any manner whatsoever.

5. FEES; APPLICABLE TAXES.

5.1 License Fee. As consideration for the licenses granted hereunder, Licensee agrees to pay CableLabs a one-time, non-refundable license fee of \$5,000 (the "**License Fee**") within thirty days of the Effective Date.

5.2 Applicable Taxes. CableLabs is exempt from income tax in the United States under Section 501(c)(6) of the Internal Revenue Code. The License Fee owed by Licensee to CableLabs is exclusive of, and Licensee shall pay, all sales, use, value added, excise, income tax, and other taxes (other than income taxes) that may be levied upon either party by taxing authorities other than the United States in connection with this Agreement (except for taxes based on CableLabs' employees) and shall pay all income taxes that may be levied upon Licensee.

6. CHANGES TO GOVERNING DOCUMENTS. The Compliance Rules and the Robustness Rules may be amended from time to time only in accordance with the procedures set forth below.

6.1 Referenced Technology. CableLabs may, from time to time, give notices to Licensee for the purpose of providing advice, correcting any errors or omissions or clarifying, but not materially amending, altering or expanding the Referenced Technology.

6.2 Changes to the Compliance Rules and Robustness Rules. Except for a minor change that does not alter existing requirements or add new requirements, and except for permissive changes that are not binding on licensee (e.g., changes to authorize additional outputs, content protection or copy protection technologies pursuant to Sections 2.4 or 3.5 of the Compliance Rules), CableLabs may change the Compliance Rules and the Robustness Rules only in accordance with this Section 6.2. CableLabs shall notify all DFAST Licensees (as defined below) simultaneously of any changes to the Compliance Rules and Robustness Rules, and Licensee shall be required to comply with such changes within 12 months following the date (the “**Change Notice Date**”) that Licensee is deemed, pursuant to Section 12.7 of this Agreement, to have received the notice from CableLabs setting forth the change in the Compliance Rules or the Robustness Rules (a “**Change Notice**”), or within such longer period as CableLabs may, at its election, specify in a Change Notice, except as provided in this Section 6.2. In the event Licensee, together with either (i) two unaffiliated licensees under a DFAST Technology License Agreement for Unidirectional Digital Cable Products (a “**DFAST Licensee**”), or (ii) such number of other DFAST Licensees that, together with Licensee, constitute a majority of all DFAST Licensees), notifies CableLabs within sixty (60) days following the Change Notice Date that it has a bona fide objection to the change on the grounds that it would materially limit the permitted functionality or capabilities of a Unidirectional Digital Cable Product, or would materially increase its cost or complexity, then the following procedures shall govern whether or not Licensee shall be required to comply with such change:

If the required number of DFAST Licensees specified above notify CableLabs that they object to the change proposed in the Change Notice:

(a) CableLabs and the DFAST Licensees shall attempt in good faith to resolve any objections that the DFAST Licensees may have with respect to the proposed change during the sixty (60) day period following the Change Notice Date.

(b) At any time during such sixty (60) day period, Licensee may file a petition at the FCC for review of the proposed change in accordance with FCC regulations for expedited resolution of disputes regarding proposed changes to the Compliance Rules and Robustness Rules. The parties anticipate that the FCC shall determine in an expedited 90-day proceeding whether the proposed change serves the public interest, taking into account its effect on consumers, Licensees and Cable Operators; competition, innovation, developments in technology; and the need to protect Controlled Content.

(c) If the FCC disapproves the proposed change on or before the date that is one hundred eighty (180) days following the Change Notice Date, the proposed change shall not become effective.

(d) If the FCC approves the proposed change on or before the date that is one hundred eighty (180) days following the Change Notice Date, Licensee shall be required to comply with such changes within twelve (12) months following such approval.

(e) If the FCC fails to approve or disapprove the proposed change within one hundred eighty (180) days following the Change Notice Date, Licensee shall be required to comply with such change within eighteen (18) months following the Change Notice Date.

7. CONFIDENTIALITY

7.1 Confidentiality of Licensed Know-How. As between CableLabs and Licensee, all of the Licensed Know-How is confidential and proprietary to CableLabs or the companies that have licensed to CableLabs. Licensee shall not use or disclose Licensed Know-How in any manner whatsoever other than in connection with the rights granted in Section 3 hereof or as otherwise permitted by this Section 7. Licensee shall implement and maintain security measures in order to keep the Licensed Know-How confidential which are at least as rigorous as Licensee employs for its own confidential information. Licensee shall implement and maintain security measures for reference source code implementations, shared secret keys, Diffie-Hellman system parameters, encryption and decryption keys, private keys and DFAST source and library files that contain DFAST constants (collectively, “Highly Confidential Information”), which are in accordance with commercial practices for managing keys, such measures to include, at a minimum, the following:

(a) Licensee shall transmit Highly Confidential Information only to its affiliates, subcontractors, consultants, agents, employees, customers and representatives who need to know the information, who are informed of the confidential nature of the information, and, in the case of affiliates, representatives, customers, subcontractors and consultants who have agreed in writing to abide by the terms and conditions of this Section 7. Licensee shall identify (by title) individuals with access to such Highly Confidential Information to CableLabs upon request.

(b) Licensee shall maintain a secure location on its premises to be identified to CableLabs in which such Highly Confidential Information shall be stored. Such secure location shall be accessible only by authorized employees who shall be required to sign in and out each time such employees visit such secure location. When such Highly Confidential Information is not in use, such information shall be stored in a locked safe at such secure location. Licensee may store such Highly Confidential Information at more than one secure location with the prior approval of CableLabs, which approval shall not be unreasonably withheld.

(c) Licensee shall maintain a security log of periodic tests of security, shipments of such Highly Confidential Information from one secure location to another (if applicable), and breaches of security at all secure locations. Licensee shall reasonably cooperate with CableLabs and its employees and agents to maintain the security of such Highly Confidential Information, including by promptly reporting to CableLabs any thefts of such Highly Confidential Information missing from Licensee’s possession.

(d) CableLabs shall have the right to review, upon five (5) business days notice, or such earlier time as may be reasonable and required due to special circumstances, the implementation of all security measures at the secure location(s) required hereunder for Highly Confidential Information on an ongoing basis, at reasonable times as agreed between Licensee and CableLabs, subject to a mutually agreed upon reasonable non-disclosure agreement prior to CableLabs' release of Highly Confidential Information to Licensee. Should Licensee prefer that such review be conducted by a third-party auditor, Licensee and CableLabs may agree upon one or more acceptable third-party auditors and a reasonable non-disclosure agreement, prior to CableLabs' release of Highly Confidential Information to Licensee.

7.2 Notification of Unauthorized Use or Disclosure. Licensee shall notify CableLabs immediately upon discovery of any unauthorized use or disclosure of Licensed Know-How, and will cooperate with CableLabs to seek to regain possession of the disclosed Licensed Know-How and to prevent its further unauthorized use or disclosure.

7.3 Liability for Breach of Confidentiality. With respect to information provided by CableLabs to Licensee, Licensee shall be responsible for any breach of Sections 7.1 through 7.2 by its affiliates, subcontractors, consultants, agents, employees, customers (other than CableLabs members), representatives, former affiliates, former agents, former employees, former customers (other than CableLabs members) and former representatives, provided that no obligation of confidentiality is imposed on information which (a) is already in or subsequently enters the public domain through no breach of Licensee's obligations hereunder and which CableLabs failed to remove from public availability or to enjoin such public disclosure within ninety (90) days after the date such information is or becomes generally known as set forth above; (b) is known to Licensee or is in its possession without conduct which would constitute a breach of Licensee's obligations hereunder prior to receipt from CableLabs; (c) is developed independently by Licensee by persons who have not had, either directly or indirectly, access to or knowledge of Licensed Know-How; or (d) is lawfully received by Licensee from another party without a duty of confidentiality to CableLabs. Notwithstanding anything in Sections 7.1 or 7.2 to the contrary, Licensed Know-How may be disclosed by Licensee pursuant to the order or requirements of a court or governmental administrative agency or other governmental body of competent jurisdiction, provided that (x) CableLabs has been notified of such a disclosure request sufficiently in advance to afford CableLabs reasonable opportunity to obtain a protective order or otherwise prevent or limit the scope of such disclosure to the extent permitted by law and (y) Licensee cooperates in good faith with CableLabs' efforts hereunder. The obligations under Sections 7.1 through 7.3 shall terminate three years after the last commercial use of the DFAST Technology by Licensee or any CableLabs licensee of the DFAST Technology; provided that Sections 7.1(b) through 7.1(d) shall cease to apply when Licensee has returned all tangible embodiments of Licensed Know-How in its possession to CableLabs.

8. TERM AND TERMINATION.

8.1 Term. The initial term of this Agreement shall be the life of the Licensed Patents and then, upon the expiration of the Licensed Patents, the term of this Agreement shall be

extended as to the Licensed Know-How automatically thereafter indefinitely on a year by year basis unless earlier terminated according to its terms; provided that under no circumstances shall the term of the license for the Licensed Patents granted pursuant to Section 3 of this Agreement exceed the patent term of the last of the Licensed Patents to expire.

8.2 Termination of Licenses for Cause. CableLabs may terminate the licenses granted hereunder for any specific model of Unidirectional Digital Cable Product that, at the time of manufacture, is in material breach of the Robustness Rules, the Compliance Rules or Section 2.2. However, CableLabs may only terminate the licenses pursuant to this Section 8.2 after the potential for a cure at low cost at the headend for the relevant service has been evaluated as a reasonable alternative and CableLabs has (a) thoroughly evaluated the potential breach with respect to the relevant model of Unidirectional Digital Cable Product, (b) consulted with Licensee regarding the problem, (c) given written notice to Licensee of CableLabs' intent to terminate the license with respect to such model of Unidirectional Digital Cable Product, and (d) provided Licensee with a reasonable opportunity to cure the breach (where such breach is capable of being cured) and such breach remains uncured for sixty days following the date of such notice, or, if such breach cannot by its nature be cured within such period, if Licensee has not commenced, and thereafter at all times diligently pursues, commercially reasonable efforts to cure as soon as possible thereafter. In circumstances where Licensee's failure subjects Controlled Content to an unreasonable risk of unauthorized copying, the maximum period for the activities in clauses (a), (b), (c) and (d) of the preceding sentence shall be forty-five days and the cure period under clause (d) of the preceding sentence shall be thirty days. Termination of the licenses granted for any specific model of Unidirectional Digital Cable Product shall not affect the licenses granted for any other model.

8.3 Termination of Agreement for Cause. CableLabs may terminate this Agreement in the event that CableLabs provides notice of Licensee's material breach of any representation, warranty or covenant set forth in Section 3.3, 5.1, 7.1 through 7.3 or 9.2 hereof and (where such breach is capable of being cured) such breach remains uncured sixty (60) days following the date of such notice.

8.4 Termination by Licensee. Licensee may terminate this Agreement at any time, upon sixty (60) days written notice to CableLabs.

8.5 Effect of Termination. Upon the termination of the licenses granted hereunder for any specific model of Unidirectional Digital Cable Product pursuant to Section 8.2, Licensee may no longer make, have made, use, sell, import or distribute such model of Unidirectional Digital Cable Product, nor use the DFAST Technology therewith except that, if the termination did not result from Licensee's failure to satisfy the requirements of the Robustness Rules, or the Compliance Rules, Licensee may sell or distribute any remaining Unidirectional Digital Cable Products in existence at the time of termination. Unless Licensee retains a license with respect to other models of Unidirectional Digital Cable Products hereunder, Licensee shall immediately return all copies of the DFAST Technology to CableLabs, or destroy all such copies to the reasonable satisfaction of CableLabs. Licenses properly granted to Licensee in conjunction with the sale or distribution of Unidirectional Digital Cable Products by Licensee pursuant to Section

3 prior to the date of termination shall remain in full force and effect. Upon any termination of this Agreement, Licensee shall return all tangible embodiments of Licensed Know-How in its possession to CableLabs. Unless otherwise stated herein, no termination of this Agreement, whether by CableLabs or by Licensee, or termination of any license granted hereunder shall relieve either party of any obligation or liability accrued hereunder prior to such termination, or rescind or give rise to any right to rescind anything done by either party prior to the time such termination becomes effective nor shall the survival provisions of Section 12.12 be affected by such termination.

9. REPRESENTATIONS AND WARRANTIES.

9.1 Representations and Warranties of CableLabs. CableLabs represents, warrants, covenants and agrees as follows:

(a) CableLabs owns all right and title to the DFAST Technology, or otherwise has the right to grant the license thereof, and to the best of CableLabs' knowledge, free of any claim or other encumbrance of any third party. None of the DFAST Technology is or ever has been declared invalid or unenforceable, or is the subject of a pending or threatened action for opposition, cancellation, declaration of invalidity, unenforceability or misappropriation or like claim, action or proceeding.

(b) Without investigation, CableLabs is not aware of any notice or claim, threatened or pending, that the use of the DFAST Technology in accordance with the terms of this Agreement infringes any third party's Intellectual Property Rights. Otherwise, the DFAST Technology is licensed on an "as is" basis.

(c) CableLabs has authorized the person who has signed this Agreement for CableLabs to execute and deliver this Agreement to Licensee on behalf of CableLabs.

(d) This Agreement constitutes a valid and binding obligation of CableLabs, enforceable according to its terms.

9.2 Representations and Warranties of Licensee. Licensee represents, warrants, covenants and agrees as follows:

(a) Licensee has authorized the person who has signed this Agreement for Licensee to execute and deliver this Agreement to Licensee on behalf of Licensee.

(b) This Agreement constitutes a valid and binding obligation of Licensee, enforceable according to its terms.

10. DISCLAIMERS; LIMITATION OF LIABILITY.

10.1 Disclaimers. Each party disclaims all other warranties, express or implied, including, but not limited to, (a) any warranty that the DFAST Technology does not infringe the

intellectual property rights of any other person or entity, (b) any warranty that any claims of the Licensed Patent are valid or enforceable, (c) any implied warranties of merchantability and fitness for a particular purpose, or (d) that the rights and licenses granted to Licensee hereunder comprise all the rights and licenses necessary or desirable to practice, develop, make or sell Unidirectional Digital Cable Products. The DFAST Technology and enhancements thereto, and any other items, deliverables, or information supplied by or on behalf of CableLabs are provided on an “as is” basis.

10.2. Limitation of Liability. Except as otherwise specifically limited by this Agreement, the parties shall have all rights available at law or in equity for any breach of this Agreement. In no event shall either party be liable to the other or to any Third-Party Beneficiary (as defined in Section 11) for consequential, incidental, special, indirect, punitive or exemplary damages of any kind, including without limitation loss of profit, savings or revenue, or the claims of third parties, whether or not advised of the possibility of such loss, however caused and on any theory of liability, arising out of this Agreement or based on the making, using, selling or importing any product that implements the DFAST Technology. In no event shall either party be liable to the other or to any Third-Party Beneficiary under any circumstances under this Agreement for any claims that, individually or in the aggregate with all other claims exceed the amount paid by Licensee to CableLabs pursuant to Section 5 herein. Notwithstanding the foregoing, the limitation of liability amount set forth above shall be replaced with a limitation of \$1,000,000 if the liability giving rise to the claim for damages arises out of Licensee’s willful and bad faith material breach of the Compliance Rules, the Robustness Rules, Section 2.2 or any provision of Section 7.1 through 7.3 regarding the security or integrity of the Licensed Know-How.

For purposes of this Agreement, a breach shall be “material” only if Licensee acted in a manner that is prohibited by this Agreement or failed to perform an obligation required under this Agreement, which act or failure has resulted in or would be likely to result in commercially significant harm to CableLabs or a Cable Operator, or constitutes a threat to the integrity or security of the DFAST Technology, or exposes Controlled Content to unauthorized copying. In addition, the following is a non-exclusive list of circumstances in which there is no material breach of the provisions of Sections 7.1 through 7.3: (1) if no Licensed Know-How was released to a third party not permitted hereunder to have such information or could reasonably have been expected to have been released to such third party as a result of the breach; (2) if Licensee maintains an internal program to assure compliance herewith (including a program to assure maintenance of inventory, samples, and confidentiality of information for purposes in addition to compliance with this Agreement), the breach was inadvertent or otherwise unintentional, and the breach did not have a material adverse effect on the integrity or security of the DFAST Technology; or (3) if Licensee brought the breach to CableLabs’ attention in a timely manner as required by this Agreement and such breach did not have a material adverse effect on the integrity or security of DFAST Technology.

11 THIRD-PARTY-BENEFICIARY RIGHTS.

11.1 Compliance of Licensee and other licensees with the terms hereof is essential to maintain the value, integrity, security and performance of the DFAST Technology and networks of Cable Operators. As part of the consideration granted herein, Licensee agrees that video programming providers that provide copyrighted works for transmission to Unidirectional Digital Cable Products and the copyright owners of such work (collectively, “**Content Providers**”) and Cable Operators (collectively, “**Third-Party Beneficiaries**”), shall each be a third-party beneficiary of this Agreement, but only with respect to their right to bring a claim or action against Licensee to seek injunctive relief against the manufacture, distribution, commercial use and sale of Licensee’s products that are in material breach of the Compliance Rules, the Robustness Rules or Section 2.2 of this Agreement, and for damages as provided in Section 11.2. In any such claim or action, reasonable attorneys’ fees shall be awarded to the prevailing party.

11.2 Such Third Party Beneficiaries may seek such actual damages (up to the aggregate limits contained in Section 10.2) only after (a) such Third Party Beneficiary has given to CableLabs written notice of the potential breach; (b) the potential for a cure at low cost at the headend for the relevant service has been evaluated as a reasonable alternative; (c) CableLabs has thoroughly evaluated the potential breach with respect to the relevant Unidirectional Digital Cable Product; (d) CableLabs has consulted with Licensee regarding the problem; (e) CableLabs has provided Licensee with a reasonable opportunity to cure the breach (where such breach is capable of being cured) and such breach remains uncured for sixty (60) days following the date of such notice, or, if such breach cannot by its nature be cured within such period, if Licensee has not commenced, and thereafter at all times diligently pursued, commercially reasonable efforts to cure as soon as possible thereafter; and (f) CableLabs has used reasonable efforts to inform all Cable Operators of such breach. Third Party Beneficiaries may seek injunctive relief only after providing CableLabs and the Licensee with notice and consultation reasonable under the circumstances with respect to such third party claim. Claims and actions under this Section 11.2 shall be made only for material breaches (as defined in Section 10.2).

12. MISCELLANEOUS

12.1 Independent Contractors. The relationship established between the parties by this Agreement is that of independent contractors. Nothing in this Agreement shall be construed to constitute the parties as partners, joint venturers, co-owners, franchisers or otherwise as participants in a joint or common undertaking for any purpose whatsoever.

12.2 No Trademark Rights Granted. Nothing contained in this Agreement shall be construed as conferring any right to use in advertising, publicity, or other promotional activities any name, trade name, trademark or other designation of either party hereto (including any contraction, abbreviation or simulation of any of the foregoing).

12.3 No Patent Solicitation Required. Except as expressly provided herein, neither party shall be required hereunder to file any patent application, secure any patent or patent rights,

provide copies of patent applications to the other party or disclose any inventions described or claimed in such patent applications.

12.4 Law and Jurisdiction. THIS AGREEMENT SHALL BE CONSTRUED, AND THE LEGAL RELATIONS BETWEEN THE PARTIES HERETO SHALL BE DETERMINED, IN ACCORDANCE WITH THE LAW OF THE STATE OF NEW YORK, UNITED STATES OF AMERICA, WITHOUT REGARD TO ITS CONFLICT OF LAWS RULES.

(a) IN CONNECTION WITH ANY LITIGATION BETWEEN THE PARTIES HERETO OR IN CONNECTION WITH ANY THIRD-PARTY-BENEFICIARY CLAIM BROUGHT HEREUNDER ARISING OUT OF OR RELATING TO THIS AGREEMENT, EACH PARTY IRREVOCABLY CONSENTS TO: (i) THE EXCLUSIVE JURISDICTION AND VENUE IN THE FEDERAL AND STATE COURTS LOCATED IN THE COUNTY OF NEW YORK, NEW YORK, AND (ii) THE SERVICE OF PROCESS OF SAID COURTS IN ANY MATTER RELATING TO THIS AGREEMENT BY PERSONAL DELIVERY OR BY MAILING OF PROCESS BY REGISTERED OR CERTIFIED MAIL, POSTAGE PREPAID, AT THE ADDRESSES SPECIFIED IN THIS AGREEMENT, OR TO THE AGENT TO BE APPOINTED PURSUANT TO THE SECTION, BELOW.

(b) IF LICENSEE DOES NOT HAVE A PRINCIPAL PLACE OF BUSINESS IN THE UNITED STATES, LICENSEE SHALL APPOINT AGENTS IN THE STATE OF NEW YORK FOR ACCEPTANCE OF SERVICE OF PROCESS PROVIDED FOR UNDER THIS AGREEMENT AND SHALL NOTIFY CABLELABS OF THE IDENTITY AND ADDRESS OF SUCH AGENT WITHIN THIRTY (30) DAYS AFTER THE EFFECTIVE DATE.

(c) LICENSEE WAIVES ANY OBJECTION TO THE JURISDICTION, PROCESS, AND VENUE OF ANY SUCH COURT, AND TO THE EFFECTIVENESS, EXECUTION, AND ENFORCEMENT OF ANY ORDER OR JUDGMENT (INCLUDING, BUT NOT LIMITED TO, A DEFAULT JUDGMENT) OF SUCH COURT PERTAINING TO THIS AGREEMENT, TO THE MAXIMUM EXTENT PERMITTED BY THE LAW OF THE PLACE WHERE ENFORCEMENT OR EXECUTION OF ANY SUCH ORDER OR JUDGMENT MAY BE SOUGHT AND BY THE LAW OF ANY PLACE WHOSE LAW MIGHT BE CLAIMED TO BE APPLICABLE REGARDING THE EFFECTIVENESS, ENFORCEMENT, OR EXECUTION OF SUCH ORDER OR JUDGMENT, INCLUDING PLACES OUTSIDE OF THE STATE OF NEW YORK AND OF THE UNITED STATES.

12.5 Compliance with Laws. In connection with this Agreement, each party shall comply with all applicable regulations and laws, including export, re-export and foreign policy controls and restrictions that may be imposed by any government. Each party shall require its customers to assume an equivalent obligation with regard to import and export controls.

12.6 No Assignment. Licensee shall not assign any of its rights or privileges under this Agreement without the prior written consent of CableLabs, such consent not to be unreasonably withheld or delayed. No consent shall be required for the assignment of this Agreement to any wholly-owned subsidiary of Licensee or for the assignment in connection with

the merger or the sale of Licensee or Licensee's business unit provided that Licensee shall remain liable for its obligations hereunder. Any attempted assignment or grant in derogation of the foregoing shall be void.

12.7 Notice. Any notices required or permitted to be made or given to either party pursuant to this Agreement shall be in writing and shall be delivered as follows with notice deemed given as indicated: (a) by personal delivery when delivered personally; (b) by overnight courier upon written notification of receipt; (c) by telecopy or facsimile transmission upon acknowledgment of receipt of electronic transmission; or (d) by certified or registered mail, return receipt requested, five days after deposit in the mail. All notices must be sent to the address set forth below, or to such other address as the receiving party may have designated by written notice given to the other party:

(a) for **CableLabs**,
Attention: General Counsel
858 Coal Creek Circle,
Louisville, CO 80027-9750
fax: 303/661-9199; and

(b) for **Licensee**,

Attention: _____
fax: _____

12.8 Amendments. No amendment or modification hereof shall be valid or binding upon the parties unless made in writing and signed by both parties.

12.9 Waiver. Any waiver by either party of any breach of this Agreement shall not constitute a waiver of any subsequent or other breach.

12.10 Severability. If any provision or provisions of this Agreement shall be held to be invalid, illegal or unenforceable, the validity, legality and enforceability of the remaining provisions shall not be in any way affected or impaired thereby.

12.11 Headings. The headings of the several sections of this Agreement are for convenience of reference only and are not intended to be a part of or to affect the meaning or interpretation of this Agreement.

12.12 Survival. The following sections of the Agreement shall survive any termination of the Agreement: Sections 2.2, 3.4, 5.2, 7.1, 7.2, 7.3, 10.1, 10.2, 11.1, 11.2 and 12.12.

12.13 Most Favored Status. CableLabs shall make available to Licensee any license terms made available to any or all manufacturers of Unidirectional Digital Cable Products

pursuant to the DFAST Technology License Agreement for Unidirectional Digital Cable Products. CableLabs also commits that the benefit of any modifications, clarifications or interpretations of language, made by CableLabs or mandated by applicable governmental or judicial authority, in a DFAST Technology License Agreement for Unidirectional Digital Cable Products shall be extended to Licensee in accordance with this Section 12.13. Where CableLabs agrees to make a change to a particular licensee’s DFAST Technology License Agreement for Unidirectional Digital Cable Products, Licensee may incorporate such change, or upgrade to such revised agreement in total, at any time. Where CableLabs has agreed to include language in a particular DFAST Technology License Agreement for Unidirectional Digital Cable Products that is more favorable than that in Licensee's DFAST Technology License Agreement for Unidirectional Digital Cable Products, CableLabs shall not enforce the language in this Agreement with respect to Licensee to the extent that such language is less favorable than that language found in such other licensee’s DFAST Technology License Agreement for Unidirectional Digital Cable Products. CableLabs shall upon the request of Licensee take reasonable steps to keep Licensee informed of any changes to the DFAST Technology License Agreement, and to provide Licensee with the most recent version. It is understood and agreed that PHILA sets forth a separate set of obligations that govern the relationship between the parties thereto, that this Agreement and the changes hereto shall not alter any provisions of any PHILA, and that changes to any PHILA shall not alter the provisions of this Agreement.

IN WITNESS WHEREOF, the parties hereto have caused this Agreement to be duly signed and to be effective as of the Effective Date above.

[Licensee]

Cable Television Laboratories, Inc.

Signature: _____

Signature: _____

Printed Name: _____

Printed Name: _____

Title: _____

Title: _____

List of Exhibits:

- Exhibit A Referenced Technology
- Exhibit A1 Constrained Image Trigger
- Exhibit B Compliance Rules
- Exhibit C Robustness Rules
- Exhibit C-1 Robustness Checklist

Exhibit A
Referenced Technology

A Unidirectional Digital Cable Product:

1. Shall include the POD interface, specified in SCTE 28 2001 as amended by DVS/519r2 (as of 11/05/02) and SCTE 41 2001 as amended by DVS/301r4 (as of 10/29/02) Support for IP flows is not required.
2. Shall include portions of EIA-818D and DVS 538 (as of 10/29/02) specifically addressing harm to the network as identified by DFAST Licensees and CableLabs.

Exhibit A1
Referenced Technology
(Constrained Image Trigger & Redistribution Control Trigger)

The Constrained Image Trigger is defined as noted below, or as adopted by SCTE in SCTE 41 in substantially the same form. The sections below present amendments to the noted sections in SCTE 41 2003:

2.4.1 COPY CONTROL INFORMATION

Copy control information (CCI) is passed from the Card to the Host across the data channel to inform the Host device of the level of copy protection required. The CCI is sent in the clear to the Host device, but the integrity of the information is maintained by authenticating the CCI using a simple protocol.

The one-byte CCI field contains information that the Host uses to control copying of content. Two EMI bits control copying on Host digital outputs, two APS bits control copying on analog outputs, one bit as a Constrained Image Trigger, one bit as a Redistribution Control Trigger, and ~~four~~ two bits are reserved.

4.3.5 CHANNEL CHANGE

When a channel change occurs, the Host shall treat all CP-scrambled content as if the EMI is set to "copy never", but shall not apply Image Constraint until the new CCI message is received. The Host shall immediately begin using the values of ~~EMI~~ the CCI when it is received from the Card. If a new CCI message is not received within 10 seconds, the Host shall apply Image Constraint as if the CIT bit was set to one, and redistribution control as if the RCT but was set to one. Channel change shall not cause a key refresh to occur.

6.1 CCI DEFINITION

CCI is a single byte, 8 bit, field conveyed from Card to Host. ~~Four~~ Six of the eight bits are defined. The remaining ~~four~~ two are reserved. The reserved bits shall be set to zero by the Card as shown in Table 6.1-A. The Host shall use the reserved bit values received from the Card only for execution of the Authenticated Tunnel Protocol described below. The Host shall ignore the reserved bit values thereafter.

Table 6-0-A CCI Bit Assignments

CCI Bits #	7	6	5	4	3	2	1	0
Card sets to	0	0	0 RCT	0 <u>CIT</u>	APS1	APS0	EMI1	EMI0
Host interprets as	rsvd	rsvd	rsvd RCT	rsvd <u>CIT</u>	APS1	APS0	EMI1	EMI0

6.1.1 EMI - DIGITAL COPY CONTROL BITS

The two LSB's of the CCI byte are the EMI bits. They shall control copy permissions for digital copies. The EMI bits shall be supplied to any Host digital output ports for control of copies made from those outputs. The EMI bits are defined in Table 6.1-B.

Table 6-0-B EMI Values and Content

EMI Value	Digital Copy Permission	Content Type
00	Copying not restricted	Not "High Value"
01	No further copying is permitted.	High Value
10	One generation copy is permitted.	High Value
11	Copying is prohibited.	High Value

6.1.2 APS - ANALOG PROTECTION SYSTEM

Bits 3 and 2 of CCI as shown in Table 6.1-A are the APS bits 1 and 0 respectively. The Host shall use the APS bits to control copy protection encoding of analog composite outputs as described in Table 6.1-C.

Table 6-0-C APS Value Definitions

APS	Description
00	Copy Protection Encoding Off
01	AGC Process On, Split Burst Off
10	AGC Process On, 2 Line Split Burst On
11	AGC Process On, 4 Line Split Burst On

6.1.3 CIT -CONSTRAINED IMAGE TRIGGER

Bit 4 of CCI as shown in Table 6.1-D is the CIT bit. The Host shall use the CIT bit to control Image Constraint of high definition analog component outputs.

Table 6-0-D CIT Values and Application

<u>CIT Value</u>	<u>Image Constraint Application</u>
<u>0</u>	<u>No Image Constraint asserted</u>
<u>1</u>	<u>Image Constraint required</u>

6.1.4 RCT – REDISTRIBUTION CONTROL TRIGGER

Bit 5 of CCI as shown in Table 6.1-D is the RCT bit. The Host shall use the RCT bit to trigger redistribution control on Controlled Content when the RCT value is set to a value of one (1) in combination with the EMI bits set to a value of zero, zero (0,0), which signals the need for redistribution control to be asserted on Controlled Content without the need to assert numeric copy control.

Table 6-0-D RCT Values and Application

<u>RCT Value</u>	<u>Redistribution Control Application</u>
<u>0</u>	<u>No Redistribution Control asserted</u>
<u>1</u>	<u>Redistribution Control required</u>

6.4.2 AUTHENTICATED TUNNEL PROTOCOL

Step 7 The Host calculates CCI_auth using the received CCI value and compares it with the CCI_auth value received from the Card. Failed equivalence generates an error condition and the Host sets EMI to 11 and applies Image Constraint as if the value were equal to 1, and redistribution control as if the RCT were equal to 1.

Exhibit B
Compliance Rules

See attached.

Exhibit C

Robustness Rules

See attached

Exhibit C-1

Robustness Checklist

See attached

EXHIBIT B

Compliance Rules

Host Devices, at the time of manufacture, must comply with the requirements set forth in this Exhibit C and be constructed so as to resist attempts at circumvention of these requirements as specified in Exhibit B, Robustness Rules. For purposes of this Exhibit C, “**at the time of manufacture**” shall have the meaning given in Section 11.2 of the Agreement.

Note: The terms of this Exhibit C do not apply with respect to Prototypes or Licensed Components.

1. Definitions

1.1 “**Consensus Watermark**” means a watermark that has been developed on a multi-industry basis pursuant to a broad consensus in an open, fair, voluntary process, and that has thereafter been identified in a notice by CableLabs to Licensee as the Consensus Watermark for purposes of this Agreement.

1.2 “**Constrained Image**” means the visual equivalent of not more than 520,000 Pixels per frame (e.g. an image with resolution of 540 vertical lines by 960 horizontal lines for a 16:9 aspect ratio). A Constrained Image can be output or displayed using video processing techniques such as line doubling or sharpening to improve the perceived quality of the image. A “**Constrained Image Trigger**” or “**CIT**” shall mean the field or bits, as described in the Specifications, used to trigger the output of a "Constrained Image" in the High Definition Analog Output of Unidirectional Digital Cable Products.

1.3 “**Constrained Image Trigger**” or “**CIT**” means the field or bits, as described in the Specifications, used to trigger the output of a "Constrained Image" in the High Definition Analog Output of Host Devices.

1.4 “**Digital Receiver Interface**” or “**DRI**” means a content transport and command and control protocol, implemented in accordance with an Issued DRI Specification, that can be applied on any digital bus, including but not limited to Ethernet, Wi-Fi, USB, and 1394.

1.5 “**DTCP**” means that method of encryption, decryption, key exchange and renewability that is described in the specification entitled “5C Digital Transmission Content Protection Release 1.0, as amended by DTLA from time to time, and reviewed by CableLabs.”

1.6 “**HDCP**” means that method of authentication, encryption, decryption, and renewability that is described in the specification entitled “High-Bandwidth Digital Content Protection System, Rev. 1.1” as supplemented (but not superseded) by the Specifications, as may be amended from time to time. In addition, “HDCP” shall include HDCP 2.0 methods as described in the “HDCP 2.0 WHDI Specification”, and the “HDCP Interface Independent Adaptation Specification” (“HDCP IIA”) but only for those HDCP IIA mappings where Digital Content Protection LLC (DCP) has provided CableLabs notice and opportunity to review such mappings.

1.7 “**High Definition Analog Form [or] Output**” means a format or output that is not digital, and has a resolution higher than Standard Definition Analog Form or Output.

1.8 “**RCD**” or “**Redistribution Control Descriptor**” means the field or bits as described in CEA-608-D.

1.9 “**RCT**” or “**Redistribution Control Information**” means the field or bits as described in CEA-805-D.

1.10 “**RCT**” or “**Redistribution Control Trigger**” means the field or bits, as described in the Specifications, used to trigger the Encryption Plus Non-assertion (“EPN”) state in DTCP protected digital outputs in the Certified Host Devices when the RCT value is set to a value of one (1) in combination with

the EMI bits set to a value of zero, zero (0,0), which signals the need for redistribution control to be asserted on Controlled Content without the need to assert numeric copy control.¹

1.11 **“Standard Definition Analog Form [or] Output”** means a format or output that is not digital, is NTSC RF, Composite, S-Video, YUV, Y,R-Y,B-Y or RGB and has no more than 483 interlace or progressive active scan lines.

1.12 **“VCPS”** means the Video Content Protection System for recording encrypted content on DVD+RW and DVD+R optical digital media protected by VCPS technology as defined in the Vidi System Description Version 1.0 dated March 2004 and the license terms governing the implementation of VCPS as provided in version 1.2 of the Video Content Protection System Agreement dated 1 September 2004, such terms including compliance with the Compliance and Robustness Rules herein.

1.13 **“CPDO”** means the secure digital recording method as specified by EnCentrus Systems, Inc. in its document entitled EnCentrus Content Protected Digital Output Port System Description; Revision 1.2 dated January 2006, such terms including compliance with the Compliance and Robustness Rules herein.

1.14 **“IPRM”** means the Motorola IPRM System Submission of New Digital Outputs and Content Protection Technologies; Revision 2.7 dated November 10, 2006, as amended, and the applicable license terms governing the implementation of IPRM as provided by Motorola, such terms including compliance with the Compliance and Robustness Rules herein.

1.15 **“Marlin”** means the Marlin digital rights management (DRM) system as defined at marlin-community.com, and documented and provided to CableLabs by the Marlin Trust Management Organization (MTMO) as of 1 July 2013.

1.16 **“PlayReady”** means the Microsoft PlayReady digital rights management (DRM) system as documented and provided to CableLabs by Microsoft, and updated as of 1 August 2013.

1.17 **“RPSP”** means the secure digital recording method as specified by Samsung in its RPSP Specification and associated license agreement available from Samsung dated 14 January 2010, such terms including compliance with the Compliance and Robustness Rules herein.

1.18 **“TivoGuard for Streaming”** means the streaming-only (non-copying) technology specified by Tivo in documents submitted to CableLabs up to May 19, 2011 (including addendums specified and agreed by Tivo), and associated license agreement available from Tivo, such terms including compliance with the Compliance and Robustness Rules herein.

1.19 **“TivoGuard for Mobile Devices”** means the copy protection technology specified by Tivo in documents submitted to CableLabs up to September 30, 2014 (including addendums specified and agreed by Tivo), and associated license agreement available from Tivo, such terms including compliance with the Compliance and Robustness Rules herein.

2. Outputs

2.1 **General.** Host Devices shall not output content, or pass content received through the Service to any output, except as permitted in this Section 2 and otherwise allowed by the tru2way Middleware application. For purposes of this Exhibit, an output shall be deemed to include, but not be limited to, any transmissions to any internal copying, recording, or storage device, but shall not include internal non-persistent or transitory transmissions that otherwise satisfy these Compliance Rules and the Robustness Rules. For the purposes of this Exhibit C, the RCD bit as defined in CEA-608-C and the RCI

¹ RCT may not be set to restrict redistribution except in content that could lawfully be marked Copy One Generation or Copy Never but is instead encoded or directed to be encoded “EPN”, and such encoding is otherwise in accordance with the DTCP license agreement. The effective date for Licensed Products to detect and honor the RCT shall be July 1, 2009.

as defined in CEA-805-B shall be set to “1” if the Redistribution Control Trigger bit is set to a value of one (1) in combination with the EMI bits set to a value of zero, zero (0,0).

2.2 Standard Definition Analog Outputs. Host Devices with any Standard Definition Analog Outputs shall only output content received through the Service, or pass content received through the Service as permitted by this Section 2.2:

2.2.1 In any transmission through an NTSC RF, Composite, Y,R-Y,B-Y, or RGB format analog output (including an S-video output and including transmissions to any internal copying, recording or storage device) of a signal, Host Devices shall generate copy control signals in response to the instructions provided in the APS bits of the Copy Control Instruction message, if any, and in accordance with the Specifications (i.e. trigger bits for Automatic Gain Control and Colorstripe copy control systems, as referenced below). The technologies that satisfy this condition and are authorized hereunder are limited to the following:

(1) For NTSC analog outputs (including RF, Composite or S-Video), the specifications for the Automatic Gain Control and Colorstripe copy control systems (contained in the document entitled “Specifications of the Macrovision Copy Protection Process for STB/IRD Products” Revision 7.1.S1, October 1, 1999);

(2) For 480i (interlace scan), YUV or Y, R-Y, B-Y outputs, the appropriate specifications for the Automatic Gain Control copy control system, as identified in the Specifications;

(3) For 480p progressive scan outputs, the appropriate specification for the Automatic Gain Control copy control system, as identified in the Specifications.

(4) Except as provided in Section 2.2.2 for Standard Definition Analog outputs not specified above, or as provided in Section 2.3, Host Devices shall not transmit content through such analog outputs until such time as this Exhibit is amended to permit same.

All Host Devices shall generate and propagate CGMS-A signals for all SD analog outputs; but shall not be required to respect the CGMS-A trigger unless required by appropriate legislation or regulation.

2.2.2 VGA. A Host Device may output content, or pass content through a VGA interface to a monitor, in Standard Definition Analog Form, in Host Devices manufactured prior to December 31, 2005. As used herein, “VGA” means a Video Graphics Array display system, typically implemented as a computer video output, that is 640 x 480 pixels.

2.3 High Definition Analog Outputs. Host Devices with any High Definition Analog Outputs shall only output content received through the Service or pass content received through the Service as permitted by this section 2.3.

2.3.1 Host Device shall be able to constrain, when required by the CIT CCI bit, the resolution of content that is High Definition to be output through a connection capable of transmitting content in High Definition Analog Form, to a Constrained Image.

2.3.2 Host Device shall include one or more approved Digital Outputs as specified in Section 2.4 below.

2.3.3 All Host Devices shall generate and propagate CGMS-A signals for all HD analog outputs; but shall not be required to respect the CGMS-A trigger unless required by appropriate legislation or regulation.

2.4 Digital Outputs. Host Device with any digital outputs shall only output content received through the Service, or pass content received through the Service as permitted by this section 2.4.

2.4.1 **1394 with DTCP.** Host Device may output Controlled Content, and pass Controlled Content to an output, in digital form over IEEE 1394 interfaces as specified by the Specifications, where such output is protected by DTCP. Host Device must support

DTCP “Full Authentication,” and may additionally support DTCP “Restricted Authentication.” When so outputting or passing such content to a DTCP-1394 output, the DTCP Source Function shall correctly map the copy control information (CCI) to the DTCP Encryption Mode Indicator (EMI), DTCP Analog Protection System (APS) signaling, DTCP Image Constraint Token (ICT), and DTCP Encryption Plus Non-assertion (EPN) signaling in accordance with the Specifications. Capitalized terms used in this Section, but not otherwise defined in this Exhibit C or the Agreement, shall have the meaning set forth in the DTCP Specification or the DTCP Adopter Agreement.

- 2.4.2 **DVI, HDMI, DisplayPort, or HDCP IIA interfaces, with HDCP.** Host Devices may output content received through the Service, and pass content received through the Service to an output, in digital form over DVI, HDMI, or DisplayPort interfaces, and such other HDCP 2.0 IIA interface mappings (collectively “HDCP Interfaces”) as specified by the HDCP specifications, and where the output always has HDCP active and on. When so outputting or passing such content to the HDCP Interfaces output, the HDCP Source Function shall pass content received through the Service to such output in digital form only when it has securely verified that the HDCP Source Function has signaled that it is engaged and able to deliver protected content, which means (i) HDCP protection is operational and always active on all HDCP Interfaces outputs; and (ii) there is no HDCP device on such output whose Key Selection Vector is in a SRM. Capitalized terms used in this Section, but not otherwise defined in this Exhibit C or the Agreement, shall have the meaning set forth in the documents identified in the definition of “HDCP” above.
- 2.4.3 **DTCP-IP.** Host Devices, including the OCUR, may output Controlled Content, and pass Controlled Content to an output in digital form where such output is protected by DTCP-IP. When so outputting or passing such content to a DTCP-IP output, the DTCP Source Function shall map the copy control information (CCI) to the DTCP Encryption Mode Indicator (EMI), DTCP Analog Protection System (APS) signaling, DTCP Image Constraint Token (ICT), and DTCP Encryption Plus Non-assertion (EPN) signaling in accordance with the Specifications. Capitalized terms used in this Section, but not otherwise defined in this Exhibit C or the Agreement, shall have the meaning set forth in the DTCP Specification or the DTCP Adopter Agreement.
- 2.4.4 **IPRM.** Host Devices may output Controlled Content, and pass Controlled Content to an output in digital form where such output and content is protected by IP Rights Management (IPRM) system.
- 2.4.5 **Microsoft PlayReady.** Host Devices may output Controlled Content, and pass Controlled Content to an output in digital form where such output and content is protected by Microsoft PlayReady.
- 2.4.6 **Marlin.** Host Devices may output Controlled Content, and pass Controlled Content to an output in digital form where such output and content is protected by Marlin.
- 2.4.7 **DRI with an Approved DRM.** Host Devices that conform to the OCUR Specification may output content, and pass content, in digital form over the DRI. One or more of the approved Digital Rights Management (DRM) systems listed in this Section 2.4.5 must be included in the OCUR implementation. Approved DRMs, and limitations, include the following DRMs, as amended by CableLabs from time to time:
- 2.4.5.1 **Microsoft PlayReady.** Content may be output over the DRI protected by Microsoft PlayReady in accordance with the DRI Content Protection Requirements set forth in the OCUR Specification, where connected to a device that runs Microsoft Windows 7, or later versions, and such device complies with the Redacted Agreement between Microsoft and CableLabs dated Dec 12, 2005.

2.4.5.2 **Real Helix DRM.** Content may be output over the DRI protected by Real Helix DRM in accordance with the DRI Content Protection Requirements set forth in the OCUR Specification, where connected to a device that runs Microsoft Windows Media Center Edition (a “MCE HMS”) and such MCE HMS complies with (1) the OEM Compliance Letter between CableLabs and the MCE HMS manufacturer, such compliant devices posted at www.opencable.com, (2) the Redacted Agreement between RealNetworks and CableLabs dated April 6, 2006; and (3) the Redacted Agreement between Microsoft and CableLabs dated Dec 12, 2005.

2.4.5.3 **DTCP-IP.** Host Devices may output Controlled Content, and pass Controlled Content to an output in digital form where such output is protected by DTCP-IP. When so outputting or passing such content to a DTCP-IP output, the DTCP Source Function shall map the copy control information (CCI) to the DTCP Encryption Mode Indicator (EMI), DTCP Analog Protection System (APS) signaling, DTCP Image Constraint Token (ICT), and DTCP Encryption Plus Non-assertion (EPN) signaling in accordance with the Specifications. Capitalized terms used in this Section, but not otherwise defined in this Exhibit C or the Agreement, shall have the meaning set forth in the DTCP Specification or the DTCP Adopter Agreement.

2.4.5.4 **Marlin.** Host Devices may output Controlled Content, and pass Controlled Content to an output in digital form where such output and content is protected by Marlin.

2.4.6 Non-Controlled Content. Host Devices may output content received through the Service, which is not Controlled Content, through digital outputs other than the outputs listed above.

2.4.7 New Digital Outputs. CableLabs shall approve or disapprove digital outputs and/or content protection technologies (or “delist” an approved technology) on a reasonable and nondiscriminatory basis within 180 days of submission by an Adopter of a request and all information necessary to evaluate such request. In the event of disapproval or delisting, CableLabs will indicate in writing the specific reasons for its action. CableLabs shall not withhold approval of any such output or content protection technology that provides effective protection to Controlled Content against unauthorized interception, retransmission or copying. In making that determination, CableLabs shall take into account (a) the effectiveness of the technology; (b) the license terms governing the secure implementation of the technology; and (c) other objective criteria. In the event that CableLabs disapproves or fails to act within the time specified above, an Adopter may petition the Federal Communications Commission concerning such denial, lack of approval, or delisting. The parties anticipate that the FCC shall determine in an expedited 90-day proceeding whether the proposed digital output and/or content protection technology provides effective protection to Controlled Content against unauthorized interception, retransmission or copying, taking into account, among other things, the factors utilized by CableLabs. CableLabs agrees to be bound by a final order of the FCC. Notwithstanding the foregoing, in the event that CableLabs is advised that four (4) member studios of the Motion Picture Association approve a digital output or content protection technology that provides effective protection to Controlled Content against unauthorized interception, retransmission or copying, such output or content protection technology shall be deemed approved by CableLabs pursuant to this Agreement, and upon receipt of notice by CableLabs of such approval by the four studios, CableLabs shall amend these Compliance Rules to include such output and/or content protection technology.

2.5 SRM. When outputting or passing content through any output, Host Devices shall process and carry all valid System Renewability Messages (“SRMs”) received via method specified in ATSC A/98. In the case of DTCP, the Host Device shall process and pass to the DTCP Source Function the DTCP SRM. Likewise, in the case of HDCP, the Host Device shall process and pass to the HDCP Source Function the HDCP SRM.

2.6 Watermark Non-Interference. Commencing eighteen months after the existence of a Consensus Watermark, Licensee shall, when selecting among technological implementations for product features for Host Devices and Licensed Components designed after such date, take commercially reasonable care (taking into consideration the technical characteristics, costs of implementation, commercial terms and conditions, and impact on Controlled Content and the effectiveness or visibility of the Consensus Watermark) that Host Devices and Licensed Components do not strip, obscure or interfere with such Consensus Watermark in Controlled Content that has been decrypted; (ii) shall not design or produce Host Devices or Licensed Components the primary purpose of which is stripping, obscuring or interfering with such Consensus Watermark in Controlled Content that has been decrypted; and (iii) shall not knowingly market or distribute or knowingly cooperate in marketing or distributing Host Devices or Licensed Components the primary purpose of which is stripping, obscuring or interfering with such Consensus Watermark in Controlled Content that has been decrypted.

Provided Licensee complies with the foregoing provisions of this Section 2.6, this Section 2.6 shall not prohibit a Host Device or Licensed Component from incorporating legitimate features (i.e., zooming, scaling, cropping, picture-in-picture, compression, recompression, image overlays, overlap of windows in a graphical user interface, audio mixing and equalization, video mixing and keying, downsampling, upsampling, and line doubling, or conversion between widely-used formats for the transport, processing and display of audiovisual signals or data, such as between analog and digital formats and between PAL and NTSC or RGB and Y,Pb,Pr formats, as well as other features as may be added to the foregoing list from time to time by CableLabs by amendment to these Compliance Rules) that are not prohibited by law, and such features shall not be deemed to strip, interfere with or obscure the Consensus Watermark in Controlled Content.

3 Copying, Recording, and Storage of Controlled Content

- 3.1 **General.** Host Devices, including, without limitation, Host Devices with inherent or integrated copying, recording or storage capability shall not copy, record, or store Controlled Content, except as permitted in this section.
- 3.2 **Mere Buffer for Display.** Host Devices may store Controlled Content temporarily for the sole purpose of enabling the immediate display of Controlled Content, provided that (a) such storage does not persist after the content has been displayed, and (b) the data is not stored in a way that supports copying, recording, or storage of such data for other purposes.
- 3.3 **Copy No More.** Host Devices shall not copy, record or store Controlled Content that is designated in the EMI bits as having been copied but not to be copied further (“copy no more”), except as permitted in section 3.2 or 3.5.2.
- 3.4 **Copy Never.** Host Devices, including, without limitation, such a device with integrated recording capability such as a so-called “personal video recorder,” shall not copy Controlled Content that is designated in the EMI bits as never to be copied (“copy never”) except as permitted in section 3.2 or by the following:
 - 3.4.1 Such a device may internally store such content, including for the purpose of pausing the program, when instructed by OCAP if the stored content is securely bound to the Host Device doing the recording so that it is not removable therefrom and is not itself subject to further temporary or other recording within the Host Device before it is rendered unusable; provided the device is made in compliance with specified robustness requirements to avoid circumvention of such restrictions. When internally storing such content, including for the purpose of implementing pause, as allowed in this section, the content shall be stored in a manner which is encrypted in a manner that provides no less security than 128-bit Advanced Encryption Standard (“AES”) or 112-bit triple DES.

Host Devices shall be designed and manufactured to be able, when required by the OCAP application, to obliterate the stored content or render unusable the stored content after a stated period of time (as

identified by the OCAP application), on a frame-by-frame, minute-by-minute, megabyte-by-megabyte basis.

3.5 Copy One Generation.

3.5.1 **Copy.** Host Devices may make a copy of Controlled Content that is designated in the EMI bits as permissible to be copied for one generation (“Copy One Generation”), as provided in section 3.2 or the first sentence of 3.4.1 or provided that the copy (a) is scrambled, encrypted or uniquely bound to that device, in each case using a form of copy protection that is identified by an amendment to this section 3.5, if any, and (b) is remarked as not to be further copied (“copy no more”) in a manner that is set forth in section 3.5 or 3.6, and will be effective to prevent such further copies being made by devices capable of receiving a transmission of such remarked data through the outputs identified in sections 2.4 or 3.5.3. In the absence of either such amendment to this section 3.5, no copy of such Controlled Content other than as permitted in sections 3.2, the first sentence of 3.4.1, or 3.6, may be made.

3.5.2 **Move.** A Host Device that makes a copy of content marked in the CCI as “Copy One Generation” in accordance with this Section 3.5 may move such content to a single removable recording medium, or to a single external recording device, only when (a) the external recording device indicates that it is authorized to perform this Move function in accordance with the requirements of this Section, and to copy such Controlled Content in accordance with the requirements of this Section 3.5; (b) such Controlled Content is marked for transmission by the originating Host Device as “Copy One Generation”; (c) the Controlled Content is output over a protected output in accordance with Sections 2.2, 2.3, 2.4 or 3.5.3 of this Exhibit C; (d) before the Move is completed, the originating Host Device recording is rendered non-useable and the moved Controlled Content is marked “Copy No More” (e) the device to which the removable recording medium is moved is unable or rendered unable to output the Controlled Content except through outputs authorized by these Compliance Rules; and (f) the copy is stored (i) using an encryption protocol approved by CableLabs herein which uniquely associates such copy with a single device so that it cannot be played on another device or, if stored to removable media, so that no further usable copies may be made thereof or (ii) otherwise using methods referenced in Section 3.5.1. Multiple moves consistent with these requirements are not prohibited.

3.5.3 Approved Methods under Section 3.5 (Copy One Generation)

3.5.3.1 **VCPS.** In accordance with Section 3.5, Host Devices may make a copy of Controlled Content that is designated as Copy One Generation, provided such copy is protected using VCPS.

3.5.3.2 **CPDO.** In accordance with Section 3.5, Host Devices may make a copy of Controlled Content that is designated as Copy One Generation, provided such copy is protected using CPDO.

3.5.3.3 **RPSP.** In accordance with Section 3.5, Host Devices may make a copy of Controlled Content that is designated as Copy One Generation or Redistribution Control, provided such copy is protected using RPSP.

3.5.3.4 **TivoGuard In-Home Streaming.** In accordance with Section 3.5, Host Devices may stream (non-copying, notwithstanding section 3.5.1) Controlled Content that is designated as Copy One Generation, provided such Controlled Content is protected using TivoGuard and such Controlled Content is streamed from Tivo Series 4 (and subsequent series) devices to other devices within the subscriber’s home network as defined in the TivoGuard for Streaming submission.

3.5.3.5 TivoGuard Copying. In accordance with Section 3.5, Tivo Series 4 Host Devices (and subsequent series) may make a copy of Controlled Content that is designated as Copy One Generation and provide such Controlled Content to Apple iOS mobile devices (e.g., iPad) or Android 4.2 (and subsequent series) devices (collectively, “TivoGuard Approved Mobile Devices”), provided such Controlled Content is protected using the content protection technology as defined in the TivoGuard for Mobile Devices submission. Further, such TivoGuard Approved Mobile Devices may include any of the following secure digital outputs: Apple AirPort, and HDMI with HDCP 2.0 (and subsequent series).

3.6 User Accessible Bus. A Host Device may use a user accessible digital interface to store Controlled Content on a storage device, if: (a) the Controlled Content is encrypted across the interface, and in storage, with an encryption algorithm that provides no less security than 128-bit Advanced Encryption Standard (“AES”) or 112-bit Triple DES Encryption Algorithm (“3DES”); (b) the Controlled Content is uniquely cryptographically associated with (i) the original Host Device, or (ii) the storage device itself, such that Controlled Content is unusable to any other product or device; (c) the interface and storage device, or the system architecture, provides protection from a "disk cloning attack"²; (d) no key information is stored on the storage device unless encrypted with security no less than AES (128 bit) or 3DES (112 bit); and (e) the move, storage and copying of Controlled Content otherwise meets the criteria set forth in the Robustness Rules and the Compliance Rules.

3.7 No Waiver. Licensee acknowledges that the provisions of this section 3 are not a waiver or license of any copyright interest or an admission of the existence or non-existence of a copyright interest.

² A “disk cloning attack” is characterized by the following example:

- A first licensed product (Host-1) correctly stores "Copy one generation" content on a hard drive (HD-1).
- A bit-for-bit copy (a "clone") of HD-1 is made (in violation of this license and federal copyright law) on a second hard drive (HD-Clone).
- Content on HD-1 is then “moved” to a second licensed product (Host-2, having HD-2) in accordance with CHILA Compliance Rules, and the content is correctly obliterated from HD-1.
- HD-1 in Host-1 is now replaced with HD-Clone, resulting in two usable copies (one on Host-1 with HD-Clone, and a second on Host-2 with HD-2).
- Further unauthorized copies may be made similarly by making multiple clone disks.

Examples of techniques used to prevent a disk cloning attacks include:

- Device maintains a database of stored content and associated usage rules, in the example above, even if a clone is made, this database would prevent the unauthorized copy being used.
- The content is not stored in entirety on one disk, content is stored scattered on two or more disks, thus a clone of one disk alone is not sufficient.
- Stored content is frequently time-stamped, and any content that has a time stamp older than the most recent time stamp is not permitted to be used.

Exhibit C

Robustness Rules

Note: The terms of this Exhibit B do not apply with respect to Prototypes or Licensed Components.

1. Construction.

1.1 Generally. Host Devices as shipped shall meet the Compliance Rules and shall be designed and manufactured in a manner to effectively frustrate attempts to modify such Host Device to defeat the Compliance Rules or functions of the Specifications.

1.2 Defeating Functions. Host Devices shall not include:

(a) switches, buttons, jumpers, specific traces that can be cut or place the Host Device in a test mode, or software equivalents of any of the foregoing; or

(b) active JTAG ports, emulator interfaces or test points to probe security functions;
or

(c) service menus or functions (including remote-control functions);

in each case by which the Licensed Technology, content protection technologies, analog protection systems, Reprotection, CGMS-A/RCI/APS signaling, output restrictions, recording limitations, or other mandatory provisions of the Specifications or the Compliance Rules can be defeated or by which Controlled Content can be exposed to unauthorized access, copying, redistribution, or modification of usage rights. For the purpose of this exhibit, "Reprotection" shall mean the application of an approved, protection technology, when required, to Controlled Content received from a CableCARD that is to be output from the Host Device, and the integrity of the system and methods by which such application is assured.

1.3 Keep Secrets. Host Devices shall be designed and manufactured in a manner to effectively frustrate attempts to discover or reveal (a) the unique number, of a specified bit length, assigned to each Host Device, or the numbers used in the process for encryption or decryption of Controlled Content (collectively, "**Keys**") and (b) the methods and cryptographic algorithms used to generate such Keys.

2.0 Documents and Robustness Certification Checklist.

Before releasing any Host Device for commercial use, Licensee must perform tests and analyses to assure compliance with this Exhibit B. A Robustness Certification Checklist is attached as Exhibit B-1 for the purpose of assisting Licensee in performing tests covering certain important aspects of this Exhibit B. Inasmuch as the Robustness Certification Checklist does not address all elements required for the manufacture of a compliant product, Licensee is strongly advised to review carefully the Specifications, the Digital Certificate authorization Agreement, the Compliance Rules and this Exhibit B so as to evaluate thoroughly both its, testing procedures and the compliance of its Host Device.

3.0 Controlled Content Paths. Content shall not be available on outputs other than those specified in the Compliance Rules, and, within such Host Device, Controlled Content shall not be present on any user accessible buses (as defined below) in non-encrypted form (compressed or uncompressed). Similarly unencrypted Keys used to support any content encryption and/or decryption in the Host Device's data shall not be present on any user accessible buses. Notwithstanding the foregoing, compressed audio data shall be output to an external Dolby Digital decoder in the clear via the S/PDIF connector. This section shall not apply to navigation data contained in the Program Association Tables (PAT) or the Program Map Tables (PMT). A "user accessible bus" means a data bus which is designed for end user upgrades or access such as PCI that has sockets or is otherwise user accessible, SmartCard,

PCMCIA, or Cardbus, but not memory buses, CPU buses and similar portions of a device's internal architecture.

Host Devices shall not allow Controlled Content on any internal interface unless secured from unauthorized interception to the level of protection specified in Section 4(e)(i). An "internal interface" means any internal interconnection not defined above as a User Accessible Bus and includes, but is not limited to any signal on a chip bonding pad, JTAG, or other testing point (any place signals move onto and off of a silicon die).

Host Devices shall not allow Keys used to support any content encryption and/or decryption to be present on any User Accessible Bus or on any internal interface unless encrypted and secured from unauthorized interception to the level of protection specified in Section 4(e)(i) and (ii).

4.0 Methods of Making Functions Robust. Host Devices shall use at least the following techniques to make robust the functions and protections specified in this Agreement:

(a) **Distributed Functions.** The portions of the Host Device that perform authentication and decryption and the MPEG (or similar) decoder shall be designed and manufactured in a manner associated and otherwise integrated with each other such that Controlled Content in any usable form flowing between these portions of the Host Device shall be secure to the level of protection described in Section 4(e) below from being intercepted or copied.

(b) **Software.** Any portion of the Host Device that implements a part of the Specifications in software shall include all of the characteristics set forth in Sections 1 and 2 of this Exhibit B. For the purposes of this Exhibit B, "Software" shall mean the implementation of the functions as to which this Agreement requires a Host Device to be compliant through any computer program code consisting of instructions or data, other than such instructions or data that are included in Hardware. Such implementations shall:

- (i) Comply with Section 1.3 by any reasonable method including but not 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 in software, using effective techniques of obfuscation to disguise and hamper attempts to discover the approaches used;
- (ii) Be designed to perform self-checking of the integrity of its component parts such that unauthorized modifications will be expected to result in a failure of the implementation to provide the authorized authentication and/or decryption function. For the purpose of this provision, a "modification" includes any change in, or disturbance or invasion of features or characteristics, or interruption of processing, relevant to Sections 1 and 2 of this Exhibit B. This provision requires at a minimum the use of code with a cyclic redundancy check that is further encrypted with a private key or a secure hashing algorithm;
- (iii) Meet the level of protection outlined in Section 4(e) below.

(c) **Hardware.** Any portion of the Host Device that implements a part of the Specifications in hardware shall include all of the characteristics set forth in Sections 1 and 2 of this Exhibit B. For the purposes of these Robustness Rules, "Hardware" shall mean a physical device, including a component, that implements any of the content protection requirements as to which this Agreement requires that a Host Device be compliant and that (i) does not include instructions or data other than such instructions or data that are permanently embedded in such device or component; or (ii) includes instructions or data that are not permanently embedded in such device or component where such instructions or data have been customized for such Host Device or Licensed Component and such instructions or data are not accessible to the end user through the Host Device or Licensed Component. Such implementations shall:

- (i) Comply with Section 1.3 by any reasonable method including but not limited to: embedding Keys, Key generation methods and the cryptographic algorithms in silicon circuitry or firmware that cannot reasonably be read, or the techniques described above for software;
- (ii) Be designed such that attempts to reprogram, remove or replace hardware elements in a way that would compromise the security or content protection features of Licensed Technology, CableLabs Technology, the Agreement or in Host Devices would pose a serious risk of damaging the Host Device so that it would no longer be able to receive, decrypt or decode Controlled Content. By way of example, a component which is soldered rather than socketed may be appropriate for this means;
- (iii) Meet the level of protection outlined in Section 4(e) below.

For purposes of these Robustness Rules, “hardware” shall mean a physical device, including a component, that implements any of the content protection requirements as to which this Agreement requires that a Host Device be compliant and that (x) does not include instructions or data other than such instructions or data that are permanently embedded in such device or component; or (y) includes instructions or data that are not permanently embedded in such device or component where such instructions or data have been customized for such Host Device or Licensed Component and such instructions or data are not accessible to the end user through the Host Device or Licensed Component.

(d) Hybrid. The interfaces between hardware and software portions of a Host Device shall be designed so that they provide a similar level of protection which would be provided by a purely hardware or purely software implementation as described above.

(e) Level of Protection. The core encryption functions of the Specifications (maintaining the confidentiality of Keys, Key generation methods and the cryptographic algorithms, conformance to the Compliance Rules and preventing Controlled Content that has been unencrypted from copying or unauthorized viewing) shall be implemented in accordance with the “Level 2” requirements of the United States Federal Information Processing Standards (see FIPS PUB 140-2 “Security Requirements for Cryptographic Modules,” May 25, 2001), and, at a minimum, in a way that they:

- (i) Cannot be reasonably foreseen to be defeated or circumvented merely by using general purpose tools or equipment that are widely available at a reasonable price, such as screw drivers, jumpers, clips and soldering irons (“Widely Available Tools”), or using specialized electronic tools or specialized software tools that are widely available at a reasonable price, such as EEPROM readers and writers, debuggers or de-compilers or similar software development tools (“Specialized Tools”), other than devices or technologies whether hardware or software that are designed and made available for the specific purpose of bypassing or circumventing the protection technologies required (“Circumvention Devices”); and
- (ii) Can only with difficulty be defeated or circumvented using professional tools or equipment (excluding Circumvention Devices and professional tools or equipment that are made available only on the basis of a non-disclosure agreement), such as logic analyzers, chip disassembly systems, or in-circuit emulators or other tools, equipment, methods or techniques not included in the definition of Widely Available Tools and Specialized Tools in subsection (i) above.

(f) Advance of Technology. Although an implementation of a Host Device when designed and shipped may meet the above standards, subsequent circumstances may arise which had they existed at the time of design of a particular Host Device would have caused such product to fail to comply with this Exhibit B (“New Circumstances”). If Licensee has (a) actual Notice of New Circumstances, or (b) actual knowledge of New Circumstances (the occurrence of (a) or (b) hereinafter referred to as “Notice”), then within eighteen months after Notice Licensee shall cease distribution of such Host Device and shall only distribute Host Device that are compliant with this Exhibit B in view of the then-current circumstances.

5.0 Update Procedure.

CableLabs will meet with cable television system operators, Licensees and Content Providers on a regular basis to revise and update these rules to ensure that Host Devices remain secure against tampering and reverse engineering directed toward defeating the CableLabs Technology and any copy protection scheme incorporated therein.

EXHIBIT C-1

Robustness Checklist

Notice: This Checklist is intended as an aid to the correct implementation of the Robustness Rules for hardware and software implementations of the Specifications in a Host Device. This Checklist does not address all aspects of the Specifications and Compliance Rules necessary to create a product that is fully compliant. Failure to perform the tests and analysis necessary to comply fully with the Specifications, Compliance Rules or Robustness Rules could result in a breach of the CableCARD Interface License Agreement and appropriate legal action taken by CableLabs or other parties under the License Agreement.

DATE: _____

MANUFACTURER: _____

PRODUCT NAME: _____

HARDWARE MODEL OR SOFTWARE VERSION: _____

NAME OF TEST ENGINEER COMPLETING CHECKLIST:

TEST ENGINEER: _____

COMPANY NAME: _____

COMPANY ADDRESS: _____

PHONE NUMBER: _____

FAX NUMBER: _____

GENERAL IMPLEMENTATION QUESTIONS

1. Has the Host Device been designed and manufactured so there are no switches, buttons, jumpers, or software equivalents of the foregoing, or specific traces that can be cut, by which the content protection technologies, analog protection systems, output restrictions, recording limitations, or other mandatory provisions of the Specifications or Compliance Rules can be defeated or by which Controlled Content can be exposed to unauthorized copying?
2. Has the Host Device been designed and manufactured so there are no service menus and no functions (such as remote-control functions, switches, check boxes, or other means) that can intercept the flow of Controlled Content or expose it to unauthorized copying?
3. Has the Host Device been designed and manufactured so there are no service menus and no functions (such as remote-control functions, switches, check boxes, or other means) that can turn off any analog protection systems, output restrictions, recording limitations, or other mandatory provisions of the Specifications or Compliance Rules?
4. Does the Host Device have service menus, service functions, or service utilities that can alter or expose the flow of Controlled Content within the device?

If Yes, please describe these service menus, service functions, or service utilities and the steps that are being taken to ensure that these service tools will not be used to expose or misdirect Controlled Content.
5. Does the Host Device have service menus, service function, or service utilities that can turn off any analog protection systems, output restrictions, recording limitations, or other mandatory provisions of the Specifications or Compliance Rules?

If Yes, please describe these service menus, service functions, or service utilities and the steps that are being taken to ensure that these service tools will not be used to defeat the encryption features of DFAST (including compliance with the Compliance Rules and the Specifications).
6. Does the Host Device have any user-accessible buses (as defined in Section 2 of the Robustness Rules)?

If so, is Controlled Content carried on this bus?

If so, then:

identify and describe the bus, and whether the Controlled Content is compressed or uncompressed. If such Data is compressed, then explain in detail how and by what means the data is being re-encrypted as required by Section 2 of the Robustness Rules.
7. Explain in detail how the Host Device protects the confidentiality of all keys.
8. Explain in detail how the Host Device protects the confidentiality of the confidential cryptographic algorithms used in DFAST.
9. If the Host Device delivers Controlled Content from one part of the product to another, whether among software modules, integrated circuits or otherwise or a combination thereof, explain how the portions of the product that perform authentication and decryption and the MPEG (or similar) decoder have been designed, associated and integrated with each other so that Controlled Content are secure from interception and copying as required in Section 3(a) of the Robustness Rules.
10. Are any DFAST functions implemented in Hardware? If Yes, complete hardware implementation questions.

11. Are any DFAST functions implemented in Software? If Yes, complete software implementation questions.

SOFTWARE IMPLEMENTATION QUESTIONS

12. In the Host Device, describe the method by which all Keys are stored in a protected manner.
13. Using the grep utility or equivalent, are you unable to discover any Keys in binary images of any persistent memory devices?
14. In the Host Device, describe the method used to obfuscate the confidential cryptographic algorithms and Keys used in DFAST and implemented in software.
15. Describe the method in the Host Device by which the intermediate cryptographic values (e.g., values created during the process of authentication between modules or devices within a Host Device) are created and held in a protected manner.
16. Describe the method being used to prevent commonly available debugging or decompiling tools (e.g., Softice) from being used to single-step, decompile, or examine the operation of the DFAST functions implemented in software.
17. Describe the method by which the Host Device self-checks the integrity of component parts in such manner that modifications will cause failure of authorization or decryption as described in Section 3(b)(ii) of the Robustness Rules. Describe what happens when integrity is violated.
18. To assure that integrity self-checking is being performed, perform a test to assure that the executable will fail to work once a binary editor is used to modify a random byte of the executable image containing DFAST functions, and describe the method and results of the test.

HARDWARE IMPLEMENTATION QUESTIONS

19. In the Host Device, describe the method by which all Keys are stored in a protected manner and how their confidentiality is maintained.
20. Using the grep utility or equivalent, are you unable to discover any Keys in binary images of any persistent memory devices?
21. In the Host Device, describe how the confidential cryptographic algorithms and Keys used in DFAST have been implemented in silicon circuitry or firmware so that they cannot be read.
22. Describe the method in the Host Device by which the intermediate cryptographic values (e.g., values created during the process of authentication between modules or devices within a Host Device) are created and held in a protected manner.
23. Describe the means used to prevent attempts to replace, remove, or alter hardware elements or modules used to implement DFAST functions?
24. In the Host Device, does the removal or replacement of hardware elements or modules that would compromise the content protection features of DFAST (including the Compliance Rules, the Specifications, and the Robustness Rules) damage the Host Device so as to render the Host Device unable to receive, decrypt, or decode Controlled Content?
25. Is the Host Device certified by NIST to FIPS Level 2?

Notice: This checklist does not supersede or supplant the Specifications, Compliance Rules, or Robustness Rules. The Company and its Test Engineer are advised that there are elements of the Specifications, the Robustness Rules and the Compliance Rules that are not reflected here but that must be complied with.

SIGNATURES:

Signature of Test Engineer with Personal Knowledge of Answers

Date

Printed Name of Test Engineer with Personal Knowledge of Answers

