

<tru2way> HOST DEVICE LICENSE AGREEMENT

1 JULY 2010

Overview

Innovation. The primary goal of tru2way technology is to promote innovation in consumer electronics devices, innovation in content and programming, and innovation in the cable network and in cable services.

For consumer electronics (CE) devices, tru2way technology enables and encourages retail devices to innovate. While operating in a defined CE Mode, tru2way devices can obtain linear basic, expanded basic, and premium cable programming (including HD and switched digital content) and combine that with content from other sources such as movies from the Internet, digital over the air broadcast, DBS, DVD, DVR, or other sources, all integrated into a guide or user interface designed by the CE manufacturer. In this CE Mode, there is no cable “monitor application” that controls the presentation of services to the user or the allocation of resources.

Tru2way technology provides a common platform that enables retail devices to receive--in one nationally standard way--the wide variety of video-on-demand services, interactive program guides, and other interactive features (such as StartOver and LookBack) that cable systems deliver through the many divergent network technologies, and deliver these cable services through a variety of retail devices. Tru2way also provides content owners and programmers a nationwide common platform for adding “write once, run anywhere” interactive applications into their content for national distribution (e.g., voting, polling, gaming, and interactive advertising). Developers may also use tru2way as a nationwide platform for innovation in interactive services and applications.

Tru2way Benefits Everyone

Consumers can enjoy a wealth of TV program innovations, convenient navigation features, viewing enhancements, interactive services and cross-platform sharing of content.	Application Developers have an exciting opportunity to create new interactive services that can be deployed seamlessly to millions of customers.
Device Makers may expand capabilities of digital TVs, portable game players and mobile phones to enable tru2way services to work both in and out of the home.	Content Holders add value to their content by using the tru2way platform to enhance their relationship with viewers through a variety of interactive services.
Retailers may sell more products by increasing consumer demand for products that offer innovative new services.	Advertisers have new ways for viewers to easily interact with commercials while leveraging more platforms to extend the reach of their message.
TV Networks and TV Programmers can explore new techniques to build viewer loyalty while expanding partnerships with sponsors to enhance interactive advertising.	Cable Operators have a national platform for delivery of interactive services, speeding delivery to customers and providing more opportunities for convergence of content across video, voice and Internet platforms.

The key elements of the <tru2way> Host Device License Agreement include:

- **tru2way Specifications.** At the core of a tru2way device is a **Java**-based middleware. A common middleware enables Content Owners, programmers, and Cable Operators to develop and deploy interactive applications nationwide, on disparate cable networks, to any tru2way device. The tru2way Java platform is also flexible in enabling device manufacturers to run their own tru2way native applications. The tru2way middleware is based on a core international standard adopted by the ITU, and used by similar standards bodies and technology consortia including Blu-Ray Disc, ATSC U.S. Broadcasters (ACAP), Broadcasters in Europe (MHP), Japan (ARIB), and in other parts of the world.

The Specifications, including hardware and middleware elements, are set forth in the OpenCable Host Core Functional Requirements (CFR) specification which is available to the public free of charge at www.opencable.com/specifications. The Specifications also address, define, and require standard methods for implementing various regulatory and consumer features such as Closed Captioning, Emergency Alert Signaling (EAS), Ratings, etc.

- **CableCARD Interface Security.** The tru2way license includes a license to a patented algorithm and secret know-how to enable a Host Device to decrypt encrypted cable content. This CableCARD interface technology is inserted into the Host Device and works cooperatively with a CableCARD provided by the Cable Operator to provide the subscriber the cable services they have ordered in a secure manner. Use of this decryption technology is available royalty-free, subject to a one-time administrative fee.
- **Certification.** Tru2way Host Device Certification testing is currently offered by CableLabs eight times per year, with test “waves” weighted towards the beginning of the year in order to meet typical seasonal consumer electronics demand. Certification testing is performed in accordance with the CableLabs Certification Wave Requirements and Guidelines publicly posted at <http://www.cablelabs.com/certqual/>. Although CableLabs performs the testing, decisions are made by an independent panel of cable industry technical experts that are unaffiliated with the products being tested. This allows for an objective testing and assessment of test results.

Availability of Test Suite. In order to make CableLabs testing as transparent as possible, the actual Tests and Test Plan (detailed instructions for executing the Tests) used by CableLabs are “locked down” and made available to Licensee approximately four (4) weeks prior to each Certification Wave. The Tests, Test Plan and other code are made available royalty free, see www.opencable.com/documents for licensing details. Thus, a Licensee should have good knowledge of the readiness of its Host Device well in advance of Certification testing. Commercial test facilities and test tools are also available from third parties.

Flexible Certification Options. In order to make Certification testing as flexible as possible several “self certification” options are available:

- **Paper Certification.** Streamlined “Paper Certification” is allowed for minor changes to previously Certified Host Devices. Paper Certification can generally be approved in approximately two (2) weeks. Paper Certification may be used, for example, to re-Certify a software upgrade to a previously Certified Host Devices that consists of changes representing functionality entirely outside the scope of the current Specifications.
- **Self Certification.** Licensees who have demonstrated that they are consistently capable of Certifying Host Devices may apply for Self Certification status. In general, successful Certification of at least one (1) Host Device in three (3) CableLabs Certification Waves within a two (2) year period indicates such capability.
- **tru2way Trademark License [Optional].** Use of the tru2way trademark is optional, but is made available for Certified tru2way Host Devices. The tru2way trademark is used and promoted

by Cable Operators, and Content Providers, programmers and application developers who develop or use tru2way applications.

- **Other tru2way Resources.** At the option of the Licensee, other tru2way resources are also made available under a royalty free license. This includes a source code Reference Implementation of the tru2way middleware stack, the Test Conformance Kit (TCK) for testing the middleware stack, and other resources. See www.opencable.com/documents.
- **IPR Policy.** Many major components of the Specification simply refer to well-established ANSI or other specifications that are under “fair reasonable and non-discriminatory” (FRAND) intellectual property licensing terms from their respective standards organizations. To provide protection for additional features added by Specifications, and for an overall “umbrella” of the combination of standards and specifications, all licensees in the “ecosystem” agree to reciprocal FRAND terms amongst their co-licensees.

This tru2way licensing overview is provided for the convenience of Licensee and is not a part of or replacement for the tru2way Host Device License Agreement.

<tru2way> HOST DEVICE LICENSE AGREEMENT

THIS tru2way HOST DEVICE LICENSE AGREEMENT (the “**Agreement**”) provides Licensee a license to certain security elements, authentication certificates, specifications, software and test materials, to develop and manufacture compliant tru2way Host Devices. The license also includes an optional trademark license to the “<tru2way>” mark for use on Certified Host Devices.

The Agreement is by and between Cable Television Laboratories, Inc. (“**CableLabs**”) a Delaware non-stock membership corporation with offices at 858 Coal Creek Circle, Louisville, Colorado 80027 USA, 303-661-9100; fax 303-661-9199, and the Licensee identified below.

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 last date signed below (the “**Effective Date**”).

Name of Licensee: _____	Individual Contact: _____
Address: _____ _____	Title: _____
City: _____ State: _____	Phone: _____
Postal Code: _____ Country: _____	Fax: _____
	E-Mail: _____

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

1.0 INNOVATION IN HOST DEVICES

The Specifications represent the baseline functionality of a retail consumer electronics Host Device that will operate on Cable Operator systems that support the tru2way technology. Licensee may include in a Host Device additional features or functionalities not specified in the Specifications. Such devices may include, but are not limited to:

- a Host Device that receives content from other sources (e.g., Internet, satellite or digital over-the-air broadcast)
- a Host Device that includes digital video recorder (DVR) functionality
- integration of linear basic, expanded basic, and premium cable programming (including HD content) into Licensee's guide and presented to the user by Licensee.
- **Commercially Available Guide Data.** Licensee acknowledges that certain Cable Operators make available commercially available guide data on selected video transport streams from time to time, but that such guide data is not owned or controlled by those Cable Operators or CableLabs, or made available by CableLabs under this Agreement.

To facilitate such innovation in multi-function Host Devices while maintaining a user friendly experience, the Specifications and the tru2way Multi-Mode Functionality Requirements define a "CE Mode," a "Cable Mode," the transition states between the two modes or environments, and basic application behavior guidelines. The Specifications and the tru2way Multi-Mode Functionality Requirements are hereby incorporated herein, and are required for Host Devices that optionally implement a CE Mode; see www.opencable.com/specifications. *For clarification, the Specifications and tru2way Multi-Mode Functionality Requirements do NOT require a cable "monitor application" to be in control of the presentation of services to the user or the allocation of resources in the Host Device, while in CE Mode.*

Innovative features and functions in the Host Device that are not specified in the Specifications are allowed and encouraged. 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 may be manufactured by Licensee. It is further understood and agreed that Licensee may enter into an agreement with an individual Cable Operator under which the Licensee's Host Device renders services provided by that Cable Operator to cable customers served from that Cable Operator's cable system in a mutually agreed upon manner as between Licensee and such Cable Operator. All other Host Devices must comply with the terms and conditions of this Agreement, including any representations and warranties made below.

Innovation in cable networks, cable services, and retail Host Devices that access cable Services is desirable. The parties agree that access to the cable network and cable Services by the Host Device shall not be a basis for limiting or freezing the cable network, cable Services, or navigation devices (retail or leased), nor imposing additional investment requirements on the cable network beyond the support of the Host Devices as contemplated herein. Neither Licensees nor Cable Operators are limited to innovations on their respective platforms.

2.0 GRANT OF LICENSES

2.1 Specifications. CableLabs hereby grants to Licensee a worldwide, non-exclusive, non-transferable, royalty-free right and license under the Intellectual Property Rights owned or licensable by CableLabs solely to:

(a) view and download the Specifications from the CableLabs website www.opencable.com/specifications ;

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

(c) **Limitations.** For the avoidance of doubt, the license granted hereunder does not include any right or license to any third party proprietary technology referenced in or required by the Specifications, such as DES, DTCP, or MPEG-2. Licensee acknowledges that designing, manufacturing, distributing, using, selling, or servicing products, or providing services, based on the Specifications may require intellectual property licenses from such third party(ies) for technology referenced in the Specifications. Licensee shall retain all copyright notices contained in the Specifications. With respect to implementations of the tru2way Middleware Specification, the license granted hereunder does not include the right to extend, superset, or subset the OpenCable Name Space as defined therein.

2.2 Development and Evaluation Use; Prototypes. Upon execution of this Agreement and payment of the one-time royalty-free Licensee Fee, CableLabs shall deliver to Licensee:

- (a) evaluation Licensed Technology;
 - (b) evaluation Device Digital Certificates; and
 - (c) an evaluation Code Verification Certificate
- (collectively “**Evaluation Technology**”).

CableLabs grants to Licensee the right to use, reproduce, and distribute the Evaluation Technology for the purpose of making, having made, and using Prototypes. The Compliance Rules and the Robustness Rules, as well as Section 11 of this Agreement, shall not apply with respect to Prototypes or the rights granted under this Section 2.2.

2.3 Pre-Certification Use. Upon (i) notification by Licensee to CableLabs that Licensee intends to submit a Host Device to CableLabs for Certification in accordance with the Certification Wave Requirements and Guidelines, and (ii) receipt by CableLabs of a complete and executed **Digital Certificate Authorization Agreement** (including all exhibits and fees), CableLabs shall verify Licensee’s identity and information therein for security purposes. Upon successful verification CableLabs shall:

- (a) deliver to Licensee the production Licensed Technology;
 - (b) authorize Licensee to receive one hundred (100) production Device Digital Certificates and one hundred (100) production DSG Device Digital Certificates. There is no per-certificate fee for these initial Device Digital Certificates.
 - (c) authorize Licensee to receive a production Code Verification Certificate for signing the code image in Licensee’s Host Device.
- (collectively “**Production Technology**”).

CableLabs grants to Licensee the right to use the Production Technology *only for internal testing in products that Licensee intends to submit to CableLabs for Certification*. The Production Technology may NOT be used in any commercial product offered for sale, or in products not manufactured in compliance to the Specifications. At all times, Licensee shall treat the Production Technology strictly in accordance with the provisions of Section 9 (Confidentiality).

2.4 Commercial Use. Upon Certification (including Self-Certification) of a Host Device, CableLabs grants to Licensee a non-exclusive, non-transferable, world-wide license under the Intellectual Property Rights owned by, or licensable from, CableLabs to make, have made, use, sell, offer to sell, import, and reproduce the Production Technology in Certified Host Devices, but only for distribution in

North America, and only in accordance with the terms and conditions of this Agreement (including Section 9 Confidentiality and the Digital Certificate Authorization Agreement).

2.5 Components. Licensee shall have the limited right to make, have made, use, sell, offer to sell, import, reproduce and distribute Licensed Components, subject to the following limitation: Licensee shall distribute the Licensed Components containing Production Technology only to parties licensed by CableLabs to use the Production Technology or to Have Made Parties. Licensee may obtain a list of current Production Technology licensees upon request to CableLabs. Licensee must separately maintain records of sales of Licensed Components, and Licensee shall, upon request provide the names and contact information of each Component purchaser to CableLabs.

2.6 Have Made Rights. Licensee shall have the right to have third parties (“Have Made Parties”) design and make Host Devices, Licensed Components and Prototypes or subparts thereof for the sole account of Licensee, provided that they (a) are to be sold, used, leased, or otherwise disposed of, by or for Licensee under the trademark, trade name, or other commercial indicia of Licensee 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 that have access to the Production Technology must be (i) licensed to use the Production Technology by Cablelabs, (ii) Affiliates of Licensee, or (iii) bound in writing to a non-disclosure agreement with Licensee on terms that are no less stringent than the terms set forth in Section 9 hereof. 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. Other than on behalf of Licensee, Have Made Parties shall receive no license, sublicense, or implied license with respect to the Production Technology.

2.7 Limitation on All Licenses. CableLabs and/or its licensors reserve all rights not expressly granted under Agreement. 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 this Section 2.3, no license is granted for any commercial Host Device that does not comply with the Specifications, the Robustness Rules and the Compliance Rules, and that is not Certified.

3.0 OPTIONAL TRU2WAY MIDDLEWARE RESOURCES

The following optional resources are made available to Licensee to facilitate the development of the tru2way Middleware implementation for use in a Host Device.

3.1 tru2way Middleware Reference Implementation. A PC-based reference implementation is made available royalty free under open source or commercial terms. This includes an entire implementation of the tru2way Middleware. The source code is maintained at java.net under open source terms, see <https://opencable.dev.java.net/>. A royalty free commercial license is available and can be downloaded from https://www.cablelabs.com/doczone/opencable/testing/ocap_resources_license_agreeme/. A CableLabs DocZone account is required.

3.2 JavaDocs. Certain software code, including Java-based API signatures, javadocs, and stubs for implementing the OCAP middleware, as well as sample applications and guidelines are provided by Cablelabs. The materials may be downloaded via royalty-free click-thru license at https://www.cablelabs.com/doczone/opencable/testing/ocap_resources_license_agreeme/. A CableLabs DocZone account is required.

3.3 Test Conformance Kit (TCK). A license to the tru2way Middleware TCK is not strictly required, but passage of the TCK on a target Host Device is a required component for Certification, <tru2way> trademark usage, and issuance of Digital Certificates. Note, the major component of the tru2way Middleware stack, Sun Java PBP 1.1, is “Self Certified” as compliant through written verification of compliance provided to CableLabs. The TCK may be downloaded via royalty-free

click-thru license at

https://www.cablelabs.com/doczone/opencable/testing/ocap_resources_license_agreeme/. A CableLabs DocZone account is required.

3.4 Automated Testing Environment (ATE). The tru2way Middleware ATE is a test harness used to run the TCK. The ATE may be downloaded via royalty-free click-thru license at https://www.cablelabs.com/doczone/opencable/testing/ocap_resources_license_agreeme/. A CableLabs DocZone account is required.

3.5 Other Resources. Other tru2way Middleware resources, including a Sun-hosted Java Developers forum and a list of support vendors and services providers are available. See <https://opencable.dev.java.net/> and www.opencable.com/.

4.0 < tru2way> TRADEMARK LICENSE [OPTIONAL]

CableLabs hereby grants to Licensee a non-exclusive license to use (at Licensee's option) the "<tru2way>" trademark (the "**Mark**") on any Certified Host Device, on packaging or advertising for the same, and on Licensee's website. Licensee shall use the Mark only in reference to Host Devices that have been Certified in accordance with the provisions of this Agreement. Licensee shall only use the Mark in accordance with the tru2way Trademark use Guidelines posted at www.tru2way.com. Licensee shall not alter the Mark in any manner, including the typeface, proportions, colors, elements, or location of any of the text in relation to the other elements of the Mark. Licensee may not animate, morph, or otherwise distort the perspective or appearance of the Mark or translate elements of the Mark into another language or change them to another character set. The Mark may be used in the form of label affixed to the Certified Host Device or may be printed or engraved on the Certified Host Device using "camera ready" artwork supplied by CableLabs. If Licensee's logo on the Certified Host Device is smaller than one inch square, the Mark may be proportionally reduced so as not to be longer along either dimension than the longest dimension of Licensee's logo. Larger sizes of the Mark may be used on packaging or marketing materials for Certified Host Devices. Licensee shall not use the Mark on materials that disparage CableLabs, its affiliated companies, or its products or services; or that violates any state, federal, or foreign law or regulation. Licensee shall include the following notice on all marketing materials that refer to CableLabs or display products bearing the Mark:

"<tru2way>" is a trademark of Cable Television Laboratories, Inc. and may not be used without authorization.

5.0 CERTIFICATION

Except as otherwise permitted under this Section 5, prior to commercially distributing a Host Device, Licensee shall submit the Host Device to CableLabs for Certification testing for conformance to the Specifications. Certification testing includes execution of the Test Suite in accordance with the Test Plan. The Certification Requirements and Guidelines located at www.cablelabs.com/certqual are incorporated herein by reference.

CableLabs shall use best efforts in the utmost of good faith to make the Certification process objective, fair and non-discriminatory. Licensee acknowledges and agrees that any production of Host Devices prior to Certification shall be undertaken at Licensee's sole risk.

As noted in the Certification Requirements and Guidelines, several streamlined Certification options also exist, including the following:

5.1 Paper Certification. "Paper Certification" is allowed for minor changes to previously Certified Host Devices. CableLabs, through its Cable Operator Certification Board, shall use best efforts to approve or disapprove Paper Certification within two (2) weeks from the date of application thereof. Licensee may make and distribute Certified Host Devices with such minor changes

concurrently with submission for Paper Certification; provided that Licensee acknowledges that any upgrades made to Certified Host Devices prior to the grant of Paper Certification shall be undertaken at Licensee's sole risk and Licensee will remain responsible for any breach of this Agreement, including Section 11.2 and compliance with the Compliance Rules, Robustness Rules and Specifications.

By way of example, Paper Certification may be approved for software maintenance upgrades or a new code version of a previously Certified Host Device that consist of changes representing functionality entirely outside the scope of the then-current Specifications.

5.2 Self-Certification. Licensees who have demonstrated that they are consistently capable of obtaining Certification of Host Devices under Section 5.0 may apply for Self Certification status. Subject to the conditions of this section, successful Certification of three (3) unique Host Devices in three (3) separate CableLabs Certification Waves within a two (2) year period, together with no Certification failures or breaches of either: 1) the then governing agreement that set forth the terms with respect to previously Certified commercial Host Devices; or 2) in the case of Certification under this Agreement, this Agreement, over such two (2) year period, shall serve as *prima facie* evidence of such capability. After successful Certification in such third Certification Wave, Licensee may apply to the Certification Board for Self-Certification status of such Licensee. The Certification Board may revoke Self-Certification status for any material breach of this Agreement by Licensee. The Self-Certification election is optional under the sole discretion of the Licensee, who may notwithstanding the acquiring of the Self-Certification status continue to use CableLabs Certification under Section 5.0 hereabove.

6.0 CHANGE MANAGEMENT

6.1 Participation in Change Process. Pursuant to the Specification Change Process, Licensee shall be provided notice and a reasonable opportunity to review and comment on any proposed Changes to the Specifications. The Specification Change Process shall include the ability of Licensee to draft and submit Engineering Change Requests (ECRs), and for Participants (including Licensee) to comment on Engineering Change Orders (ECOs), and have the opportunity to participate in Specification drafting working groups. Parties to the Specification Change Process may also include Content Providers who have also signed the Confidential Information Access Agreement. See www.opencable.com for further details on the Specification Change Process.

6.2 Specifications. Issued Specifications may be amended from time to time, but only in accordance with the Specification Change Process. 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 Specifications ("New Specifications") (collectively, "Changes"). New Specifications may include, by way of example and not of limitation, Changes that would require new technical features, optional extensions (e.g., like DVR), or Changes 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 would 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.

6.3 Effect of Changes

(a) Existing Products. 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 Requirements and Guidelines), notwithstanding any Changes or Sunsetting (as defined below) of Certification. Changes or Sunsetting shall not trigger any obligation to re-Certify a previously Certified product, to Certify a product not previously subject to the Certification Criteria, nor to modify or re-label Certified Products. Notwithstanding, such existing products may not implement new features or services facilitated by the Changes or otherwise offered by Cable Operators.

(b) Editorial Changes. Editorial Changes shall become effective on the date specified in the Engineering Change Notice (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 specified in the ECN, as defined by the applicable ECR Working Group after reasonably considering the impact to vendors with products that may be affected by the Minor Change, including the following: (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 if 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) Synchronization to Issued Specifications. The then-current Issued Specification consists of the Issued Specification, plus all effective ECNs for a given Certification Wave. ECNs representing Minor Changes and Editorial Changes will be periodically aggregated and added to new Issued Specifications.

(e) Available of Issued Specifications. Licensee shall have the access to the same version of Issued tru2way Middleware Specification (and the accompanying rights and licenses under this Agreement) at the same time as such Issued version is made available for use and deployment by Cable Operators.

(f) New Specifications. New Specifications are effective on the date they are first published as Issued Specifications. New Specifications shall not automatically obsolete existing specifications.

(g) Test Suite and Test Plan. CableLabs shall revise the Test Suite and Test Plan to accommodate Changes, and otherwise to conform the tests to the Specifications.

6.4 Sunsetting of Certification. CableLabs reserves the right to discontinue Certification of Host Devices (a) conforming to a Specification version that (a) has been Issued for three or more years, or (b) the lapse of one year during which no Host Device conforming to the Specification version has been submitted to CableLabs for Certification. Notwithstanding the sunsetting, the Paper Submission process described in the Certification Requirements and Guidelines may still be used for the minor changes applicable to paper Certification to maintain Certification of Host Devices certified to such sunset Certification (but such Host Devices may not be capable of implementing new features and receiving new services).

6.5 Revision to Compliance Rules. CableLabs shall provide Licensee at least sixty days' notice of any proposed changes to the Compliance Rules. 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 such changes to the Compliance Rules within twelve (12) months after notification if the changes are mutually agreed by CableLabs and Licensee 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 the event that Licensee disagrees with a change to the Compliance Rules, Licensee may use the Dispute Resolution process identified below.

6.6 Successor Technology. In the event that CableLabs undertakes to define specifications for a successor technology on Digital Cable Systems, and Licensee remains a current party to the OpenCable Contribution Agreement, then Licensee may participate in such undertaking under the terms of said OpenCable Contribution Agreement. The parties participating in such undertaking shall use commercially reasonable efforts to make such successor technology available under RAND or royalty-free terms. As used in this section, “Digital Cable System” means a cable system required to provide CableCARDS under 47 C.F.R. §76.1204(a)(1) which have one or more channels utilizing QAM modulation for transporting programs and services from its headend to receiving devices.

6.7 Dispute Resolution. In the event that Licensee reasonably, and in good faith, objects to Changes (including the effective date of such Changes), or the sunset 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.

7.0 INTELLECTUAL PROPERTY

7.1 IPR Policy. Licensee, on behalf of itself and its Affiliates, hereby agrees to be bound by the terms and conditions of the IPR Policy attached hereto and incorporated herein as *Exhibit A* (“**IPR Policy**”).

8.0 FEES

8.1 Licensed Technology License Fee. As consideration for the licenses granted hereunder, Licensee agrees to pay CableLabs a one-time, non-refundable license fee of \$5,000 (the “**License Fee**”) within thirty days of the Effective Date. If Licensee has previously paid a fee to CableLabs for an evaluation license for the CableLabs Technology or has otherwise paid a license fee to CableLabs for the Licensed Technology, no License Fee shall be due.

8.2 Certification Fees. Fees for Certification (including Self-Certification) of Host Devices are posted at http://www.cablelabs.com/downloads/Cert_Fees.pdf. Fees may be modified annually by CableLabs, but all fees shall be fair, reasonable and non-discriminatory.

8.3 Digital Certificates. Fees for Digital Certificates are posted at http://www.cablelabs.com/downloads/Cert_Fees.pdf. Fees may be modified annually by CableLabs, but all fees shall be fair, reasonable and non-discriminatory.

8.4 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 that may be levied upon Licensee by taxing authorities in connection with this Agreement.

9.0 CONFIDENTIALITY

9.1 Confidential Information. “Confidential Information” shall include the Licensed Know-How, Highly Confidential Information (as defined below) and may also include confidential information of Licensee that is clearly marked as “Confidential” or a similar expression. CableLabs and Licensee may be either a Recipient or a Discloser. “Confidential Information” shall not include information which: (a) was in the possession of, or was known by, Recipient prior to its receipt from Discloser, without an obligation owed to Discloser, or its licensors, to maintain its confidentiality; (b) is or becomes generally known to the public without violation of this Agreement by Licensee or any other

Licensee, and which CableLabs or Licensee 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; (c) is obtained by Recipient from a third party, without an obligation owed to such third party to keep such information confidential; or (d) is independently developed by Recipient without use of any Confidential Information.

Recipient agrees that it shall use reasonable care to keep the Confidential Information strictly confidential and not disclose it to any other person except to its employees, Affiliates, contractors, consultants, agents, customers (other than CableLabs members) and representatives who have a “need to know” for the purposes of this Agreement. Recipient shall be responsible for any breach of confidentiality by such parties, including former employees, Affiliates, contractors, consultants, agents, customers (other than CableLabs members) and representatives. Recipient shall protect the Confidential Information with the same degree of care as it normally uses in the protection of its own similar confidential and proprietary information, but in no case with any less degree than reasonable care.

Notwithstanding anything in this Section 9 to the contrary, Confidential Information may be disclosed by Licensee pursuant to the order or requirements of a court or governmental administrative agency or other governmental body of competent jurisdiction, provided that (x) Discloser has been notified of such a disclosure request sufficiently in advance to afford Discloser reasonable opportunity to obtain a protective order or otherwise prevent or limit the scope of such disclosure to the extent permitted by law and (y) Recipient cooperates in good faith with such efforts by Discloser.

The obligations under this Section 9 shall terminate three years after the last commercial use of the Licensed Technology by Licensee or any CableLabs licensee of the Licensed Technology; provided that Sections 9.2(b), 9.2(c), and 9.3 shall cease to apply when Licensee has returned all tangible embodiments of Licensed Know-How in its possession to CableLabs.

9.2 Highly Confidential Information. “Highly Confidential Information” shall include reference source code implementations, shared secret keys, Diffie-Hellman system parameters, encryption and decryption keys, private keys and the DFAST source and library files that contain DFAST constants.

Licensee shall implement and maintain security measures for Highly Confidential Information that are in accordance with commercial practices for managing keys and other such information, such measures to include, at a minimum, the following:

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

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

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

(d) Obligations for maintaining confidentiality and security of Highly Confidential Information in the form of private keys associated with Licensee's Digital Certificates are set forth in the Digital Certificate Authorization Agreement.

(e) Licensee shall notify CableLabs immediately upon discovery of any unauthorized use or disclosure of Highly Confidential Information, and will cooperate with CableLabs to seek to regain possession of the Highly Confidential Information disclosed and to prevent its further unauthorized use or disclosure.

9.3 Security Audit. CableLabs (or the third party auditors identified) shall have the right to review, upon five (5) business days notice (or earlier if CableLabs has a good faith belief that the Highly Confidential Information has been, or will be, compromised in any manner) the implementation of all security measures at the secure location(s) required hereunder for the Highly Confidential Information no more frequently than once per year (unless CableLabs has a good faith belief that the Highly Confidential Information has been, or will be, compromised in any manner) at reasonable times as agreed between Licensee and CableLabs. Such audit shall be subject to the confidentiality provisions of Section 9.1 hereof, with respect to Confidential Information marked pursuant to Section 9.1 or otherwise reasonably designated by Licensee. CableLabs and Licensee hereby consent to use of the following third-party auditors: Verisign or any other third parties mutually agreed by Licensee and CableLabs. If the auditor finds a material breach, it will only report the facts directly relevant to such breach that are necessary to enforce this Agreement and safeguard the Highly Confidential Information. In the event that the auditor finds no material breach of this Agreement with respect to Licensee's handling and safeguarding of the Highly Confidential Information, the auditor will limit its report solely to such finding.

10.0 TERM AND TERMINATION

10.1 Term. The term of this Agreement shall be for the life of the later of U.S. Patent No. 4,860,353, and U.S. Patent No. 5,684,876 to expire, and shall be extended automatically thereafter indefinitely on a year by year basis unless earlier terminated according to its terms; provided that under no circumstances shall the term of the license for the Licensed Patents granted pursuant to Section 2 of this Agreement exceed the patent term of the last of the Licensed Patents to expire.

10.2 Termination by CableLabs per Model for Cause. CableLabs may terminate the license associated with a particular model of Certified Host Device that materially breached Sections 2 or 11 (as those obligations applied at the time the device was Certified or Self-Certified, or at the time Host Device was later updated). 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 after CableLabs has (a) evaluated the potential breach, (b) consulted with Licensee regarding the potential breach, (c) given written notice to Licensee of CableLabs' intent to terminate the license with respect to such model of Host Device, and (d) provided Licensee with a reasonable opportunity to cure the breach (where such breach is capable of being cured) and such breach remains uncured for 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, or distribution, then, a longer cure period as reasonably determined by CableLabs shall be given. Termination of the licenses granted for any specific model of Certified Host Device shall not affect the licenses granted for any other model.

10.3 Termination by CableLabs of Agreement for Cause. CableLabs may terminate this Agreement in the event that CableLabs provides notice of Licensee's material breach of any term, representation, warranty or covenant set forth in Section 2, 4, 5, 8, 9 or 11 hereto and (where such breach is capable of being cured) such breach remains uncured sixty days following the date of such notice. Termination of the Agreement shall have the effect of terminating the licenses granted hereunder for all models of Host Devices.

10.4 Termination by Licensee. Licensee may terminate this Agreement at any time upon written notice to CableLabs.

10.5 Effect of Termination. Upon the termination of the licenses granted hereunder for any specific model of Host Device, Licensee may no longer make, have made, use, sell, import or distribute such model of Host Device, use the Production Technology therewith, nor use the Mark in connection with such model of Host Device, except that, if the termination did not result from Licensee's failure to satisfy the requirements of the Robustness Rules or the Compliance Rules, Licensee may sell or distribute any remaining Certified Host Devices. End user licenses properly granted by Licensee in conjunction with the sale or distribution of a Certified Host Device by Licensee pursuant to Section 3 prior to the date of termination shall remain in full force and effect. Unless otherwise stated herein, no termination of this Agreement, whether by CableLabs or by Licensee, or termination of any license granted hereunder shall relieve either party of any obligation or liability accrued hereunder prior to such termination, or rescind or give rise to any right to rescind anything done by either party prior to the time such termination becomes effective nor shall the survival provisions of Section 10.5 be affected by such termination.

10.6 Survival. 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 7, 9, 11, 13, 14, 15, 16, and Section 3 of the IPR Policy (for a period of 12 months from termination, plus one day). In addition, except as they relate to Prototypes developed pursuant to Section 2.2, Exhibits B and C shall survive any termination of this Agreement with respect to products that are both Certified and distributed under this Agreement.

11.0 REPRESENTATIONS, WARRANTIES, AND COVENANTS; DISCLAIMERS

11.1 CableLabs. CableLabs represents, warrants and covenants that:

- (a) It has the right to enter into this Agreement;
- (b) Without investigation, it is not aware of any notice or claim, threatened or pending, that the use of the Production 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.

11.2 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 CableLabs on behalf of Licensee;
- (b) This Agreement constitutes a valid and binding obligation of Licensee, enforceable according to its terms; and
- (c) As to each of the Host Devices made under this Agreement, and notwithstanding additional features allowed under Section 1.0 hereof, the Host Device shall:
 - (i) be compliant with the applicable Specifications;
 - (ii) include no feature or functionality that (i) technically disrupts, impedes or impairs the delivery Services to any cable customer; for the avoidance of doubt, such services shall be delivered to the cable customer in a substantially similar 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 applicable Specifications, and there is no

alternative compliant implementation), including the display of applications in the manner that the Specifications direct that such applications should be displayed, and the order in which such programming is offered (including all advertising), i.e., no “disaggregation” of the cable services is permitted; (ii) causes physical harm to the cable network or the CableCARD; (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; or (v) interferes with or disables the ability of a Cable Operator to communicate with or disable a CableCARD or to disable services being transmitted through a CableCARD;

(iii) while in CE Mode (as defined in the Specifications and the tru2way Multi-Mode Functionality Requirements), operate in accordance with the tru2way Multi-Mode Functionality Requirements, which are hereby incorporated by reference herein;

(iv) at the time of manufacture, contain no integrated circuit, ROM, RAM, software or other device or functionality that enables copying or recording of Controlled Content, other than as permitted by the Compliance Rules;

(v) at the time of manufacture, maintain control of content copies consistent with copy control instructions or the encryption mode indicator bits transmitted with digital signals as specified in the Specifications;

(vi) at the time of manufacture, be designed to effectively frustrate tampering and reverse engineering directed towards defeating copy protection requirements in accordance with the Robustness Rules; and

(vii) at the time of manufacture, not transmit or decode Controlled Content received from the cable television transmission without proper authorization from the Cable Operator.

As used in this section 11.2(c), “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 any Host Device that it determines to have been modified after manufacture so as to be non-compliant with the Specifications.

11.3 Disclaimers. EXCEPT AS EXPRESSLY SET FORTH IN THIS SECTION 11, EACH PARTY DISCLAIMS ALL OTHER WARRANTIES, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO, (A) ANY WARRANTY THAT THE PRODUCTION TECHNOLOGY OR ANY SPECIFICATIONS DOES NOT INFRINGE THE INTELLECTUAL PROPERTY RIGHTS OF ANY OTHER PERSON OR ENTITY, (B) ANY WARRANTY THAT ANY CLAIMS OF THE LICENSED PATENT ARE VALID OR ENFORCEABLE, (C) ANY IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT, OR (D) THAT THE RIGHTS AND LICENSES GRANTED TO LICENSEE HEREUNDER COMPRISE ALL THE RIGHTS AND LICENSES NECESSARY OR DESIRABLE TO PRACTICE, DEVELOP, MAKE OR SELL HOST DEVICES. THE PRODUCTION TECHNOLOGY AND ENHANCEMENTS THERETO, AND ANY OTHER ITEMS, DELIVERABLES, OR INFORMATION SUPPLIED BY OR ON BEHALF OF CABLELABS ARE PROVIDED ON AN “AS IS” BASIS. Licensee acknowledges that the Specifications may contain materials, including normative and other references, not owned or controlled by CableLabs, or made available by CableLabs under this Agreement. Licensee understands that implementation of the Specifications may necessitate implementation or use of such materials, including normative references. Licensee further acknowledges that it may be required to enter into agreements with parties holding intellectual property rights related to such 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 Specifications, and/or a reciprocal grant of essential IPRs.

12.0 INDEMNIFICATION

Licensee and CableLabs will each defend, indemnify and hold harmless the other and the other's Members, Affiliates, licensors, 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. 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 Licensee or CableLabs under this Section are conditioned on the other giving Licensee or CableLabs: (a) prompt written notice of any Claim for which indemnification is sought; (b) control of the defense and settlement of such Claim; and (c) reasonable assistance and cooperation in such defense, at Licensee's or CableLabs' expense.

13.0 THIRD PARTY BENEFICIARIES

Licensee agrees that Third Party Beneficiaries that are Cable Operators shall each be a third-party beneficiary of this Agreement. Licensee agrees that Third Party Beneficiaries that are Content Providers shall each be a third party beneficiary of this Agreement only with regard to a material breach of this Agreement by Licensee that results in any unauthorized access, copying or distribution 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 14) 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; and (e) CableLabs has informed all Cable Operators of such breach.

14.0 LIMITATION OF LIABILITY

EXCEPT IN THE CASE OF A BREACH OF SECTIONS 2 (LICENSE) OR 11.2 (WARRANTY), OR CLAIMS ARISING UNDER SECTION 9 (CONFIDENTIALITY) OR 12 (INDEMNIFICATION) OF THIS AGREEMENT, IN NO EVENT SHALL ANY PARTY (INCLUDING CABLELABS, ITS LICENSORS, 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, EXEMPLARY, 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 10, Licensee may be liable to CableLabs and/or Third Party Beneficiaries, but in no event will Licensee's liability to CableLabs or any Third Party Beneficiary 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.

For purposes of this Agreement, a breach shall be "**material**" only if Licensee acted in a manner that is prohibited by this Agreement or failed to perform an obligation required under this Agreement, which act or failure has resulted in or would be likely to result in commercially significant harm to CableLabs, or

constitutes a threat to the integrity or security of the Production Technology, or exposes Controlled Content to unauthorized use, copying, or distribution.

15.0 GENERAL

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

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

15.3 No Patent Solicitation Required. Except as expressly provided herein, neither party shall be required hereunder to file any patent application, secure any patent or patent rights, provide copies of patent applications to the other party or disclose any inventions described or claimed in such patent applications.

15.4 Publicity. Following the execution of this Agreement, each party may disclose in media releases, public announcements and other public disclosures, including without limitation promotional or marketing materials, the fact that this Agreement has been executed by Licensee. CableLabs may post a signed copy of this Agreement to its website, so long as such copy is redacted to remove references to Licensee's name and address and any other information that could reasonably reveal Licensee's identity.

15.5 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.

15.6 Service Denial for Cable Services. For the avoidance of doubt, and without limitation of any available rights of Licensee outside of this Agreement, Licensee acknowledges that nothing in this Agreement shall prevent a Cable Operator from denying services to any individual CableCARD, or set of CableCARDS, refusing to issue CableCARDS for use in any individual devices or set of devices, or otherwise preventing cable content from flowing to any individual device or set of devices built by Licensee hereunder. Notwithstanding the foregoing, 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, or distribution, or is in material breach of Section 2.0 (GRANT OF LICENSE) or Section 11.0 (WARRANTY) above.

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

15.8 Compliance with Laws. In connection with this Agreement, each party shall comply with all applicable regulations and laws, including export, re-export and foreign policy controls and

restrictions that may be imposed by any government. Each party shall require its commercial customers with a contractual relationship that may export Host Devices to assume an equivalent obligation with regard to import and export controls.

15.9 No Assignment. Licensee shall not assign any of its rights or privileges under this Agreement without the prior written consent of CableLabs, such consent not to be unreasonably withheld or delayed. No consent shall be required for the assignment of this Agreement to any wholly-owned subsidiary of Licensee or for the assignment in connection with the merger or the sale of Licensee or Licensee's business unit provided that Licensee shall remain liable for its obligations hereunder. Any attempted assignment or grant in derogation of the foregoing shall be void.

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

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

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

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

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

15.15 Entire Agreement. This Agreement, together with the appendices and the documents incorporated herein by reference, embody the entire understanding of the parties with respect to the licenses granted hereunder and supersedes all prior oral or written agreements with respect to the subject matter hereof (such agreements may include, CableCARD-Host Interface License Agreement (CHILA) and the OCAP Implementers License Agreement). Notwithstanding, the parties may enter into the DFAST Agreement and the DFAST Agreement may coexist separately with this Agreement, or, Licensee may terminate this Agreement and continue to build products under the DFAST Agreement as contemplated and covered under such DFAST Agreement, without any additional licensing fee.

15.16 Most Favored Status. In the event that CableLabs enters into a tru2way Host Device License Agreement (the "**tru2way Agreement**") with another manufacturer of Certified Host Devices, and such other agreement has terms that are materially different from and more favorable to such other manufacturer 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 tru2way Agreement contains other material modifications from the terms of this Agreement, Licensee also agrees to be bound by such other modifications. CableLabs shall post to the www.OpenCable.com website (with redaction of company-specific information) the most recent "MFNed" tru2way Agreement entered into by CableLabs. It is understood and agreed that the DFAST Agreement sets forth a separate set of obligations that govern the relationship between the parties thereto, that this tru2way Agreement and the changes hereto shall not alter any provisions of any DFAST Agreement, and that changes to any DFAST Agreement shall not alter the provisions of this tru2way Agreement.

16.0 Definitions.

- “**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.
- “**Automated Test Environment**” (or “**ATE**”) means the software and related documentation provided by CableLabs (and updated by CableLabs from time to time) to assist Licensee in running the tru2way Middleware TCK. The ATE does NOT include any hardware or other software that may be required to run the ATE. The ATE is licensed under a click through license available at www.CableLabs.com/Doczone.
- “**Cable Operator**” means any cable operator that CableLabs identifies on its website <www.cablelabs.com> as a member, and any other cable operator that provides CableCARDS to customers in connection with the provision of cable services in North America.
- “**CableCARD**” means an individual addressable device for authorizing and deauthorizing the decryption or descrambling of Services and individual programs and events delivered through the Host Device on a Service by Service or individual program or event basis that conforms to the CableCARD Interface Specification and the CableCARD Copy Protection System Specification (including the multi-stream versions thereof), as posted at www.cablelabs.com/specifications.
- “**Certification Wave Requirements and Guidelines**” means the procedures for submitting a Host Device for Certification, including submission requirements, dates of testing, fees, and appeal process, as updated from time to time. The Certification Wave Requirements and Guidelines are publicly available at www.cablelabs.com.
- “**Certify**” or “**Certification**” means the process by which it is determined that a Host Device conforms to the Specifications. Certification is initially determined by the Certification Board, but as used herein, includes devices that are Self-Certified by Licensee in accordance with this Agreement. The process includes testing the Host Devices against the most recent Test Suite in accordance with the Test Plan (which includes the TCK tests and test plan), as amended from time to time in accordance with Section 4. The Test Suite and Test Plan are made available to Licensee prior to Certification testing. “**Certified**” means that the Host Device has obtained Certification. See also the Certification Wave Requirements and Guidelines.
- “**Changes**” shall have the meaning as described in Section 6.3 hereof.
- “**Code Verification Certificate**” or “**CVC**” means a secure code verification certificate that is signed by the CableLabs CVC Certification Authority, which chains to the CableLabs CVC Root CA. The CVC is used by Licensee to sign the code image contained in a Host Device in order to deter theft or unauthorized access to Services and Controlled Content.
- “**Compliance Rules**” mean the rules, including a list of Approved Outputs, described on Exhibit C hereto which apply to Host Devices and are generally for the purpose of preventing the unauthorized distribution or copying of Controlled Content.
- “**Confidential Information Access Agreement**” means the agreement posted at www.opencable.com/howto, also known as the OpenCable NDA. This agreement allows Licensee to access Draft Specifications, and make comments, prior to public posting.
- “**Content Providers**” means any video programming providers that provide copyrighted works for transmission to Certified Host Devices and the copyright owners of such work.
- “**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); (c) the copy control information

(CCI) otherwise marked to indicate restrictions on access, copying, redistribution, or usage rights, or (d) as defined through the tru2way Middleware application.

“**Device Digital Certificate**” means a secure end-entity device digital certificate that chains to the CableLabs MFG Root Certification Authority. One or more unique Device Digital Certificates are included in each Host Device in order to deter theft or unauthorized access to Services and Controlled Content.

“**DFAST Agreement**” shall mean the most recent version of the “DFAST Technology License Agreement for Unidirectional Digital Cable Product” as found at <http://www.cablelabs.com/udcp/>. The DFAST Agreement does *not* include a license for use in bi-directional devices, a license to various OCAP technologies, or a license to digital certificates used in bi-directional devices.

“**Digital Certificate Authorization Agreement**” (DCAA) means the agreement posted at http://www.opencable.com/downloads/OC_Host_Device_DCAA.pdf. The DCAA must be completed and executed prior to submission for Certification of Licensee’s Host Device. The DCAA authorizes License to use industry-standard x.509 digital security certificates to authenticate the Host Device itself, the Host Device code, and tru2way applications.

“**Digital Certificate**” means collectively the Code Verification Certificates and the Device Digital Certificates.

“**Draft**” means, with respect to versions of the various Specifications, a document that is specifically identified by CableLabs as a “Work in Progress” or “Draft” version. Draft specifications are only made available by CableLabs for review and comment by Participants that have signed a Confidential Information Access Agreement in substantially the same form as the agreement found at www.opencable.com. Draft specifications specifically exclude Issued specifications.

“**Have Made Parties**” shall have the meaning as described in Section 2.6 hereof.

“**Highly Confidential Information**” shall have the meaning as described in Section 7.1 hereof.

“**Host Device**” means a set-top terminal, television or navigation device for selecting Services on a program by program basis and that conforms to the Specifications. Host Device includes Licensed Components.

“**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.

“**IPR Policy**” means the fair, reasonable and non-discriminatory IPR contribution policy used in drafting the Specifications and granting the licenses hereunder. See **Exhibit A**.

“**Issued**” means, with respect to versions of the various Specifications, that is identified by CableLabs as a current issued version applicable for Certification and identified as *Issued* on the cover page. Upon becoming an Issued specification, the specification is no longer considered a Draft specification; that is, Issued specifications shall not include Draft versions of specifications released from time to time by CableLabs.

- “Licensed Components”** means component products which utilize the Licensed Technology and which are designed for incorporation into Prototypes or Host Devices.
- “Licensed Know-How”** means all know-how, associated technology, trade secrets, copyrighted works, reference source code implementations, shared secret keys, Diffie-Hellman system parameters, private keys, encryption and decryption keys, software development tools, methodologies, processes, technologies or algorithms, test data sets and test cases and other implementations of technology, and any related documentation, that CableLabs provides to Licensee to assist in incorporating the Licensed Technology into Licensed Components, Prototypes, or Host Devices.
- “Licensed Patents”** means U.S. Patent No. 4,860,353 (also known as the DFAST Patent) and U.S. patent No. 5,684,876 (also known as the residual block handling patent), and any division, continuation or continuation in part of the foregoing patents, any patents reissuing on or reissuing pursuant to a reexamination of the foregoing patents and all foreign equivalents.
- “Licensed Technology”** means the Licensed Patent(s) collectively with the Licensed Know-How.
- “Members”** means the CableLabs Cable Operator members as posted at www.cablelabs.com .
- “OpenCable Contribution Agreement”** means the agreement posted at www.opencable.com providing for reasonable and non-discriminatory (RAND) intellectual property (IP) terms for contributions made to OpenCable Specifications, document, and related test materials.
- “OpenCable Name Space”** means designations for class, package, or interface names or declarations contained in or referred to by the Specifications which originate from CableLabs or its licensors, which may include such as package or class names beginning with org.ocap, org.cablelabs, java, javax, sun.com, org.davic, org.dvb, org.havi, or their equivalents in any subsequent class, interface, and/or package naming convention reasonably adopted by CableLabs, or its licensors.
- “Participant”** means an entity that has signed, and not terminated, a *Confidential Information Access Agreement* in substantially the same form as the agreement found at www.opencable.com.
- “Prototype”** means a pre-production model of a Host Devices or Licensed Component that utilizes the Licensed Technology and is not made commercially available.
- “Robustness Rules”** mean the rules described on Exhibit B hereto which apply to Host Devices and are for the purpose of resisting attempts to modify CableCARDS or Host Devices to defeat the functions of the Specifications or the Compliance Rules.
- “Service”** means video, audio, or data signals (other than signals delivered via DOCSIS protocols), 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.
- “Specification Change Process”** means the process described in Section 6 and as posted at www.opencable.com for making Changes to the Specification.
- “Specifications”** means Issued versions, as of the date of this Agreement, of the OpenCable Host Core Functional Requirements Specification (including reference to the required the tru2way Middleware Specification), the CableCARD Interface Specification, and the CableCARD Copy Protection System Specification (including the multi-stream versions thereof), plus any applicable optional extensions implemented by Licensee in a Host Device (e.g., Home Networking, DVR, etc.), and other later versions or specifications that may be added as described in Section 6.3. The Specifications are publicly available at no charge at www.cablelabs.com/specifications.
- “Test Conformance Kit” or “TCK”** means the tru2way Middleware Test Conformance Kit (TCK), also known as the Conformance Test Package (“CTP”) that is used to show conformance to the tru2way Middleware Specification, as updated from time to time.

“**Test Plan**” means the procedures for operating test equipment and Host Devices during the execution of the Test Suite, also known as the Acceptance Test Plan (ATP) and the Requirements Matrix (REQ).

“**Test Suite**” means the audit tests used in the process of Certifying a Host Device, also known as the Protocol Implementation Conformance Statements (PICS). This includes the tru2way Middleware TCK used to test the middleware implementation. The Test Suite is executed in accordance with the Test Plan. Although the Test Suite and Test Plan are used to “audit” test the Host Device, Host Devices must conform to the Specifications.

“**Third Party Beneficiary**” means any Content Provider or Cable Operator.

“**tru2way Middleware**” means the required middleware component of a tru2way Host Device, also known as the OpenCable Application Platform or OCAP. The tru2way Middleware is a defined component of the overall tru2way Host Device Specifications.

“**tru2way Multi-Mode Functionality Requirements**” means the document located at www.opencable.com/specifications. Coupled with the Specifications, the tru2way Multi-Mode Functionality Requirements further define the appropriate behavior of a Host Device that implements a “CE Mode” and a “Cable Mode” for a friendly user experience that allows innovation in both a CE Host Device and in Cable Operator Services.

LIST OF EXHIBITS

Exhibit A: IPR Policy

Exhibit B: Robustness Rules

Exhibit C: Compliance Rules

Exhibit A
CableLabs® OpenCable RAND
INTELLECTUAL PROPERTY RIGHTS (IPR) POLICY
(“OPENCABLE IPR POLICY”)

Licensee, by and on behalf of itself and its Affiliates, agrees to the terms of this OpenCable IPR Policy. Without prejudicing the right of Licensee to offer its intellectual property on fair, reasonable, and non-discriminatory terms, CableLabs strongly urges all parties to make such licenses available royalty-free. This OpenCable IPR Policy does not affect other CableLabs projects (e.g., DOCSIS, PacketCable, CableHome, VOD MetaData, etc.), which remain under royalty-free intellectual property arrangements. Pursuant to a separate written agreement, CableLabs reserves the right to establish royalty-free licensing terms for future Specifications, or portions thereof, that Licensee may choose to join, or not join, at its discretion.

1. DEFINITIONS

Capitalized words used in this OpenCable IPR Policy and not otherwise defined herein shall have the meaning ascribed to them in the **tru2way Host Device License Agreement**.

1.1 “Contribution” shall mean any documents, software, tables, charts, descriptions, engineering change requests (ECRs), comments, e-mails, submissions, white papers, technical notes, or other information or materials that are, or have been, submitted by Licensee to CableLabs for incorporation into the Specifications, and including any verbal contributions that are later confirmed in writing by the Licensee.

1.2 “Essential Claim” 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 Issued Specification. Essential 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 an Specification, but that is not set forth in an Specification; (c) any enabling technologies that may be necessary to make or use any product or portion thereof that complies with the Issued Specification, but are not themselves expressly set forth in the Issued Specification (e.g., semiconductor manufacturing technology, 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 Essential Claims.

2. COPYRIGHT LICENSE

2.1 Draft Specifications. Licensee grants to CableLabs, under any applicable IPRs of Licensee (excluding patents, patent applications, trademark applications or trademarks) a world-wide, royalty-free, nontransferable, nonexclusive, perpetual, irrevocable, right and license to use, reproduce, make derivative works, distribute and sublicense any Contribution, and any such derivative works, to CableLabs members, other licensees, and Participants in the OpenCable Project, but only for the purpose of creating a Specification.

2.2 Issued Specifications. Licensee grants to CableLabs, under any applicable IPRs of Licensee (excluding patents, patent applications, trademark applications or trademarks) a nonexclusive, nontransferable, worldwide, royalty-free, perpetual, irrevocable, sublicenseable right and license to: (a) use, copy, distribute, and make derivative works of any Contribution, to the extent it is included in an Issued Specification, and to implement such Contribution and derivative works thereof; and (b) use, make, reproduce, sell, distribute, import, and transmit implementations of the Contribution and derivative works thereof, to the extent the same are included in an Issued Specification. For the avoidance of doubt, no other express or implied license is granted under this Section 2.2, including no express or implied patent license.

3.0 AVAILABILITY OF PATENT LICENSE

3.1 Notice of Essential Claims. Within sixty (60) days after receipt of any Draft Specification, Licensee shall submit to CableLabs in writing a list of the Essential Claims (to the extent that such would be Essential Claims in the event the Draft Specification matures to an Issued Specification) in all patents and published patent applications owned, licensable, or otherwise controlled by Licensee or any of its Affiliates for which Licensee will *not* (or has no free right to) make licenses (or sublicenses), or cause licenses (or sublicenses) to be made, available on a reasonable and non-discriminatory basis to any third party (such notice, an “**Essential Claim Notice**”). In addition, Licensee shall have sixty (60) days from the Effective Date to submit an Essential Claim Notice to CableLabs relating to any existing Issued or Draft Specifications in existence at the time of the Effective Date. Unless noted otherwise by Licensee, a valid Essential Claim Notice provided by Licensee shall also serve as a valid Essential Claim Notice for any subsequent versions of such Draft Specification or Issued Specification. Licensee shall, on a supplemental and ongoing basis, but no less than annually from the Effective Date, update Licensee’s list of Essential Claims on the Essential Claim Notice, and submit such to CableLabs in writing. Licensee may not submit an Essential Claim Notice as to Essential Claims that are necessarily infringed as a result of implementing any Contribution made by Licensee, or any portion thereof (an “**Invalid Essential Claim Notice**”). If such an Invalid Essential Claim Notice is received by CableLabs, it shall have no force or effect, and the applicable Essential Claims within such Invalid Essential Claim Notice shall be treated pursuant to Section 3.2 of this OpenCable IPR Policy. Any other valid Essential Claim Notice received by CableLabs in accordance with this Section 3.1 shall be effective as to the Essential Claims in the Essential Claim Notice thirty (30) days following receipt by CableLabs of such Essential Claim Notice.

3.2 Availability of License to Essential Claims. With respect to all Essential Claims of all patents or published patent applications owned, licensed, or otherwise controlled by Licensee or any of its Affiliates which are *not* validly noticed to CableLabs by Licensee in accordance with the procedure set forth in Section 3.1 of this OpenCable IPR Policy, Licensee agrees to make licenses, or cause licenses to be made, available for such Essential Claims on reasonable and non-discriminatory terms and conditions to any third party that desires to implement or has implemented any such Issued Specification. Such license may be limited to use of such Essential Claims with respect to products or services that comply with the relevant portion of the Issued OpenCable Specification.

3.3 Reciprocity. With respect to third parties, Licensee shall only be bound by this OpenCable IPR Policy to the extent such third parties submit to an equivalent undertaking with respect to any Essential Claims such third parties may own, license, or otherwise control. For the avoidance of doubt, the foregoing obligation shall lapse with respect to any third party that initiates a claim against Licensee alleging it infringes any Essential Claims of such third party.

Exhibit B

Robustness Rules

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

1. Construction.

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

1.2 Defeating Functions. Host Devices shall not include:

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

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

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

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

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

2.0 Documents and Robustness Certification Checklist.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

5.0 Update Procedure.

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

EXHIBIT B-1

Robustness Checklist

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

DATE: _____

MANUFACTURER: _____

PRODUCT NAME: _____

HARDWARE MODEL OR SOFTWARE VERSION: _____

NAME OF TEST ENGINEER COMPLETING CHECKLIST:

TEST ENGINEER: _____

COMPANY NAME: _____

COMPANY ADDRESS: _____

PHONE NUMBER: _____

FAX NUMBER: _____

GENERAL IMPLEMENTATION QUESTIONS

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

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

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

If so, is Controlled Content carried on this bus?

If so, then:

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

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

SOFTWARE IMPLEMENTATION QUESTIONS

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

HARDWARE IMPLEMENTATION QUESTIONS

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

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

SIGNATURES:

Signature of Test Engineer with Personal Knowledge of Answers

Date

Printed Name of Test Engineer with Personal Knowledge of Answers

EXHIBIT C

Compliance Rules

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

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

1. Definitions

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

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

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

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

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

1.6 “**HDCP 1.0**” means that method of authentication, encryption, decryption, and renewability that is described in the specifications entitled “High-Bandwidth Digital Content Protection System, Rev. 1.1” as supplemented (but not superseded) by the Specifications, as may be amended from time to time.

1.7 “**HDCP 2.0**” means the HDCP 2.0 method of authentication, encryption, decryption, and renewability that is described in the specifications maintained by the Digital Content Protection, LLC at http://www.digital-cp.com/hdcp_technologies, unless otherwise noted or supplemented in the CableLabs Specifications.

1.8 “**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.

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

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

1.11 “**RCT**” or “**Redistribution Control Trigger**” means the field or bits, as described in the Specifications, used to trigger the Encryption Plus Non-assertion (“EPN”) state in DTCP protected digital

outputs in the Certified Host Devices when the RCT value is set to a value of one (1) in combination with the EMI bits set to a value of zero, zero (0,0), which signals the need for redistribution control to be asserted on Controlled Content without the need to assert numeric copy control.¹

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

1.13 **“VCPS”** means the Video Content Protection System for recording encrypted content on DVD+RW and DVD+R optical digital media protected by VCPS technology.

1.14 **“CPDO”** means the secure digital recording method as specified by EnCentrus Systems, Inc. in its document entitled EnCentrus Content Protected Digital Output Port System Description; Revision 1.2 dated January 2006.

1.15 **“RPSP”** means the secure digital recording method as specified by Samsung Electronics Co., LTD in its document entitled Recording Protection System for Portable extension Technical Specification; Revision 0.92 dated November 2009.

2. Outputs

2.1 **General.** Host Devices shall not output content, or pass content received through the Service to any output, except as permitted in this Section 2 and otherwise allowed by the tru2way Middleware application. For purposes of this Exhibit, an output shall be deemed to include, but not be limited to, any transmissions to any internal copying, recording, or storage device, but shall not include internal non-persistent or transitory transmissions that otherwise satisfy these Compliance Rules and the Robustness Rules. For the purposes of this Exhibit C, the RCD bit as defined in CEA-608-C and the RCI as defined in CEA-805-B shall be set to “1” if the Redistribution Control Trigger bit is set to a value of one (1) in combination with the EMI bits set to a value of zero, zero (0,0).

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

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

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

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

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

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

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

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

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

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

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

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

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

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

2.4.1 **1394 with DTCP.** Host Device may output Controlled Content, and pass Controlled Content to an output, in digital form over IEEE 1394 interfaces as specified by the Specifications, where such output is protected by DTCP. Host Device must support DTCP "Full Authentication," and may additionally support DTCP "Restricted Authentication." When so outputting or passing such content to a DTCP-1394 output, the DTCP Source Function shall correctly map the copy control information (CCI) to the DTCP Encryption Mode Indicator (EMI), DTCP Analog Protection System (APS) signaling, DTCP Image Constraint Token (ICT), and DTCP Encryption Plus Non-assertion (EPN) signaling in accordance with the Specifications. Capitalized terms used in this Section, but not otherwise defined in this Exhibit C or the Agreement, shall have the meaning set forth in the DTCP Specification or the DTCP Adopter Agreement.

2.4.2 **DVI, HDMI, or DisplayPort with HDCP 1.0.** Host Devices may output content received through the Service, and pass content received through the Service to an output, in digital form over DVI, HDMI, or DisplayPort interfaces as specified by the Specifications, and where the output always has HDCP active and on. When so outputting or passing such content to a DVI, HDMI, or DisplayPort output, the HDCP Source Function shall pass content received through the Service to such output in digital form only when it has securely verified that the HDCP Source Function has signaled that it is engaged and able to deliver protected content, which means (i) HDCP protection is operational and always active on all DVI, HDMI, or DisplayPort outputs; and (ii) there is no HDCP device on such output whose Key Selection Vector is in a SRM. Capitalized terms used in this Section, but not otherwise defined in this Exhibit

C or the Agreement, shall have the meaning set forth in the HDCP Specification or the HDCP License Agreement.

- 2.4.3 **HDCP 2.0.** Host Devices may output content received through the Service, and pass content received through the Service to an output, in digital form using HDCP 2.0 as defined above (including the approved interfaces identified therein), where the output always has HDCP active and on. When so outputting or passing such content to such outputs the HDCP Source Function shall pass content received through the Service to such output in digital form only when it has securely verified that the HDCP Source Function has signaled that it is engaged and able to deliver protected content, which means (i) HDCP protection is operational and always active on all such outputs; and (ii) there is no HDCP device on such output whose Key Selection Vector is in a SRM. Capitalized terms used in this Section, but not otherwise defined in this Exhibit C or the Agreement, shall have the meaning set forth in the HDCP 2.0 Specifications or the HDCP License Agreement.
- 2.4.4 **DTCP-IP.** Host Devices may output Controlled Content, and pass Controlled Content to an output in digital form where such output is protected by DTCP-IP. When so outputting or passing such content to a DTCP-IP output, the DTCP Source Function shall map the copy control information (CCI) to the DTCP Encryption Mode Indicator (EMI), DTCP Analog Protection System (APS) signaling, DTCP Image Constraint Token (ICT), and DTCP Encryption Plus Non-assertion (EPN) signaling in accordance with the Specifications. Capitalized terms used in this Section, but not otherwise defined in this Exhibit C or the Agreement, shall have the meaning set forth in the DTCP Specification or the DTCP Adopter Agreement.
- 2.4.5 **IPRM.** Host Devices may output Controlled Content, and pass Controlled Content to an output in digital form where such output and content is protected by IP Rights Management (IPRM) system in accordance with the Motorola IPRM System Submission of New Digital Outputs and Content Protection Technologies; Revision 2.7 dated November 10, 2006, as amended, and the applicable license terms governing the implementation of IPRM as provided by Motorola, such terms including compliance with the Compliance and Robustness Rules herein.
- 2.4.6 **DRI with an Approved DRM.** Host Devices that conform to the OCUR Specification may output content, and pass content, in digital form over the DRI. One or more of the approved Digital Rights Management (DRM) systems listed in this Section 2.4.5 must be included in the OCUR implementation. No other outputs, other than a single DRI-compliant output, may exist on the OCUR. Approved DRMs, and limitations, include the following DRMs, as amended by CableLabs from time to time:
- 2.4.5.1 **Microsoft Windows Media Digital Rights Management (WMDRM).** Content may be output over the DRI protected by Microsoft WMDRM in accordance with the DRI Content Protection Requirements set forth in the OCUR Specification, where connected to a device that runs Microsoft Windows Media Center Edition (a “MCE HMS”) and such MCE HMS complies with (1) the OEM Compliance Letter between CableLabs and the MCE HMS manufacturer, such compliant devices posted at www.opencable.com, and (2) the Redacted Agreement between Microsoft and CableLabs dated Dec 12, 2005.
- 2.4.5.2 **Real Helix DRM.** Content may be output over the DRI protected by Real Helix DRM in accordance with the DRI Content Protection Requirements set forth in the OCUR Specification, where connected to a device that runs Microsoft Windows Media Center Edition (a “MCE HMS”) and such MCE HMS complies with (1) the OEM Compliance Letter between CableLabs and the MCE HMS manufacturer, such compliant devices posted at www.opencable.com, (2)

the Redacted Agreement between RealNetworks and CableLabs dated April 6, 2006; and (3) the Redacted Agreement between Microsoft and CableLabs dated Dec 12, 2005.

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

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

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

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

Provided Licensee complies with the foregoing provisions of this Section 2.6, this Section 2.6 shall not prohibit a Host Device or Licensed Component from incorporating legitimate features (i.e., zooming, scaling, cropping, picture-in-picture, compression, recompression, image overlays, overlap of windows in a graphical user interface, audio mixing and equalization, video mixing and keying, downsampling, upsampling, and line doubling, or conversion between widely-used formats for the transport, processing and display of audiovisual signals or data, such as between analog and digital formats and between PAL and NTSC or RGB and Y,Pb,Pr formats, as well as other features as may be

added to the foregoing list from time to time by CableLabs by amendment to these Compliance Rules) that are not prohibited by law, and such features shall not be deemed to strip, interfere with or obscure the Consensus Watermark in Controlled Content.

3 Copying, Recording, and Storage of Controlled Content

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

Host Devices shall be designed and manufactured to be able, when required by the OCAP application, to obliterate the stored content or render unusable the stored content after a stated period of time (as identified by the OCAP application), on a frame-by-frame, minute-by-minute, megabyte-by-megabyte basis.

3.5 Copy One Generation.

- 3.5.1 Host Devices may make a copy of Controlled Content that is designated in the EMI bits as permissible to be copied for one generation (“Copy One Generation”), as provided in section 3.2 or the first sentence of 3.4.1 or provided that the copy (a) is scrambled, encrypted or uniquely bound to that device, in each case using a form of copy protection that is identified by an amendment to this section 3.5, if any, and (b) is remarked as not to be further copied (“copy no more”) in a manner that is set forth in section 3.5 or 3.6, and will be effective to prevent such further copies being made by devices capable of receiving a transmission of such remarked data through the outputs identified in section 2.4. In the absence of either such amendment to this section 3.5, no copy of such Controlled Content other than as permitted in sections 3.2, the first sentence of 3.4.1, or 3.6, may be made.
- 3.5.2 A Host Device that makes a copy of content marked in the CCI as “Copy One Generation” in accordance with this Section 3.5 may move such content to a single removable recording medium, or to a single external recording device, only when (a) the external recording device indicates that it is authorized to perform this Move function in accordance with the requirements of this Section, and to copy such Controlled Content in

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

3.5.3 **VCPS.** In accordance with Section 3.5.1, Host Devices may make a copy of Controlled Content that is designated 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.

3.5.4 **CPDO.** In accordance with Section 3.5.1, Host Devices may make a copy of Controlled Content that is designated as Copy One Generation providing such copy is protected using CPDO in accordance with the EnCentrus Content Protected Digital Output Port System Description; Revision 1.2 dated January 2006 and the draft license terms governing the implementation of CPDO as provided in CPDO License Agreement dated December 20, 2005, such terms including compliance with the Compliance and Robustness Rules herein.

3.5.5 **RPSP.** In accordance with Section 3.5.1, Host Devices may make a copy of Controlled Content that is designated as Copy One Generation providing such copy is protected using RPSP. Host Devices may also make a copy of Controlled Content that is signaled to have redistribution control asserted providing such copy is protected using RPSP. Such copies produced using RPSP shall be made in accordance with the Recording Protection System for Portable extension Technical Specification; Revision 0.92 dated November 2009 and the license terms governing the implementation of RPSP as provided in the Recording Protection System for Portable extension Agreement dated November 2009.

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

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

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

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

device unless encrypted with security no less than AES (128 bit) or 3DES (112 bit); and (e) the move, storage and copying of Controlled Content otherwise meets the criteria set forth in the Robustness Rules and the Compliance Rules.

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

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