

DCAS Host License Agreement

THIS LICENSE AGREEMENT is made as of _____ (“**Effective Date**”), by and between Cable Television Laboratories, Inc., a Delaware non-stock company with offices at 858 Coal Creek Circle, Louisville, Colorado 80027 USA (“**CableLabs**”) and the party identified below (“**Licensee**”).

Name of Licensee: _____	Licensee Contact: _____
Address: _____	Title: _____
_____	Phone: _____
_____	Fax: _____
_____	E-Mail: _____

Licensee is in the business of, among other things, designing, developing, manufacturing and distributing devices and/or components for use in the cable television industry. CableLabs owns or has the rights to certain technology necessary for implementing a downloadable conditional access system (DCAS) on the cable network.

CableLabs desires to grant licenses to certain specifications, patents, and know-how, and Licensee desires to acquire such a license for the purpose of developing and/or creating and distributing devices that utilize the Licensed Technology. The license granted hereunder is conditioned upon CableLabs certification that the Host Devices comply with the DCAS Specifications, the requirements of this Agreement, and that such devices are interoperable in order to foster retail availability.

LICENSEE HAS READ AND AGREES TO BE BOUND BY THE TERMS AND CONDITIONS OF THIS AGREEMENT, INCLUDING THOSE TERMS CONTAINED ON THE FOLLOWING PAGES HEREOF. The parties have executed this Agreement and enter into this Agreement as of the Effective Date.

CABLE TELEVISION LABORATORIES, INC.	LICENSEE: _____
Signed: _____	Signed: _____
Name: _____	Name: _____
Title: _____	Title: _____

1. DEFINITIONS

1.1 “Affiliate” means any entity that directly or indirectly owns or controls, is owned or controlled by, or under the common control of another entity, wherein the term “control” means voting control over greater than fifty percent (50%) of: (a) an entity’s common shares; or (b) the total number of board members sitting on the entity’s board of directors.

1.2 “ATP” means the acceptance test procedure utilized by CableLabs to test and certify Host Devices.

1.3 “Cable Operator” means any cable operator that CableLabs identifies as providing Service to customers in North America using the DCAS Technology.

1.4 “Certify” “Certified” or “Certification” means the CableLabs testing process to verify that a proposed Host Device is in compliance with the DCAS Specifications. Certification is conducted against the then-current DCAS PICS and ATP in accordance with the CableLabs Certification Guidelines. All such documents are posted at www.opencable.com/dcas.

1.5 “Certified Host Device” means a Host Device that has obtained Certification.

1.6 “CHILA” means the CableCARD Host Interface License Agreement entered into by Licensee in connection herewith. CHILA provides Licensee a license to the DFAST Technology and know-how.

1.7 “Compliance Rules” mean the rules described in **Exhibit C** hereto which apply to Host Devices and components thereof.

1.8 “Content Providers” means any video programming providers that provide copyrighted works for transmission to Certified Host Devices and the copyright owners of such works.

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

1.10 “DCAS Host License Agreement” means an agreement substantially similar to this Agreement.

1.11 “DCAS Know-How” means the know-how, trade secrets, copyrighted works, reference source code implementations, shared secret keys, Diffie-Hellman system parameters, encryption and decryption keys, Root Public Keys, signature verification/generation methodologies, software development tools, methodologies, processes, technologies or algorithms, test data sets and test cases that CableLabs or its agent may deliver to Licensee to assist in incorporating the Licensed Technology into Licensed Products, and any and all information relating to the Licensed Technology made available to Licensee by CableLabs, its designees or representatives or any DCAS Participants, including, without limitation, specifications, software, hardware, firmware, documentation, designs, flow charts, technical data, outlines, blueprints, notes, drawings, prototypes, templates, systems, manuals, know-how, processes and methods of operation.

1.12 “DCAS Participant” means a party identified by CableLabs that provides products and/or services, or portions thereof, licensed to use the DCAS Technology.

1.13 “DCAS Patents” means any Necessary Claims owned or licensable by CableLabs, including claims found in the patents identified in Exhibit A and any division, continuation or continuation in part, or any patent reissuing on or reissuing pursuant to a reexamination of the foregoing patents, and all foreign equivalents owned or licensable by CableLabs.

1.14 “DCAS Specifications” means the family of specifications posted at www.opencable.com/dcas as modified by CableLabs from time to time.

1.15 “DCAS Technology” means, collectively, the technology licensed to the DCAS Participants, including, but not limited to, the DCAS Specifications and DCAS Know-How.

1.16 “DFAST Technology” shall have the meaning set forth in CHILA.

1.17 “Document Handling Rules for DCAS” refers to the set of rules under such title distributed by PolyCipher, as it may be amended from time to time in accordance with its terms.

1.18 “Highly Confidential Information” means reference source code implementations, shared secret keys, authority signing keys, encryption and decryption keys, private keys, Key usage and sizing descriptions, network authentication and key exchange protocols; One Time Programmable (OTP) values (unique numbers) of a specified bit length assigned to each Certified Host Device, Qualified Transport Processor, Qualified Secure Micro or any component of such devices, and any of the numbers or values used in the process for encryption, decryption, digital signatures, or key exchanges of Controlled Content; all DCAS Technology that is not identified by CableLabs on its face as public information; all DCAS Know-How made available to Licensee by or on behalf of PolyCipher; and all application programming interfaces (APIs) and software associated with DCAS Know-How.

1.19 “Host Device” means a bi-directional set-top terminal, television or navigation device for selecting Services on a program by program basis and that utilizes the Licensed Technology.

1.20 “Host Profile” means the minimal technical functional requirements for one or more Host Devices, as designated in the DCAS Specifications and the DCAS Know-How.

1.21 “Intellectual Property Rights” or “IPR” means all intellectual property rights owned or licensable without restriction or obligation to pay a royalty to a licensor, worldwide, 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, and (d) 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, but not including trademarks, trade dress, trade name, design patent and service mark rights, whether or not registered.

1.22 “Licensed Components” means component products which utilize in whole or in part the Licensed Technology, and which are designed for incorporation into Prototypes or Certified Host Devices.

1.23 “Licensed Product” means the Licensee’s Host Device and includes Licensed Components.

1.24 “Licensed Technology” means the technology identified in Exhibit A of this Agreement, including the DCAS Specifications, the DCAS Patents, and the DCAS Know-How specified therein; provided however, that Licensed Technology does not include technology licensed under separate agreements from CableLabs, including CHILA (the DFAST Technology), the OCAP Implementers License Agreement, the Digital Certificate Authorization Agreement, or any third party proprietary technology referenced in or required by the DCAS Specifications or the DCAS Know-How, such as DTCP, or MPEG-2.

1.25 “Necessary Claims” means a claim of any patent or published patent application throughout the world that is issued now or in the future, that is necessarily infringed as a result of implementing any portion of the DCAS Technology. Necessary Claims shall not include: (a) claims in design patents or design registrations; (b) claims related to technology or know-how that may be necessary to make or use a product or service, or portion thereof, that complies with the DCAS Technology, but that is not set forth in the DCAS Technology; (c) any enabling technologies that may be necessary to make or use any product or portion thereof that complies with the DCAS Technology, but are not themselves expressly set forth in the DCAS Technology (*e.g.*, compiler technology, object oriented technology, basic operating system technology, etc.); or (d) any claims other than as set forth above, even if contained in the same patent or published patent application as Necessary Claims.

1.26 “PICS” means the Protocol Implementation Compliance Statements, or tests, utilized by CableLabs to test and Certify Host Devices.

1.27 “PolyCipher” refers to NGNA, LLC d/b/a PolyCipher.

1.28 “Prototype” means a pre-production model of a device (including Host Devices or Licensed Components) that utilizes the Licensed Technology in whole or in part, and is not made commercially available.

1.29 “Qualified Secure Micro” means a microprocessor that utilizes the DCAS Technology under the terms of a DCAS Secure Micro License Agreement with CableLabs and has been qualified by CableLabs.

1.30 “Qualified Transport Processor” means a microprocessor that utilizes the DCAS Technology under the terms of a DCAS Transport Processor License from CableLabs and that has been qualified by CableLabs.

1.31 “Robustness Rules” mean the rules described in **Exhibit B** hereto. These rules apply to Host Devices and are for the purpose of resisting attempts to modify Host Devices, Qualified Secure Micros or Qualified Transport Processors or otherwise circumvent or defeat any function of the DCAS Specifications, the DCAS Technology, or the Compliance Rules.

1.32 “Service” means video, audio, or data signals, whether in analog or digital format, transmitted over the cable system to (or from) the Host Device, for the purposes of effectuating the reception or transmission of information, entertainment, or communications content. Service

includes signals received via DSG as provided in the DCAS Specifications, but does not include signals received by retail DOCSIS cable modem service.

1.33 “Third Party Beneficiary” means any Content Provider or Cable Operator and PolyCipher.

2. GRANT OF LICENSES

2.1 DCAS Specifications. Subject to and conditioned upon Licensee’s compliance with the terms of this Agreement, CableLabs grants to Licensee a limited, worldwide, non-exclusive, perpetual (unless this Agreement is terminated pursuant to the terms hereunder), non-transferable (except as permitted under this Agreement), royalty-free right and license under the Intellectual Property Rights owned or licensable by CableLabs solely to:

(a) view or download the DCAS Specifications identified in Exhibit A; and

(b) use, reproduce, and distribute the DCAS Specifications identified in Exhibit A for the purpose of making Host Devices, Prototypes, Licensed Components and Certified Host Devices.

2.2 Prototypes. Upon the execution of this Agreement and payment of the License Fee (as defined below), and subject to the applicable terms and conditions set forth herein, Licensee shall have the limited right and license:

(a) to develop, make, have made, use and test no more than one hundred Prototype Host Devices and/or Licensed Components which are designed for incorporation into Prototypes, or more upon reasonable justification and written authorization by CableLabs, and to possess, reproduce and otherwise use the Licensed Technology for such purposes;

(b) to distribute such Prototypes, but only to DCAS Participants that have been licensed to view and use any Highly Confidential Information that can be obtained from possession of the Prototype,

(c) to exchange information about and test interoperability with the Licensed Technology, but only with other DCAS Participants and only in accordance with Section 6 of this Agreement, and

(d) to distribute such Prototypes to Cable Operators in North America (including the United States and Canada) for the purpose of field trials and technology evaluation, but not for retail or commercial use, provided that no Highly Confidential Information is revealed in such distribution.

Sections 2.3, 2.4, 4 and 7.2(b), and Exhibits B and C, shall not apply with respect to Prototypes.

2.3 Certified Host Devices. Subject to the terms and conditions set forth herein, including without limitation the Robustness Rules and the Compliance Rules, CableLabs hereby grants to Licensee, a non-exclusive, non-transferable (except as allowed hereunder) world-wide license under the Intellectual Property Rights owned by, or licensable from, CableLabs in the Licensed Technology to:

(a) make, have made, use, sell, offer to sell, import and otherwise distribute Certified Host Devices that incorporate the Licensed Technology, including practicing any method or process under the DCAS Patents;

(b) coordinate with other DCAS Participants regarding the development of or modifications to products that utilize DCAS Technology, and regarding implementation of the Licensed Technology, subject to the confidentiality terms set forth in Section 6 of this Agreement, including any additional terms established pursuant to Section 6.1;

(c) provided that, notwithstanding the licenses granted herein, the use of the Licensed Technology shall be limited to use in Certified Host Devices distributed in North America; and

(d) provided further that, notwithstanding the license granted above, Licensee shall not include the Licensed Technology in any commercially offered Host Devices prior to Certification of such Host Device by CableLabs.

2.4 Licensed Components. Licensee shall have the limited right to make, have made, use, sell, offer to sell, import and otherwise distribute Licensed Components, subject to the following limitation: Licensee shall distribute the Licensed Components containing the Licensed Technology, or parts thereof, only to DCAS Participants that have been licensed to view and use any Highly Confidential Information that can be obtained from possession of the Licensed Component. Licensee must separately maintain records of sales of Licensed Components, and Licensee shall, upon request provide the names and contact information of each purchaser to CableLabs.

2.5 Have Made Rights. Licensee shall have the right under licenses granted under Sections 2.1 through 2.4 to have third parties (“Have Made Parties”) make (including for the avoidance of doubt, design) Prototypes, Licensed Products, Licensed Components, or subparts thereof for the sole account of Licensee, provided that with respect to Licensed Products, Licensed Components, or subparts thereof they (a) are to be sold, used, leased, or otherwise disposed of, by or for Licensee under the trademark, tradename, or other commercial indicia of Licensee or an entity to which Licensee is authorized hereunder to sell such, Licensed Products, or Licensed Components and (b) are made by such Have Made Parties using designs or specifications supplied by or for Licensee. Licensee shall be fully responsible for such Have Made Parties’ compliance with all terms of this Agreement as if Licensee itself were performing such manufacture. Have Made Parties must have obtained a license from CableLabs or PolyCipher to use DCAS Know-How, be an Affiliate of Licensee, or be bound in writing to an applicable non-disclosure agreement with Licensee on terms that are no less stringent than the terms set forth in Section 6 hereof. In addition, each Have Made party which is implementing DCAS Specifications or DCAS Know-How or has access to Highly Confidential Information, or other information or materials from which Highly Confidential Information could reasonably be derived must be contractually bound to the provisions set forth in Sections 2.8, 6, 7.2(d), 12, 13.5, 13.6, 13.8 and 13.11 of this Agreement by a written instrument provided to CableLabs. Affiliates shall receive no license, sublicense, or implied license with respect to the DCAS Technology or any copyrights in the OpenCable Specifications. Licensee must separately maintain records of sales of Licensed Components, and Licensee shall, upon request provide the names and contact information of each purchaser to CableLabs. Licensee agrees and acknowledges that the fact that it has contracted with a Have Made Party shall not relieve Licensee of any of its obligations under this Agreement.

2.6 Limitation on All Licenses. The Licensed Technology shall be used by Licensee only for receipt, decryption and handling of Services received from a Cable Operator, and for no

other purpose. CableLabs and/or its licensors reserve all rights in and to the Licensed Technology not expressly granted to Licensee in this Agreement and all applicable Exhibits hereto. Licensee shall not reverse engineer, disassemble, or decompile the Licensed Technology. All Licensed Technology, and media containing such Licensed Technology shall remain the property of CableLabs or its licensors. There are no implied licenses under this Agreement, and any rights not expressly granted to Licensee hereunder are reserved by CableLabs and its licensors. Except for the limited license granted under Section 2.2, no license is granted for any commercial Host Device that does not comply with the DCAS Specifications, the DCAS Know-How, the Robustness Rules, the Compliance Rules and the Certification Criteria.

2.7 Flexible Implementations. Nothing in this Agreement shall preclude Licensee from including in a Certified Host Device additional features or functionalities not specified in the DCAS Specifications so long as such additional features are in conformance with Section 7.2 below and no change is made to the Licensed Technology. Such devices may include, but are not limited to, Host Devices with an integrated recording device that otherwise meet the requirements of this Agreement. It is further understood and agreed that nothing in this Agreement shall affect any other products manufactured by Licensee not under this Agreement, other than Host Devices, and that this Agreement shall in no way impose any limit on the types of devices that do not use the Licensed Technology that may be manufactured by Licensee.

2.8 Authorization by CableLabs. Within ten (10) days of the later of (a) execution of this Agreement, (b) receipt of the Fees hereunder, and, as applicable, (x) execution of the Digital Certificate Authorization Agreement and complete verification of Licensee's information therein for security purposes, and (y) execution of the OCAP Implementers License Agreement, CableLabs shall cause PolyCipher to provide to Licensee, subject to security approval, the relevant portions of DCAS Know-How that Licensee has not previously received, and to make arrangements for receipt of appropriately keyed Qualified Secure Micros and Qualified Transport Processors as required for Certified Host Devices. Licensee may contact PolyCipher at:

Shannon Johnson
PolyCipher
999 18th St., Suite 1925
Denver, CO 80202
Shannon.Johnson@PolyCipher.com

3. Change Management.

3.1 Specifications. The DCAS Specifications, including the Licensed Technology, may be amended from time to time by CableLabs, but only in accordance with the OpenCable Change Process as more fully described in Exhibit D. Changes may be made for the purpose of correcting any errors or omissions or clarifying, but not materially amending, altering or expanding the same ("Editorial Changes"); altering the existing requirements or adding new requirements ("Minor Changes"); and creating new Host Profiles and/or new variations of the DCAS Specifications ("New Specifications") (collectively, "Changes"). New Specifications may include, by way of example and not of limitation, changes that would require new technical features not included in previous DCAS Specifications, or that would materially increase the cost or complexity of Host Devices. In adopting any Changes, CableLabs shall consider, among other things, the economic burden that Licensee will bear as a result of implementing such change, taking into account such factors as cost to implement, production cycles, backward compatibility and existing inventory of Licensee, the cumulative effects of Changes on software architecture, as well as consumer choice, interest in innovation, economic burden on the Cable Operator, and developments in technology. Any change in the DCAS Specifications that would effectively amend the Compliance Rules shall

be subject to the terms of Section 3.6. The DCAS Know-How may be amended from time to time by PolyCipher pursuant to the PolyCipher change process as more fully described in Exhibit E hereto.

3.2 Participation in Change Process for DCAS Specifications. Licensee shall be provided notice of and a reasonable opportunity to review and comment on any proposed changes to DCAS Specifications identified in Exhibit A, subject to its execution of applicable non-disclosure and contribution agreements. CableLabs represents and warrants that all DCAS Specifications are subject to the OpenCable Change Process as more fully described in Exhibit D hereto. The OpenCable Change Process shall include the ability of Licensee to draft and submit ECRs, and for CableLabs' NDA participants (including Licensee) to comment on ECOs and have an opportunity to participate in the ECR Working Groups. In addition, if Licensee disagrees with a decision to either issue an ECO or to dismiss an ECO, Licensee shall have the opportunity to discuss the matter with a senior member of CableLabs' management, and CableLabs shall give due consideration to Licensee's concerns with regard to the proposed ECO. Parties to the OpenCable Change Process may also include Content Providers. It is understood and agreed that all interested parties described above shall have executed a version of the OpenCable Confidential Information Access Agreement that is substantially in the same form as that executed by Licensee, before being afforded access to any proposed revisions.

3.3 Effect of Changes.

(a) Existing Products. Unless required by (1) a change to the Compliance Rules under Section 3.6 of this Agreement, (2) a change to the Robustness Rules under Section 5 of the Robustness Rules, or (3) a change to the DCAS Technology which CableLabs has reasonably designated as being critical to preventing theft of service, harm to the network or breach of the Compliance Rules or Robustness Rules or to safety, Licensee may continue to manufacture, use, sell, or distribute any previously Certified Product (and may continue to seek Certification pursuant to the paper submission process described in the Certification Wave Guidelines), notwithstanding any Changes or sunseting of Certification.

(b) Editorial Changes. Editorial Changes shall become effective on the date specified in the ECN. Editorial Changes shall not interfere with the capabilities of previously Certified products.

(c) Minor Changes. Minor Changes shall become effective on a commercially reasonable date defined by the applicable ECR Working Group (as specified in the ECN) after reasonably considering the impact to vendors with products that may be affected by the Minor Change. The commercially reasonable effective date established by the applicable ECR Working Group may be altered as follows: (i) any Changes requiring a change in silicon, or the addition of a component where the lead time for acquiring the component is longer than ninety (90) days shall not become effective in less than twelve (12) months, unless otherwise agreed by Licensee or unless reasonably designated by CableLabs as being critical to preventing theft of service, harm to the network or breach of the Compliance Rules or Robustness Rules or to safety; and (ii) Licensees who have provided CableLabs with 120 days written notice of their intent to bring products to CableLabs for Certification at the next Certification Wave will *not* be required to (but may choose to) implement such Minor Changes in such products for such Certification Wave, unless such Minor Changes have been reasonably designated by CableLabs as being critical to preventing theft of service, harm to the network or breach of the Compliance Rules or Robustness Rules or to safety. Minor Changes shall not interfere with the capabilities of previously Certified products.

(d) **Updates to Issued Specifications.** Minor Changes and Editorial Changes (in the form of ECNs) will be aggregated and added to existing DCAS Specifications from time to time.

(e) **New Specifications.** New specifications are effective on the date they are first published. New specifications shall not automatically obsolete existing specifications.

3.4 Dispute Resolution. In the event that Licensee reasonably, and in good faith, objects to Changes (including the effective date of such Changes), or the sunseting of Certification, it shall provide written notice of such objection to CableLabs (the “Objection Notice”). The parties shall attempt in good faith to resolve the dispute within ten (10) days following CableLabs’ receipt of such Objection Notice. In the event that the parties are unable to resolve the dispute in such ten-day period, the matter shall be escalated to senior executives of each party, designated by each party, who shall attempt in good faith to resolve the dispute within ten (10) days following their designation and no more than thirty (30) days following CableLabs’ receipt of the Objection Notice.

3.5 Revision to Certification Criteria. When required by Changes described in this Section 3, CableLabs shall also revise the Certification Criteria, including the PICS, Acceptance Test Plan, or other testing procedures to accommodate such Changes. Prior to any revision of the Certification Criteria, Licensee shall be given notice of, and the opportunity to comment on, such proposed revision, at least sixty days prior to the date the revised Certification Criteria take effect (thirty days in the case of revisions reasonably designated by CableLabs as being critical to preventing theft of service, harm to the network or breach of the Compliance Rules or Robustness Rules or to safety). CableLabs shall in good faith consider Licensee’s comments. It is understood and agreed that all interested parties described above shall have executed a version of the OpenCable Confidential Information Access Agreement that is substantially in the same form as that executed by Licensee, before being afforded access to any proposed revisions.

3.6 Revision to Compliance Rules. CableLabs may, from time to time, revise the Compliance Rules. CableLabs shall give Licensee at least sixty days’ notice of any proposed changes to the Compliance Rules (thirty days in the case of revisions reasonably designated by CableLabs as being critical to preventing theft of service, harm to the network or breach of the Compliance Rules or Robustness Rules or to safety). In adopting such changes, CableLabs shall consider, among other things, the economic burden that Licensee will bear as a result of implementing such change, taking into account such factors as cost to implement, production cycles, backward compatibility and existing inventory of Licensee, as well as consumer choice, interest in innovation, and developments in technology. Licensee shall be required to comply with all changes to the Compliance Rules within twelve (12) months after notification of the changes has been sent as specified in this Section 3.6, or, in extraordinary cases, within such shorter or longer period as reasonably specified by CableLabs in accordance with this Section. In the event that Licensee disagrees with a change to the Compliance Rules, or has been denied a request to change the Compliance Rules (e.g., by submitting a new digital output technology), Licensee may use the Dispute Resolution process identified in Section 3.4 hereof.

~~**3.7SRMs.** For the avoidance of doubt, the parties agree that CableLabs may provide notice to Licensee to include in all newly manufactured Licensed Products a technical method for propagating System Renewability Messages (“SRMs”), including, but not limited to, receiving, acknowledging, honoring, storing, and further distributing SRMs. Such SRM method and the criteria for using that propagation method to be developed on a multi industry basis pursuant to a broad consensus in an open, fair, voluntary process.~~

4. Testing and Certification.

4.1 Prior to commercially distributing a Host Device, Licensee shall participate in the CableLabs-sponsored DCAS interoperability tests for the purpose of verifying that the proposed Host Device conforms in all material respects to the Certification Criteria. Licensee's submission for Certification shall be in compliance with the then-current CableLabs Certificate Wave Testing Guidelines. CableLabs shall use best efforts in the utmost of good faith to make the Certification Criteria and the certification process objective, fair and non-discriminatory. Licensee acknowledges and agrees that any production of Host Devices prior to completion of testing and Certification contemplated by this Section shall be undertaken at Licensee's sole risk.

5. Payments.

5.1 License Fee. As consideration for the licenses granted hereunder, Licensee agrees to pay CableLabs a one-time, non-refundable license fee of \$20,000 within thirty days of the Effective Date. All payments shall be made in US Dollars.

5.2 Applicable Taxes. All fees owed by Licensee to CableLabs are exclusive of, and Licensee shall pay, all sales, use, value added, excise, and other taxes (other than income taxes) that may be levied upon either party by any domestic or foreign taxing authorities in connection with this Agreement, and shall pay all income taxes that may be levied upon Licensee.

6. Confidentiality.

6.1 Confidentiality. Licensee shall protect the confidentiality of any information that is confidential or proprietary to CableLabs or PolyCipher using safeguards that are at least as rigorous as Licensee employs for its own confidential, proprietary information, and in any case using no less than a reasonable degree of care. Licensee must comply with all of the terms for the protection of such information that are set forth in the Document Handling Rules for DCAS, as amended from time to time and any additional standards for the secure handling of DCAS Know-How and Highly Confidential Information supplied by PolyCipher, and shall not use or disclose Confidential or Highly Confidential Information in any manner whatsoever except as permitted by such terms. Licensee shall reasonably cooperate with CableLabs and its employees and agents to maintain the security of Confidential and Highly Confidential Information.

6.2 Review of Confidentiality Measures. CableLabs and PolyCipher (or, as provided below, a mutually agreed third-party auditor) shall have the right to review, upon fifteen (15) 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 under the Document Handling Rules for DCAS no more frequently than once per year (unless CableLabs has a good faith belief that Highly Confidential Information has been, or will be, compromised in any manner) at reasonable times as agreed between Licensee and CableLabs and PolyCipher. At the option of CableLabs, PolyCipher or Licensee, this review may be conducted by a mutually acceptable third-party auditor. Confidential information disclosed in connection with an audit may be shared only with persons who have responsibility for implementation of the Licensed Technology, enforcement of DCAS License Agreements, or the conduct of the audit, and may not be used for purposes unrelated to the exercise of such responsibilities. CableLabs and Licensee hereby consent to use of the following third-party auditors: Verisign, Merdan, Symantec/@Stake, CyberTrust, and RSA Security Inc.

6.3 Notification of Unauthorized Use or Disclosure. Licensee shall report any form of security breach related to the requirements under this Agreement with respect to physical security, theft or loss of Highly Confidential Information, theft of equipment, theft and/or compromise of keys, security tokens, entry keys, system passwords or other abnormal conditions to CableLabs and PolyCipher within 24 hours of its detection. Licensee shall notify CableLabs immediately upon discovery of any unauthorized use or disclosure of DCAS Technology, and will cooperate with CableLabs and PolyCipher in every reasonable way to regain possession of the disclosed DCAS Technology and to prevent its further unauthorized use or disclosure.

6.4 Liability for Breach of Confidentiality. Licensee shall be responsible for any breach of confidentiality under this Agreement by its Affiliates, subcontractors, consultants, agents, employees, suppliers, officers, directors, customers (other than members of CableLabs), representatives, former Affiliates, former subcontractors, former consultants, former agents, former employees, former suppliers, former officers, former directors, former customers (other than CableLabs members), former representatives, or any other person to the extent such breach results from disclosure by Licensee to such party of confidential DCAS Technology. No obligation of confidentiality is imposed on information which (i) is already in or subsequently enters the public domain through no breach of Licensee's obligations hereunder and which CableLabs or PolyCipher failed to remove, or to initiate efforts to remove, from public availability or to enjoin such public disclosure within 90 days after the date such information is or becomes generally known as set forth above; or (ii) 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 or PolyCipher. Notwithstanding anything in Sections 6.1 and 6.2 to the contrary, DCAS Know-How may be disclosed by Licensee pursuant to the order or requirements of a court or governmental administrative agency 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, (y) Licensee cooperates in good faith with such efforts by CableLabs and (z) Licensee discloses only the least possible information necessary to satisfy such legal requirement. The obligations under Section 6 shall terminate three years after the last commercial use of the DCAS Technology by Licensee or any DCAS Participant; except that Section 6.2 shall cease to apply when Licensee has returned all tangible embodiments of DCAS Know-How in its possession to CableLabs and/or PolyCipher.

7. WARRANTIES

7.1 Licensee. Licensee represents, warrants, and covenants that:

(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; and

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

7.2 Licensee represents, warrants, and covenants that each Certified Host Device shall:

(a) at the time of manufacture, be compliant with the applicable DCAS Specifications and DCAS Know-How;

(b) at the time of manufacture:

(i) contain no integrated circuit, ROM, RAM, software or other device or functionality that (1) enables access, copying, distribution, or usage of Controlled Content, other than as permitted by the Compliance Rules or (2) interferes with or disables the ability of an Operator to communicate with or disable conditional access or services being transmitted;

(ii) maintain control of content and copies consistent with content protection instructions or the encryption mode indicator bits transmitted with digital signals as specified in the DCAS Specifications;

(iii) be designed to effectively frustrate tampering and reverse engineering directed towards defeating content protection requirements in accordance with the Robustness Rules; and

(iv) not transmit or decode Controlled Content received from the cable television transmission without proper authorization from the Cable Operator.

(v) As used in this section 7.2, “at the time of manufacture” shall mean at the time of manufacture of the Host Device and shall also include, but is not limited to, any subsequent modifications, upgrades, downloads, modules, plug-ins, or attachments to such Host Device made by or at the direction of Licensee or its Affiliates, or otherwise specifically promoted, marketed, distributed by or at the direction of Licensee or its Affiliates. Licensee shall not service or support any Host Device that it determines to have been modified after manufacture to be non-compliant with these provisions, unless otherwise authorized by the Cable Operator providing service to that Host Device. Licensee shall promptly notify CableLabs and PolyCipher of any such modifications that is known or suspected to cause an unreasonable risk of unauthorized access to any content or the DCAS Technology, or unauthorized copying, distribution, or modification of usage rights.

(c) consistent with the technical capabilities of the device, display content and applications in the manner that the DCAS Specifications direct that such content and applications should be displayed; and

(d) include no feature or functionality that (i) technically disrupts, impedes or impairs the delivery of services to any cable customer, including, but not limited to, for clarification purposes and subject to Section 2.7 above, delivering all services provided by the Cable Operator to the Certified Host Device in the same manner that such services are delivered by equivalent Cable Operator devices to the cable customer (except where such disruption, impediment, or impairment is a necessary consequence of complying with the DCAS Specifications, and there is no alternative compliant implementation); (ii) causes physical harm to the cable network; (iii) facilitates theft of service or otherwise interferes with reasonable actions taken by Cable Operators to prevent theft of service; (iv) jeopardizes the security of any services offered over the cable system; (v) interferes with or disables the ability of a Cable Operator to communicate with or disable services being transmitted through the cable System; or (vi) facilitates device cloning or otherwise interferes with reasonable actions taken by Cable Operators to prevent device cloning.

7.3 CableLabs. CableLabs represents, warrants and covenants that:

(a) CableLabs is authorized to enter into this Agreement and has obtained all Intellectual Property Rights in the Licensed Technology owned or licensable by PolyCipher that

are within the scope of the rights granted by this Agreement, subject to Section 7.3(b) and Section 7.4 and all other terms and conditions of this Agreement;

(b) without investigation, it is not aware of any notice or claim, threatened or pending, that the use of the Licensed Technology in accordance with the terms of this Agreement infringes any third party's intellectual property rights, except as identified by CableLabs to Licensee;

(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; and

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

7.4 Disclaimer of Warranties. OTHER THAN AS SET FORTH IN SECTION 7.3, THE LICENSED TECHNOLOGY IS LICENSED "AS IS," AND ALL REPRESENTATIONS AND WARRANTIES, INCLUDING ANY IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT, ARE HEREBY DISCLAIMED BY CABLELABS. Licensee acknowledges that the Licensed Technology does not include a license to use any third party proprietary technology referenced in or required by the DCAS Specifications or the DCAS Know-How, such as DTCP, or MPEG-2, that is not owned or controlled by CableLabs. Licensee understands that implementation of the DCAS Specifications or the DCAS Know How may necessitate implementation or use of such materials, that third parties may take the position that Licensee is required to enter into separate agreements for the use of such technology or materials, and that such agreements may include obligations in addition to those contained herein, including, without limitation, a duty to pay royalties to such parties, full compliance with the provisions of such materials, and/or a reciprocal grant of essential IPRs.

8. IPR Provisions

8.1 Reciprocal Non-Assertion Agreement. Licensee, on behalf of itself and its Affiliates, promises not to assert or maintain against CableLabs, PolyCipher or any DCAS Participant that has agreed to and remains subject to this same provision and Affiliates thereof, and accepts DCAS Participant's promise not to assert or maintain, any claim of infringement under its or their respective Necessary Claims, as well as under any trade secrets or copyrights embodied in the DCAS Technology for the making, having made, use, import, offering to sell, sale, copying, or distribution of any products or services that are licensed to use the DCAS Technology; provided that in each case such promise shall not extend to features of a product which are not required to comply with the DCAS Technology or for which there exists a noninfringing alternative. If a DCAS Participant (a) is willfully in material breach of its obligations under its DCAS Participant agreement, (b) fails to comply with its non-assertion agreement with respect to Licensee, or (c) is otherwise in material breach of its DCAS Participant agreement, which breach has not been cured or is not capable of cure within thirty (30) days of such DCAS Participant's receipt of notice thereof, then the promises made by Licensee in this Section 8.1 do not apply with respect to that DCAS Participant.

8.2 Joint Defense of Intellectual Property Claims. If CableLabs on the one hand, and/or Licensee or any DCAS Participant on the other hand (each a "**Defendant**"), should be sued on a single claim or related claims that products or services that implement the DCAS Technology necessarily infringe the patent or other rights of non-DCAS Participant (a "**Suit**"), then CableLabs and each DCAS Participant Defendant 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 DCAS Participant 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 each Defendant 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.

8.3 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 products or services that implement the DCAS 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 DCAS Technology and does not infringe such patent.

8.4 Review Period. The provisions of Sections 8.1 and 8.2 shall not be effective until thirty (30) days after receipt of the materials delivered under Section 2.8 (the "Review Period"), with no receipt by CableLabs of a notice of termination by Licensee under of this Agreement during such Review Period. In the event that termination by Licensee of this Agreement occurs within such Review Period, the provisions of Section 8.1 and 8.2 shall not be effective or binding on Licensee.

9. TERM AND TERMINATION

9.1 Term. The term of this Agreement shall commence on the Effective Date and shall continue indefinitely, unless terminated earlier by mutual consent of the parties or in accordance with this Section.

9.2 Licensee Termination for Convenience. Licensee shall have the right to terminate this Agreement at any time, for any reason or no reason, on thirty (30) days prior notice to CableLabs.

9.3 CableLabs Termination for Material Changes. In the event that material changes to this Agreement are necessitated by technological modifications and advancements to the DCAS Technology, governmental processes, or industry negotiation, CableLabs shall have the right to terminate this Agreement on thirty (30) days prior notice to Licensee; provided that CableLabs shall negotiate with Licensee to accommodate the resulting changes into a modified form of DCAS Host License Agreement which will be made available to Licensee in place of the terminated Agreement.

9.4 CableLabs Termination for Material Breach. CableLabs may terminate the license associated with a particular model of Certified Host Device as to which Licensee has materially breached Section 2 or 7.2 (as those obligations applied at the time the device was licensed and/or Certified). Upon cure of such breach hereunder, Licensee may continue to manufacture such model under the terms of this Agreement. However, CableLabs may only terminate the licenses pursuant to this Section 9.4 after CableLabs has (a) evaluated the potential breach, (b) consulted with Licensee regarding the potential breach, (c) and thereafter given written notice to Licensee of CableLabs' intent to terminate the license with respect to such chip or model, and (d) provided Licensee with a reasonable thirty (30) day opportunity to cure the breach (where such breach is capable of being cured) and such breach remains uncured for thirty (30) days following the date of such notice, or, if such breach cannot by its nature be cured within such

period, and the breach does not subject cable content to an unreasonable risk of unauthorized access, copying, distribution, or modification of usage rights, and is not a breach of Sections 2 or 7.2 of this Agreement, then for a longer period as reasonably determined by CableLabs. Termination of the licenses granted for any specific model of Certified Host Device shall not affect the licenses granted for any other model.

9.5 Obligations Upon Termination.

(a) **No Use of Licensed Technology.** Upon the termination of the licenses granted hereunder for any specific model of Certified Host Device pursuant to Section 9.4, Licensee may no longer make, have made, use, sell, import or distribute such model, nor use the Licensed Technology therewith. Licenses properly granted by Licensee in conjunction with the sale or distribution of a Certified Host Device by Licensee pursuant to Section 2 prior to the date of termination shall remain in full force and effect. Licensee may continue to service any Host Device that was compliant at the time of manufacture with the requirements of Section 7.2 and that has not been modified after manufacture to be non-compliant with those provisions, and any Host Device for which it has been authorized by the Cable Operator providing service to that Host Device. Unless otherwise stated herein, no termination of this Agreement 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 9.5(b) be affected by such termination.

(b) **Survival.** Unless specified otherwise in this Agreement, termination of this Agreement will not relieve either party from fulfilling its obligations that by their terms or nature survive termination, including, but not limited to, Sections 1, 6-13. Notwithstanding any termination of this Agreement, the provisions of Section 8.1 (Reciprocal Nonassertion Agreement) shall apply to all patents existing at the time of termination, and all patents issuing from patent applications filed by Licensee, with respect to Necessary Claims only, within one year and one day from the date of such termination.

10. INDEMNIFICATION. Licensee and CableLabs will each defend, indemnify and hold harmless the other and the other's member companies, licensors (including but not limited to PolyCipher), and contractors, including all officers, directors, employees or agents thereof (the "**Indemnitees**"), against any third party claims and suits ("**Claims**") that arise from or relate to any claim alleging facts that would constitute a material breach by Licensee or CableLabs of any of the terms, conditions, covenants, representations or warranties set forth in this Agreement (including, without limitation, the obligation not to use the Licensed Technology outside of the scope of the licenses granted herein). Licensee or CableLabs shall pay any and all losses, liabilities, damages, costs, fees, and expenses (including reasonable attorneys' fees) finally awarded against the other or its Indemnitees or paid in settlement of such Claims. The obligations of the indemnifying parties under this Section are conditioned on the Indemnitees giving the indemnifying parties: (a) prompt written notice of any Claim for which indemnification is sought but only to the extent that the failure to give such notice materially prejudices the indemnifying parties; (b) control of the defense and settlement of such Claim, provided however, that the indemnifying parties shall not be allowed to admit liability on behalf of the Indemnitees or to enter into any settlement or agreement obligating the Indemnitee(s) to pay money without such Indemnitee(s)' consent; and (c) reasonable assistance and cooperation in such defense, at the indemnifying parties' expense.

11. LIMITATION OF LIABILITY. EXCEPT IN THE CASE OF A BREACH OF SECTIONS 2, 6 OR 7, OR CLAIMS ARISING UNDER SECTION 10 OF THIS AGREEMENT (INCLUDING,

WITHOUT LIMITATION, USE OF THE LICENSED TECHNOLOGY OUTSIDE OF THE SCOPE OF THE LICENSE GRANTED HEREIN), IN NO EVENT SHALL ANY PARTY (INCLUDING CABLELABS, ITS LICENSORS (INCLUDING BUT NOT LIMITED TO POLYCIIPHER), LICENSEE (AND THEIR AFFILIATES), ANY CABLELABS MEMBER, OR ANY OTHER VENDOR) BE LIABLE TO THE OTHER PARTY, OR ANY THIRD PARTY BENEFICIARY, FOR ANY INDIRECT, INCIDENTAL, SPECIAL, CONSEQUENTIAL OR PUNITIVE DAMAGES IN CONNECTION WITH OR RELATING TO THIS AGREEMENT (INCLUDING LOSS OF PROFITS, USE, DATA, OR OTHER ECONOMIC ADVANTAGE), NO MATTER WHAT THEORY OF LIABILITY, EVEN IF SUCH PARTY HAS BEEN ADVISED OF THE POSSIBILITY OR PROBABILITY OF SUCH DAMAGES. Notwithstanding the foregoing, in the event of a material breach that is not cured within the time specified in Section 9, Licensee may be liable to CableLabs and/or Third Party Beneficiaries, but in no event will Licensee's liability to CableLabs and/or Third Party Beneficiaries under this Agreement and the OCAP Implementers License Agreement exceed \$5,000,000 per instance of breach. As used herein an "instance" shall be defined as a breach attributable directly or indirectly to one cause (including a series of similar problems related to a single cause) and may, for example, affect multiple models of devices sharing a common chassis.

12. THIRD PARTY BENEFICIARIES. Licensee agrees that Cable Operators and PolyCipher are Third Party Beneficiaries of this Agreement. Licensee agrees that Content Providers shall each be Third Party Beneficiaries of this Agreement only with regard to a breach of this Agreement by Licensee that results in any unauthorized copying, distribution, or modification of usage rights of Controlled Content. In any claim or action brought by a Third Party Beneficiary that is a Content Provider, reasonable attorneys' fees shall be awarded to the prevailing party. Such Third Party Beneficiaries may seek injunctive relief or, for material breaches, actual damages (up to the limits contained in Section 11) only after the occurrence of all of the following: (a) such Third Party Beneficiary has given to CableLabs written notice of the potential breach; (b) CableLabs has thoroughly evaluated the potential breach; (c) CableLabs has consulted with Licensee regarding the problem; (d) CableLabs has provided Licensee with a reasonable opportunity to cure the breach and such breach remains uncured for thirty (30) days following the date of such notice, or a longer period as reasonably determined by CableLabs pursuant to Section 9.4; and (e) CableLabs has informed all Cable Operators of such breach.

13. ADDITIONAL TERMS

13.1 Reports. Licensee shall provide to CableLabs a confidential, non-binding, aggregated production forecast of Host Devices made by Licensee hereunder ("Forecasts"). Such Forecasts will be aggregated with other similar licensees, and other licensees of the Licensed Technology so that Licensee's individual information is not identifiable. This aggregated information will be used solely to inform Cable Operators of the potential number of Host Devices entering the marketplace; CableLabs shall not, and Cable Operators shall be bound not to, use it for any other purpose. Licensee agrees to provide such monthly forecasts for a rolling five-month period for the term of this Agreement, plus five months. CableLabs acknowledges that the Forecasts may fluctuate and do not create any binding obligations. Licensee is not required under this Agreement to provide any information regarding its production or sales other than these aggregated production forecasts.

As between CableLabs and Licensee, the Forecasts are confidential and proprietary to Licensee. CableLabs shall not use or disclose the Forecasts in any manner whatsoever other than in connection with distribution of aggregated information to the Cable Operators as noted above. CableLabs shall implement and maintain security measures in order to keep the Forecasts confidential which are at least as rigorous as CableLabs employs for its own confidential

information. CableLabs may disclose Forecasts to its Affiliates, subcontractors, consultants, agents, employees, customers and representatives who have a need to know and an obligation to keep the Forecasts confidential.

In order to provide Service to a Certified Host Device, Licensee shall also provide to PolyCipher, or its designated agent such secure reports of PolyCipher chip and device identification as is called for in the Licensed Technology, the Digital Certificate Authorization Agreement and the Digital Keying Authorization Agreement. This will include: A unique identification number for the Qualified Secure Micro and Certified Transport Processor included in the Host Device; the serial numbers of the paired Secure Micro and Transport Processor chips; a unique identification number for the Host Device; and the serial number, model and firmware revision of the Host Device. These reports shall be considered Highly Confidential Information.

13.2 Most Favored Status. In the event that CableLabs enters into a DCAS Host License Agreement with another licensee and such other agreement has terms that are materially different from and more favorable to such other licensee than the terms in this Agreement are to Licensee, then Licensee shall have the option of amending this Agreement to reflect such material modification, *provided, however, that* if such other DCAS Host License Agreement contains other material modifications from the terms of this Agreement, Licensee also agrees be bound by such other modifications. CableLabs shall successively post to the OpenCable website (with redaction of company-specific information) all DCAS Host License Agreements entered into by CableLabs which have any term materially different from the terms of this Agreement.

13.3 Amendments. Except as otherwise provided in this Agreement, no change, modification, extension, termination or amendment of or to this Agreement, or any of the provisions or Exhibits herein contained, shall be valid unless made in writing and signed by duly authorized representatives of the parties hereto.

13.4 Assignment. This Agreement may be assigned or transferred by either party to any successor by merger, purchase, or transfer of all or substantially all of its business or that portion of its business to which this Agreement relates, or other form of corporate reorganization. This Agreement may also be assigned or transferred by CableLabs to an entity which controls, is controlled by, or under common control with CableLabs. No consent shall be required for the assignment of this Agreement to any wholly-owned subsidiary of Licensee. Except as set forth above, neither party may assign or sublicense any rights or delegate any duties under this Agreement in whole or in part without the other party's prior written consent (such consent not to be unreasonably withheld), and any such attempted assignment shall be void and of no effect. This Agreement shall be binding upon and inure to the benefit of each of the parties, their successors and permitted assigns.

13.5 Governing Law. This Agreement shall be governed and construed in accordance with the laws of the State of New York as applied to agreements made, entered into and performed entirely in New York and solely by New York residents.

13.6 Compliance with Laws. Licensee shall comply with all applicable laws and regulations, 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. This Section shall explicitly survive any termination of this Agreement.

13.7 Independent Contractors. The relationship of CableLabs and Licensee established by this Agreement is that of independent contractors. Nothing in this Agreement

should be construed to create a partnership, agency, joint venture, or employer-employee relationship between or among any of the parties. Neither party has the authority to assume or create any obligation, express or implied, on behalf of the other for any purpose whatsoever. This Agreement does not give either party the power to direct and control the day-to-day activities of the other.

13.8 Notices. 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 addresses listed on the first page of this Agreement, or to such other address that the receiving party may have provided for the purpose of notice in accordance with this Section.

13.9 Severability. If any provision of this Agreement is held to be invalid or unenforceable for any reason, the remaining provisions will continue in full force without being impaired or invalidated in any way, and the parties agree to replace any invalid provision with a valid provision that most closely approximates the intent and economic effect of the invalid provision.

13.10 No Waiver. No term or provisions hereof shall be deemed waived, and no breach excused, unless such waiver or consent is in writing and signed by the party claimed to have waived or consented. The waiver by either party of a breach of any provision of this Agreement will not operate or be interpreted as a waiver of any other or subsequent breach.

13.11 Injunctive Relief. Licensee acknowledges that material breach of this Agreement will cause CableLabs, and/or the Third Party Beneficiaries hereto, to suffer immediate and irreparable harm, damage for which money alone cannot fully compensate. Licensee therefore agrees that upon such material breach, CableLabs shall be entitled to entry of a temporary restraining order, preliminary injunction, permanent injunction or other injunctive relief, without posting any bond or other security, compelling Licensee to comply with such obligations. This paragraph shall not be construed as an election of any remedy, or as a waiver of any right available to either party under this agreement or the law, including the right to seek damages, nor shall this paragraph be construed to limit the rights or remedies available under applicable law for any violation of any provision of this Agreement.

13.12 Service Denial for Cable Services. For the avoidance of doubt, Licensee acknowledges that nothing in this Agreement shall prevent a Cable Operator from denying services to any individual Host Device, or otherwise preventing cable content from flowing to any individual device or set of devices built by Licensee hereunder. Notwithstanding, CableLabs shall notify Licensee of any such proposed use of service denial, of which CableLabs is aware, to a model or class of devices made by Licensee hereunder prior to the use of such service denial by a Cable Operator and facilitate discussions between Licensee and the Cable Operator to alleviate the circumstances giving rise to the Cable Operator's desire to deny such service; provided that no Cable Operator shall be restrained from immediately denying such service if it reasonably believes that Controlled Content is subject to an unreasonable risk of unauthorized access, copying, distribution, or modification of usage rights, or is in material breach of Section 2 or 7 above.

13.13 Entire Agreement. Licensee acknowledges that Licensee will be required to enter into additional agreements (including the OCAP Implementers License Agreement, a Digital

Certificate Authorization Agreement, and implementation of the requirements established under Section 6.1 of this Agreement) in connection with the manufacture of Host Devices. This Agreement, including all Exhibits hereto (which are hereby incorporated into and made a part of this Agreement), constitutes the final, complete and exclusive statement of the agreement between the parties with respect to the licensing of the Licensed Technology and supersedes any previous proposals, negotiations, or agreements, whether oral or written, made between the parties with respect to the licensing of the Licensed Technology.

EXHIBIT A

The Licensed Technology licensed under this Agreement includes:

CableLabs Specifications:

OpenCable DCAS Specifications – Host Device 2.5 Core Functional Requirements

OpenCable DCAS Specifications – DCAS System Overview Technical Report

DCAS Know How:

The DCAS Know How contained in:

DCAS Content Protection Specification

DCAS Authorized Service Domain - DVR Specification

DCAS Authorized Service Domain – Host Home Networking Specification

DCAS Host Software Requirements Specification

DCAS Pairing System Interface Specification

DCAS Pairing System Operations Guide

EXHIBIT B

Robustness Rules

Note: The terms of this Exhibit B do not apply with respect to Prototypes, and only apply to Licensed Components to the extent they are incorporated into Host Devices. Licensed Products must comply with the terms of this Exhibit B.

1. Construction.

1.1 Generally. The Licensed Products as shipped shall meet the Compliance Rules and shall be designed and manufactured in a manner to effectively frustrate attempts to circumvent or modify such Licensed Products to defeat the Compliance Rules or functions of the Licensed Technology. The Secure Micro within Host Devices must provide Common Criteria EAL Level 5+ security as and when required by PolyCipher to protect keys, entitlements and security technologies in the security microprocessor. Licensed Products shall be designed and manufactured in a manner to effectively frustrate attempts to compromise the security methods for the Secure Download system known as DCAS or the Conditional Access Systems (CAS) delivering content protection keys.

1.2 Licensed Product Defeating Functions. Licensed Products shall not include:

- (a) switches, buttons, jumpers, specific traces that can be cut or place the Licensed Product 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 security technology, content protection technologies, analog or digital protection systems, CGMS-A/RCI/APS signaling, output restrictions, recording limitations, redistribution limitations or other mandatory provisions of the Licensed Technology 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.

1.3 Transport Processor Functions

Each Certified Host Device shall include a Qualified Transport Processor. The Qualified Transport Processor shall include:

- (a) a non-readable and non-writable Bootloader which shall exist in internal read-only memory (ROM) or locking flash memory (as used herein a Bootloader shall mean secure code implemented in accordance with the Bootloader API Specification and licensed from an authorized provider, and shall at all times operate in accordance with the DCAS Security Specification);
- (b) all code loaded into the transport chip processor must be authenticated using digital signatures utilizing a predefined key that is stored in non-volatile Read-Only Memory (ROM); and
- (c) a Security interface between the Qualified Transport Processor and the Qualified Secure Micro as specified in the DCAS Host Security Specification.

1.4 Secure Micro Functions

Each Certified Host Device shall include a Qualified Secure Micro and operate in accordance with the DCAS Security Specification. The Qualified Secure Micro shall include:

- (a) externally non-readable and non-writable Bootloader, security primitives, and other functions which shall exist in internal read-only memory (ROM) or locking flash memory;
- (b) all code loaded into the Qualified Secure Micro must be authenticated using digital signatures and a secure Network Protocol and Messaging as defined in the DCAS Host Security Specification;
- (c) internal tamper resistant protection of keys as defined in the secure micro specifications; and
- (d) intrusion detection and alarm circuitry to erase keys or protect extraction of device keys and other secrets as defined in the secure micro specifications.

1.5 Keep Secrets.

- (a) Licensed Products shall be designed and manufactured in a manner to effectively frustrate attempts to discover or reveal:
 - (i) the One Time Programmable (OTP) values (unique numbers), of a specified bit length, assigned to each Certified Host Device, Qualified Transport Processor and Qualified Secure Micro, or any of the numbers or values used in the process for encryption, decryption, digital signatures, or key exchanges of Controlled Content (collectively, “**Keys**”), and
 - (ii) the methods and cryptographic algorithms used to generate such Keys.
- (b) Host Devices shall be designed and manufactured with an OTP key for setting a secure channel to decrypt keys received from a Qualified Secure Micro.

2. Documents and Robustness Certification Checklist.

2.1 Before releasing any Licensed Product, 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 a Host Licensee in performing tests covering certain important aspects of this Exhibit B and for providing a *required* documentation record for submission to CableLabs as part of Certification. Inasmuch as the Robustness Certification Checklist does not address all elements required for the manufacture of a compliant Host Device, a Host Licensee is strongly advised to review carefully the Licensed Technology for the implementation in question, the Compliance Rules and this Exhibit B so as to evaluate thoroughly both its testing procedures and the compliance of its Licensed Products. Licensee is strongly advised to utilize commercial test tools to meet the requirements of the Licensed Technology, the Compliance Rules and this Exhibit B or to consult known device security experts in the development of an ASIC security technology or similar technology for Licensed Products.

2.2 Licensee specifically acknowledges and agrees that it must provide copies of the Compliance Rules, the Robustness Rules, and, for Host Licensees, the Robustness Certification Checklist and the Licensed Technology for the Host Profile in question to its responsible supervisors of product design and

manufacture in such manner and at such times as to effectively induce compliance with such materials and , for Host Licensees, completion, signing and submission of the Robustness Certification Checklist.

3. Controlled Content Paths.

3.1 Licensed Products shall not allow Controlled Content to be available on or through outputs other than those specified in the Compliance Rules.

3.2 Licensed Products shall not allow Controlled Content to be present in compressed form on any User Accessible Bus (as defined below) unless encrypted and secured from unauthorized interception to the level of protection specified in Section 4(e)(i) and 4(e)(ii).

3.3 Licensed Products shall not allow Controlled Content to be present in uncompressed form on any User Accessible Bus (as defined below) unless encrypted and secured from unauthorized interception to the level of protection specified in Section 4(e)(i).

3.4 Licensed Products 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).

3.5 Licensed Products 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).

3.6 Notwithstanding the foregoing:

(a) compressed or uncompressed audio data may be output in the clear via the S/PDIF connector to an external Dolby Digital decoder or PCM receiver; and

(b) no restrictions are placed on the use or output of navigation data contained in the Program Association Tables (PAT) or the Program Map Tables (PMT).

3.7 A “User Accessible Bus” means a data bus which is designed for end user upgrades or access such as PCI and PCI Express 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.

3.8 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).

4. Methods of Making Functions Robust. Licensed Products 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 Licensed Product that perform authentication, encryption, decryption, digital signatures, key exchanges, and the video 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 functional portions of the Licensed Product 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 Licensed Product that implements a part of the Licensed Technology 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 Licensed Product 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 Sections 1.3-1.5 by any reasonably secure 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 Secure Memory Management (in the security hardware device) to disguise and hamper attempts to discover the approaches used and any secrets, Keys, Key management techniques, or Key generation methods;

(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 secure hashing function that is further encrypted with a private key (a hardware based digital signature); and

(iii) Meet the level of protection outlined in Section 4(e) below.

(c) **Hardware.** Any portion of the Licensed Product that implements a part of the Licensed Technology 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 Licensed Product 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 Licensed Product or Licensed Component and such instructions or data are not accessible to the end user through the Licensed Product or Licensed Component. Such implementations shall:

(i) Comply with Sections 1.3-1.5 by any reasonably secure method including but not limited to: embedding Keys, Key generation methods and the cryptographic algorithms in silicon circuitry (as defined with countermeasures defined in the applicable Licensed Technology) or firmware that cannot 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 the Licensed Technology, the Agreement or in Licensed Products would pose a serious risk of damaging the Licensed Product 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 is required to be designed in this manner; and

(iii) Meet the level of protection outlined in Section 4(e) below.

(d) **Hybrid.** The interfaces between hardware and software portions of a Licensed Product 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 cryptographic functions of the Licensed Technology (maintaining the confidentiality of Keys, digital signatures, Key management techniques, Key generation methods, encryption, decryption, authentication, and the cryptographic algorithms,

conformance to the Compliance Rules and preventing Controlled Content that has been unencrypted from being copied or unauthorized viewing) shall be implemented in a way that they:

(i) Cannot be defeated or circumvented merely by using 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, Smartcard readers, 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, bus analyzers, ROM emulators, forced ion beam devices, laser for local light attacks, electron microscopes, 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 Licensed Product 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 Licensed Product 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 Licensed Product and shall only distribute Licensed Products that are compliant with this Exhibit B in view of the then-current circumstances.

5. Update Procedure.

Security technologies will continue to advance. As such CableLabs will meet and confer with Cable Operators, PolyCipher, equipment manufacturers and Content Providers on a regular basis to revise and update these rules and incorporate new countermeasures to ensure that the Licensed Products remain secure against tampering and reverse engineering directed toward defeating the Licensed Technology, the Compliance Rules, and any protection scheme incorporated therein intended to protect Controlled Content against to unauthorized access, copying, distribution, or modification of usage rights.

EXHIBIT B-1

ROBUSTNESS CHECKLIST

Notice: Completion of this Checklist is intended as part of the correct implementation of the Robustness Rules for hardware and software implementations of the DCAS Specifications in a Licensed Product. This Checklist does not address all aspects of the DCAS 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 Licensed Technology, Compliance Rules or Robustness Rules could result in a breach of the DCAS Host License Agreement and appropriate legal action taken by CableLabs or other parties under the DCAS Host 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 Licensed Product 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 DCAS Specifications or Compliance Rules can be defeated or by which Controlled Content can be exposed to unauthorized copying or redistribution?
2. Has the Licensed Product 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 or redistribution?
3. Has the Licensed Product 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, CGMS-A/RCI/APS signaling, recording limitations, redistribution limitations, or other mandatory provisions of the DCAS Specifications or Compliance Rules?
4. Does the Licensed Product 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 Licensed Product have service menus, service function, or service utilities that can turn off any analog protection systems, output restrictions, recording limitations, redistribution limitations, or other mandatory provisions of the DCAS 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 the DCAS Technology (including compliance with the Compliance Rules and the DCAS Specifications).

6. Does the Licensed Product 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 Licensed Product protects the confidentiality of all keys.
8. Explain in detail how the Licensed Product protects the confidentiality of the confidential cryptographic algorithms used in the Licensed Technology.

9. If the Licensed Product 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, copying, and/or redistribution as required in Section 4(a) of the Robustness Rules.

10. Are any Licensed Technology functions implemented in Hardware?

If Yes, complete hardware implementation questions.

11. Are any Licensed Technology functions implemented in Software?

If Yes, complete software implementation questions.

SOFTWARE IMPLEMENTATION QUESTIONS

12. In the Licensed Product, 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 Licensed Product, describe the method used to obfuscate the confidential cryptographic algorithms and Keys used in the DCAS Technology and implemented in software.

15. Describe the method in the Licensed Product by which the intermediate cryptographic values (e.g., values created during the process of authentication between modules or devices within a Licensed Product) 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 DCAS Technology functions implemented in software.

17. Describe the method by which the Licensed Product 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 DCAS Technology functions, and describe the method and results of the test.

19. Please explain how code images for your products are digitally signed and managed as they are deployed for production.

20. Please describe how digital signature keys are managed in your fabrication process and how the code signing ceremonies are managed before software is released to production and deployed into the field.

HARDWARE IMPLEMENTATION QUESTIONS

- 21.** In the Licensed Product, describe the method by which all Keys are stored in a protected manner and how their confidentiality is maintained.
- 22.** Using the grep utility or equivalent, are you unable to discover any Keys in binary images of any persistent memory devices?
- 23.** In the Licensed Product, describe how the confidential cryptographic algorithms and Keys used in the Licensed Technology have been implemented in silicon circuitry or firmware so that they cannot be read.
- 24.** Describe the method in the Licensed Product by which the intermediate cryptographic values (e.g., values created during the process of authentication between modules or devices within a Licensed Product) are created and held in a protected manner.
- 25.** Describe the means used to prevent attempts to replace, remove, or alter hardware elements or modules used to implement Licensed Technology functions?
- 26.** In the Licensed Product, does the removal or replacement of hardware elements or modules that would compromise the content protection features of Licensed Technology (including the Compliance Rules, the DCAS Specifications, and the Robustness Rules) damage the Licensed Product so as to render the Licensed Product unable to receive, decrypt, or decode Controlled Content?
- 27.** Does the Licensed Product contain a Secure Micro that is certified to NIST Common Criteria EAL Level 5 and contain the PolyCipher authorized bootloader? What version of the bootloader is installed?
- 28.** Does product implement a custom Transport chip to decrypt video from a live MPEG-2, DOCSIS channel, or PVR?
- 29.** If Yes, Does this chip contain One Time Programmable keys and configuration data (OTP) for securing keys between the security processor and the Transport Chip? Please explain the methods implemented for protecting the OTP, tunnel key and content keys.
- 30.** Does this chip have the ability to receive and validate digitally signed or encrypted messages to securely control the enabling and disabling of the transport decryption and DVR encryption from messages sent from the security processor?
- 31.** Are the circuit traces between the security processor and the Transport Chip buried in the board and inaccessible or probing?
- 32.** Did your company or a contracted company develop the Secure Micro Driver and client security software and firmware? Please explain how the security software, build process, and design specifications are controlled to prevent unauthorized distribution.
- 33.** In the implementation that you have developed, does the transport processor have the MPEG decoder or Advanced Video Codec (AVC) built into the single chip solution? If no, how do you protect the compressed digital video when it exits one chip and enters the next chip for decoding?

34. Please explain how keys are injected into devices into your factory fabrication process. If keys are present in the chips that you purchase, please explain how you track these chips and related keys as they are received, handled, manufactured into products and leave your facility.

Notice: This checklist does not supersede or supplant the DCAS Specifications, Compliance Rules, or Robustness Rules. The Company and its Test Engineer are advised that there are elements of the DCAS Specifications, DCAS Know-How, 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

EXHIBIT C

COMPLIANCE RULES

Note: The terms of this Exhibit C apply to Certified Host Devices and components thereof, and not to Prototypes.

Licensed Products, 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.

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.

1.3 “Constrained Image Trigger” or “CIT” means the field or bits, as described in the draft Amendment to SCTE 41 2003 set forth in Exhibit C-1 hereto, used to trigger the output of a “Constrained Image” in the High Definition Analog Output of Licensed Products.

1.4 “Controlled Content” means content that has been transmitted from the headend with: (a) the Encryption Mode Indicator (“EMI”) bits set to a value other than zero, zero (0,0); (b) the EMI bits set to a value of zero, zero (0,0), but with the RCT value set to one (1); or (c) the copy control information (CCI) otherwise marked to indicate restrictions on access, copying, redistribution, or usage rights.

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,” that may be amended from time to time, as supplemented (but not superseded) by the DCAS Specifications.

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,” that may be amended from time to time, as supplemented (but not superseded) by the DCAS Specifications.

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-C.

1.9 “RCI” or “Redistribution Control Information” means the field or bits as described in CEA-805-B.

1.10 “RCT” or “Redistribution Control Trigger” means the field or bits, as described in the draft amendment to SCTE 41 2003 as described in Exhibit C-1 hereto, 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 or Y,R-Y,B-Y 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.

2. Outputs

2.1 General. Licensed Products shall not output content, or pass content received through the Service to any output, except as permitted in this Section 2. 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-user-accessible outputs that are 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 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), as defined in the DCAS Specifications.

2.2 Standard Definition Analog Outputs. Licensed Products 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:

(a) In any transmission through an NTSC RF, Composite, YUV, Y,Pb,Pr or Y,R-Y,B-Y format analog output (including an S-video output and including transmissions to any internal copying, recording or storage device) of a signal, Licensed Products shall generate the appropriate copy control signaling (CGMS-A, RCI or RCD, and APS) in response to the copy control information (CCI) and the analog copy protection signals in response to the instructions provided in the APS bits of the copy control information (CCI), if any, and in accordance with the DCAS Specifications (i.e. trigger bits for Automatic Gain Control and Colorstripe copy control systems, as referenced below). These requirements also apply to the standard definition analog output of downconverted Controlled Content that, when originally received, was High Definition. The technologies that satisfy this condition and are authorized hereunder are limited to the following:

(i) For 480i (interlace scan) RF, Composite or S-Video:

¹ RCT may not be set to restrict redistribution except in content that could lawfully be marked Copy One Generation but is instead marked Copy Freely.

1. the Automatic Gain Control and Colorstripe copy control systems (specified in the document entitled “Specification of the Macrovision Copy Protection Process for STB/IRD Products” Revision 7.1.S1, October 1, 1999) in response to the instructions provided in the APS bits of the copy control information (CCI), if any, (i.e., trigger bits for Automatic Gain Control and Colorstripe copy control systems); and
2. CGMS-A and APS signaling, as defined in CEA-608-C for inclusion on Line 21 of field 2. RCD signaling as defined in CEA-608-C specification for inclusion on Line 21 of field 2. For avoidance of doubt, the “copy control signaling” is independent of the requirement to appropriately apply APS “copy protection signals” using the Automatic Gain Control and Colorstripe systems as defined in Section 2.2(a)(i)(1) above.

(ii) For 480i (interlace scan), YUV, Y,Pb,Pr or Y,R-Y,B-Y outputs:

1. the Automatic Gain Control and Colorstripe copy control systems (specified in the document entitled “Specification of the Macrovision Copy Protection Process for STB/IRD Products” Revision 7.1.S1, October 1, 1999) in response to the instructions provided in the APS bits of the Copy Control Instruction message, if any, (i.e., trigger bits for Automatic Gain Control and Colorstripe copy control systems); and
2. CGMS-A and APS signaling, as defined in CEA-608-C for inclusion on Line 21 of field 2. RCD signaling as defined in CEA-608-C specification for inclusion on Line 21 of field 2. For avoidance of doubt, the “copy control signaling” is independent of the requirement to appropriately apply APS “copy protection signals” using the Automatic Gain Control and Colorstripe systems as defined in Section 2.2(a)(i)(1) above.

(iii) For 480p (progressive scan) YUV, Y,Pb,Pr or Y,R-Y,B-Y outputs:

1. the Automatic Gain Control and Colorstripe copy control systems (specified in the document entitled “Specification of the Macrovision AGC Copy Protection Waveforms for DVD Applications with 525p (480p) Progressive Scan Outputs, Revision 1.1.1 (August 15, 2002)”) in response to the instructions provided in the APS bits of the copy control information (CCI), if any, (i.e., trigger bits for Automatic Gain Control and Colorstripe copy control systems);
2. CGMS-A, RCI and APS signaling as defined in CEA-805-B. For avoidance of doubt, the “copy control signaling” of APS is independent of the requirement to appropriately apply APS “copy protection signals” using the Automatic Gain Control and Colorstripe systems as defined in Section 2.2(a)(iii)(1) above.

2.3 High Definition Analog Outputs. Licensed Products 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.

(a) Such Licensed Products shall be designed and manufactured to be able to constrain the resolution of Controlled Content that is High Definition to be output through a connection capable of transmitting content in High Definition Analog Form, to a Constrained Image when signaled by the Constrained Image Trigger in the copy control information (CCI).

(b) If a Licensed Product has an output capable of transmitting content in High Definition Analog Form, it is required to have one or more protected digital output(s), defined in Section 2.4 below, for outputting Controlled Content.

(c) In any transmission through a component YUV, Y,Pb,Pr, or Y,R-Y,B-Y format analog output (including transmissions to any internal copying, recording or storage device) of a signal including Controlled Content, Licensed Products shall generate the appropriate copy control signaling (CGMS-A, RCI, and APS) in response to the copy control information (CCI) and in accordance with the DCAS Specifications. These requirements also apply to the high definition analog output of upconverted Controlled Content that, when originally received, was Standard Definition. The technologies that satisfy this condition and are authorized hereunder are limited to the following:

(d) For 720-line progressive scan video and 1080-line interlace scan video, Licensed Products shall generate CGMS-A, RCI and APS signaling as defined in CEA-805-B.

(e) All Licensed Products shall generate and propagate CGMS-A signals for all HD analog outputs as specified above; but shall not be required to respect the CGMS-A trigger unless required by appropriate legislation or regulation.

2.4 Digital Outputs. Licensed Product 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. Licensed Product may output Controlled Content, and pass Controlled Content to an output, in digital form over IEEE 1394 interfaces as specified by the DCAS Specifications, only if such output is protected by DTCP. The DTCP source function in the Licensed Product must support DTCP “Full Authentication,” and may additionally support DTCP “Restricted Authentication.” In addition, the DTCP source function is required to: (a) process all validly received DTCP System Renewability Messages (“SRM”) [as received via ATSC A/98](#); (b) convey downstream all validly received System Renewability Messages supported by DTCP through its 1394 with DTCP output; and (c) 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 as defined in the DCAS 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. If required by the applicable license for DTCP, content that is *not* Controlled Content shall be output on the IEEE 1394 output without DTCP protection.

2.4.2 DVI/HDMI with HDCP. If Licensed Product includes any form of the Digital Visual Interface (“DVI”) output, including, without limitation, High Definition Multimedia Interface (“HDMI”), such Licensed Product (a) must pass all validly received HDCP System Renewability Messages (“SRM”) [as received via ATSC A/98](#) to the HDCP source function; and (b) 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 DVI or HDMI outputs; (ii) processing of validly received SRMs associated with such content, if any, has occurred, as defined in the HDCP specification, [as received via ATSC A/98](#); and (iii) there is no HDCP device on such output whose Key Selection Vector is in such 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 HDCP Specification or the HDCP License Agreement.

2.4.3 DTCP-IP. Licensed Product 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 Licensed Product is required to: (a) process all valid DTCP System Renewability Messages (“SRM”) received via ATSC A/98; and (b) 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 Exhibit C-1. 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 Other Digital Outputs. For digital outputs not specified above, Licensed Products shall not transmit Controlled Content through such digital outputs until such time as this Exhibit C is amended by CableLabs to permit same. From time to time, CableLabs may approve additional digital outputs and/or content protection technologies on a reasonable and nondiscriminatory basis, and add such provisions to this Section. Licensed Product may output content received through the Service, which is not Controlled Content, through digital outputs other than the outputs listed above.

2.5 Watermark Non-Interference. Commencing eighteen (18) months after the existence of a Consensus Watermark, Licensee: (i) shall, when selecting among technological implementations for product features for Licensed Products 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 Licensed Products 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 Licensed Products or Licensed Components the primary purpose of which is to strip, obscure or interfere 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 Licensed Products or Licensed Components the primary purpose of which is to strip, obscure or interfere with such Consensus Watermark in Controlled Content that has been decrypted.

Provided Licensee complies with the foregoing provisions of this Section 2.5, this Section 2.5 shall not prohibit a Licensed Product 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 NTSC 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.** Licensed Products, including, without limitation, Licensed Products 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.** Licensed Products 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.** Licensed Products shall not copy, record or store Controlled Content that is designated in the copy control information associated with the Controlled Content as having been copied but not to be copied further (“Copy No More”), except as permitted in Section 3.2 or 3.5.2 of this Exhibit C.
- 3.4 Copy Never.** Licensed Products, 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 of this Exhibit C or by the following:

- 3.4.1** Such Licensed Products with integrated recording capability may internally store such content, including for the purpose of trick play or pausing the program, when instructed by OCAP if the stored content is: (a) securely bound to the Licensed Product doing the recording so that it is not removable therefrom; (b) not itself subject to further temporary or other recording or copying within or outside the Licensed Product before it is rendered unusable; (c) internally stored in an encrypted manner that securely binds the content so that it can only be decrypted by the Licensed Product receiving and storing such content; and (d) encrypted using an algorithm that provides no less security than 128-bit Advanced Encryption Standard (“AES”) or 112-bit Triple DES Encryption Algorithm (“3DES”); and (e) obliterated or otherwise rendered unusable no more than ninety (90) minutes (or after a stated period of time as outlined in Section 3.4.2) from the time of initial reception by the Licensed Product on a frame-by-frame, minute-by-minute, megabyte-by-megabyte basis, but in no event shall such unit of data exceed one (1) minute of content.

In addition, such internal recording of content is permitted provided the integrated recording capability requirements are implemented in a manner consistent with the Robustness Rules set forth in Exhibit B to avoid circumvention of such restrictions and the playback of such stored content follows the Compliance Rules set forth in this Exhibit C, including, without limitation, the output rules.

- 3.4.2** Licensed Products with integrated recording capability manufactured in accordance with Section 3.4.1 above shall be designed and manufactured to be able, when required by the OCAP application, to obliterate or render unusable the stored content after a stated period of time identified by the OCAP application, on a frame-by-frame, minute-by-minute, megabyte-by-megabyte basis, but in no event shall such unit of data exceed one (1) minute of content.

3.5 Copy One Generation.

3.5.1 Licensed Products with integrated recording capability 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 Section 3.4.1 and 3.4.2 of this Exhibit C, provided that the copy is scrambled or is otherwise made secure using one or more of the following methods, in each case using a form of copy protection that is identified by an amendment to this section 3.5, such that no further useable copies may be made thereof, or they may treat such Controlled Content as “Copy Never”:

(a) the copy is encrypted in a manner that securely binds the content to the Licensed Product receiving the content so that the recording is not removable, can only be decrypted by the Licensed Product receiving and recording such content, and meets the requirements outlined in Sections 3.4.1(a), (b), (c) and (d) of this Exhibit C;

(b) the copy is encrypted in a manner that securely binds the content to the removable media, so that no further useable copies may be made thereof and meets the requirements outlined in Section 3.4.1(b), (c), and (d) of this Exhibit C; or

(c) the copy is protected using an encryption-based, one-generation copy protection technology approved by CableLabs in the future.

Any copies made of Copy One Generation content by an integrated recording function in a Licensed Product must be remarked to indicate that the copy shall not to be further copied (“Copy No More”). In addition, such recording of content as defined in Section 3.5.1 (b) and (c) is permitted provided the integrated recording capability requirements are implemented in a manner consistent with the Robustness Rules set forth in Exhibit B to avoid circumvention of such restrictions and the playback of such stored content follows the Compliance Rules set forth in this Exhibit C, including, without limitation, the output rules.

3.5.2 A Licensed Product 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 Licensed Product as “Copy One Generation”; (c) the Controlled Content is output over a protected output in accordance with Sections 2.2, 2.3 or 2.4 of this Exhibit C; (d) before the Move is completed, the originating Licensed Product 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 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 of this Exhibit C. Multiple moves consistent with these requirements are not prohibited.

- 3.5.3** In accordance with Section 3.5.1, Licensed Products may make a copy of Controlled Content that is marked in the CCI as “Copy One Generation” using VCPS in accordance with 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.

3.6 Copy Control Not Asserted, Redistribution Controlled.

3.6.1 Licensed Products with integrated recording capability may make copies of Controlled Content that has been transmitted from the headend with the EMI bits set to a value of zero, zero (0,0), and the RCT value set to one (1) (“Copy Control Not Asserted, Redistribution Controlled”), provided that such copies are scrambled or are otherwise made secure using one or more of the following methods, in each case using a form of copy protection that is identified by an amendment to this section 3.6, such that no further redistribution may be made thereof, or they may treat such Controlled Content as “Copy Never”:

- (a) the copy is encrypted in a manner that securely binds the content to the Licensed Product receiving the content so that the recording is not removable, can only be decrypted by the Licensed Product receiving and recording such content, and meets the requirements outlined in Sections 3.4.1(a), (b), (c), and (d) of this Exhibit C;
- (b) the copy is encrypted in a manner that securely binds the content to the removable media and meets the requirements outlined in Section 3.4.1(b) and (c) of this Exhibit C; or
- (c) the copy is protected using an encryption-based, secure recording technology that supports redistribution content control that may be approved by CableLabs in the future.

Any copies of “Copy Control Not Asserted, Redistribution Controlled” content made by an integrated recording function in a Licensed Product must be marked “Copy Control Not Asserted, Redistribution Controlled.” In addition, such recording of content as defined in Section 3.6.1 (b) and (c) is permitted provided the integrated recording capability requirements are implemented in a manner consistent with the Robustness Rules set forth in Exhibit B to avoid circumvention of such restrictions and the playback of such stored content follows the Compliance Rules set forth in this Exhibit C, including, without limitation, the output 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.

EXHIBIT C-1

CONSTRAINED IMAGE TRIGGER & REDISTRIBUTION CONTROL TRIGGER

The Constrained Image Trigger and Redistribution Control Trigger are 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 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 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. Five Six of the eight bits are defined. The remaining three 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	<u>RCT</u>	<u>CIT</u>	APS1	APS0	EMI1	EMI0
Host interprets as	rsvd	rsvd	<u>RCT</u>	<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 bit were equal to 1.

All references to CCI bits received from the Card shall be deemed to be references to CCI bits received from the headend.

EXHIBIT D

OPENCABLE CHANGE PROCESS

OVERVIEW

As OpenCable™ specifications are ISSUED, they become subject to the formal Change Process that is summarized below.

This process can be initiated by anyone with an interest in the specification at any time during the life of the issued specification. Engineering Change Requests (ECRs) should be submitted electronically to opencable-ec@cablelabs.com using the ECR form available at https://www.cablelabs.com/doczone/opencable/requirements/ecs/DocZoneFolder_view

If Licensee is claiming any intellectual property rights in an ECR submission, such rights should be specifically identified so that such property may be treated appropriately.

Due to the large numbers of vendors that have expressed interest in OpenCable documents, vendors should be aware that the OpenCable staff will not be able to provide individual responses to each vendor's ECR. Receipt of ECR submissions will be confirmed by email, either directly or by copying the author on the submission of the ECR to the appropriate OpenCable Working Group. Please be assured that all ECRs will be duly considered. Final disposition of ECRs is at the sole discretion of the OpenCable MSO Technical Review Team.

Upon receipt of an ECR, it will be assigned to the appropriate OpenCable Working Group comprising vendors, MSOs, and CableLabs staff. Discussions of the Working Group may be held either via e-mail or teleconference. The goal of the Working Group discussions are to clarify any issues related to the ECR, identify impact on the specification and testing regime, make changes to the ECR or submit additional ECRs, and agree upon final wording for the ECO

If a consensus is reached regarding the ECR, an Engineering Change Order (ECO) will be issued to all participants in the OpenCable Project that have executed the Confidential Information Access Agreement via email reflector (over 500 companies). In order to make this process successful, participants must monitor the OpenCable reflectors to ensure that the proposed changes, and discussions/subsequent changes are for the greater good of the industry and not for any one particular vendor company. Upon approval of the ECO by the OpenCable MSO Technical Team, an Engineering Change Notice (ECN) is issued.

THE DIAGRAM AND OUTLINE ON THE FOLLOWING PAGES PROVIDES AN OVERVIEW OF THE ECR, ECO, ECN PROCESS. THIS PROCESS IS SUBJECT TO CHANGE AS REASONABLY DETERMINED BY CABLELABS.

**CableLabs(
OpenCable™ Engineering Change Request**

EC TRACKING INFORMATION (TO BE COMPLETED BY CABLELABS ONLY)

Engineering Change Identifier			
Affected Spec			
ECR Posting Date		Comment Period End Date	N/A for ECRs
ECO Date		Comment Period End Date	
ECN Date			
Effective Date/Cert Wave			
Severity (check one)	Priority -	High FORMCHECKBOX	
		Normal FORMCHECKBOX	
		Low FORMCHECKBOX	

AUTHOR INFORMATION

Primary Author	
Company	
Address	
City, State Zip	
Country	
Phone	
Fax	
E-mail Address	
Additional Authors/Contributors	
Date sent to CableLabs	
Date of Revision Request -	
Brief Revision Description -	

SPECIFICATION CHANGE DETAILS

Affected Specification To obtain latest spec #, click here: http://www.opencable.com/specifications/ Please include the spec code – i.e. OC-SP-HOST-CFR-Ixx-yyymmdd)	
Type of Change - Request contains technical changes Yes <input type="checkbox"/> No <input type="checkbox"/>	
Technical changes may require a vendor to change the design of the product. Editorial changes are points of clarification or clean-up but would not under any circumstances require a change to the product. <i>Note: If the ECR contains changes of both types, please identify the type of change in the text below prior to each change.</i>	

ONE-SENTENCE SUMMARY OF PROPOSED ENGINEERING CHANGE -

DETAILED PROBLEM DESCRIPTION -

PROPOSED SPECIFICATION CHANGES (include section number, title, and paragraph. This section is only for changes affecting text and graphics in specification, a separate section is provided below for changes to APIs/java code files in the Exhibits.)

CHANGE #1 – PLEASE INDICATE WHETHER TECHNICAL OR EDITORIAL: _____

ORIGINAL SPEC TEXT:

NEW SPEC TEXT:

CHANGE #2 – PLEASE INDICATE WHETHER TECHNICAL OR EDITORIAL: _____

ORIGINAL SPEC TEXT:

NEW SPEC TEXT:

PROPOSED OCAP API/JAVA SOURCE CODE CHANGES (include API/java file name, cut and paste old code and new code, make sure you have checked the code to ensure it compiles correctly) -

CHANGE #1 – PLEASE INDICATE WHETHER TECHNICAL OR EDITORIAL: _____

ORIGINAL JAVA CODE (source code available on LiveLink at <http://livelink.cablelabs.com/Livelink/livelink.exe?func=ll&objId=1593714&objAction=browse&sort=name>):

NEW JAVA CODE:

CHANGE #2 – PLEASE INDICATE WHETHER TECHNICAL OR EDITORIAL: _____

ORIGINAL JAVA CODE:

NEW JAVA CODE:

PICS CHANGE DETAILS
(required before advancing to ECO)

PICS	
------	--

document affected	
Device affected (Host/POD)	

PROPOSED PICS CHANGES

Change #1

ORIGINAL TEST CASE TEXT:

NEW TEST CASE TEXT:

End of Request

EXHIBIT E

CHANGE PROCESS

Issued PolyCipher Specifications are subject to the formal PolyCipher Change Process that is summarized below.

This process can be initiated with an Engineering Change Requests (ECR) by any DCAS Participant licensed to use the Specification at issue.

Any IPR included in an ECR is governed by the IPR Provisions of the Licensee's applicable DCAS Technology License, which includes a Reciprocal Non-Assertion Agreement.

Licensees should be aware that the PolyCipher staff will not be able to provide individual responses to each Licensee's ECR. Receipt of ECR submissions will be confirmed by email. Please be assured that all ECRs will be duly considered. Final disposition of ECRs is at the sole discretion of PolyCipher.

Upon receipt of an ECR, it will be assigned to the appropriate PolyCipher Working Group comprising Licensees, MSOs, and PolyCipher staff. Discussions of the Working Group may be held either via e-mail or teleconference. The goal of the Working Group discussions are to clarify any issues related to the ECR, identify impact on the specification and testing regime, make changes to the ECR or submit additional ECRs, and agree upon final wording for the ECO.

If a consensus is reached regarding the ECR, an Engineering Change Order (ECO) will be issued to all DCAS Participants licensed to use the Specification at issue. Participants are responsible for monitoring any applicable PolyCipher reflectors for proposed changes and discussions. Upon approval of the ECO by PolyCipher, an Engineering Change Notice (ECN) is issued.

This process is subject to change as reasonably determined by PolyCipher.