DIGITAL TRANSMISSION PROTECTION LICENSE AGREEMENT
Evaluation License Convertible to Product License

This DIGITAL TRANSMISSION PROTECTION LICENSE AGREEMENT, ("Agreement") is effective as of the latest date set out on the signature page hereof (the "Effective Date") by and between Digital Transmission Licensing Administrator, LLC, a Delaware limited liability company ("DTLA") and the "Adopter" which is named immediately below:

Name of Adopter:	
Description of Adopter's Business	
Location of Principal Office:	
Jurisdiction of Adopter's Formation:	
Year of Formation:	
Number of Employees:	
Amount of Capital:	

BACKGROUND

A. The Founders have developed a certain method for encryption, decryption, key exchange, authentication, and renewability for purposes of protecting certain digital content from unauthorized interception, retransmission and copying.

B. The Founders have licensed the method to DTLA for purposes of further licensing the system and administering such licenses.

C. Adopter wishes to receive a license, subject to the terms and conditions set forth in this Agreement for the purpose of developing and evaluating such method including, but not limited to, adherence to the Compliance Rules.

Therefore, DTLA and Adopter agree as follows:

AGREEMENT

1. DEFINITIONS.

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

1.1 "**Activation"** means that the Adopter has executed the Activation Notice and has paid the fees referenced in Section 2.2, which are required to activate the Adopter's manufacturing license.

1.2 **"Adopter"** means the entity named at the beginning of this Agreement and includes its Affiliates.

1.3 **"Adopter Agreement"** means this Agreement and any other Digital Transmission Protection License Agreement entered into by DTLA and any other adopter of DTCP.

1.4 **"Affiliate"** means with respect to any person or entity, any other person or entity directly or indirectly controlling or controlled by or under direct or indirect common control with such person or entity. "Control" means the possession of beneficial ownership of more than 50% of the stock or other similar interest entitled to vote for election of the Board of Directors or similar managing authority.

1.5 **"Commercial Entertainment Content"** is defined in the Compliance Rules.

1.6 **"Common Device Key and Common Device Certificate"** means a common Device Key and common Device Certificate as contemplated in Section 2.2 of the Procedural Appendix.

1.7 **"Compliance Rules"** means both the requirements set out in Exhibit B and the Robustness Rules set out in Exhibit C, as such exhibits may be amended by DTLA from time to time pursuant to Section 3.2.

1.8 **"Compliant"** refers to a product which is in compliance with all applicable Compliance Rules and, in the case of a product that incorporates a common Device Key or common Device Certificate, is also in compliance with Section 2.2 of the Procedural Appendix.

1.9 **"Confidential Information"** means Proprietary Information that is either marked "confidential" or "proprietary" when disclosed in written form or indicated as "confidential" or "proprietary" when disclosed orally and confirmed in writing within thirty (30) days after such disclosure.

1.10 **"Content Participant"** means a company which has executed a Content Participant Agreement with DTLA, or with an entity authorized by DTLA to execute such agreements. DTLA will identify such companies periodically.

1.11 **"Content Participant Agreement"** means any Content Participant Agreement entered into by a provider of Commercial Entertainment Content and DTLA or any entity authorized by DTLA to execute a Content Participant Agreement.

1.12 **"Device Certificate"** means a cryptographically encoded value which may be provided by DTLA or its designee which authorizes a device to exchange certain Commercial Entertainment Content.

1.13 **"Device Keys"** means cryptographic values which may be provided by DTLA or its designee for use in devices, and include the "Private Device Key" and the "Public Device Key" and keys associated with Restricted Authentication, all identified in the Specification.

1.14 "**DTCP**" means that certain method for encryption, decryption, key exchange, authentication and renewability for purposes of protecting certain digital content from unauthorized interception and copying which method is described in the Specification.

1.15 **"DTCP Associates"** means entities which have executed an agreement relating to the handling and redistribution of Licensed Components and who are designated as DTCP Associates by DTLA. DTLA will identify such entities periodically.

1.16 **"Fellow Adopters"** means the Founders and any other entity which has executed an Adopter Agreement and delivered it to DTLA or its designee.

1.17 **"Founders"** means Hitachi Maxell, Ltd., Intel Corporation, Panasonic Corporation, Sony Corporation, and Toshiba Corporation.

1.18 **"Generator"** means DTLA or an entity that has been retained by DTLA to generate Device Certificates and Device Keys for use by Adopters.

1.19 **"Highly Confidential Information"** means Proprietary Information that is marked "Highly Confidential Information" when disclosed in written form or is otherwise designated as such hereunder**.**

1.20 **"Interface"** means the protocols (including cryptographic algorithms), packet formats, and data structures disclosed in the Specification.

1.21 **"Licensed Component"** means a product, such as an integrated circuit, circuit board, or software module, which is designed to be assembled into a Licensed Product and which embodies a portion of the Specification (including, for avoidance of doubt, a product that incorporates a Device Key or Device Certificate), and which does not embody the entirety of the Specification or does not completely satisfy the Compliance Rules.

1.21.1 **"Licensed Component (Schedule 1)"** means a Licensed Component which is in any way not Compliant, other than a Licensed Component (Schedule 2) or as otherwise specifically permitted hereunder.

1.21.2 **"Licensed Component (Schedule 2)"** means a Licensed Component which is not Compliant only to the extent that it outputs Decrypted DT Data (as defined in the Compliance Rules) in decompressed form which output is not compliant with Section 4, Part I of Exhibit B.

1.22 **"Licensed Product"** means a product, including a hardware device or software application, which:

1.22.1 Embodies the designs set out in the Specification,

1.22.2 Is Compliant, and

1.22.3 Is designed for the transmission and/or receipt of digital transmissions comprising Commercial Entertainment Content.

1.23 **"Necessary Claims"** means claims of a patent or patent application relating to the Interface that must be infringed in order to make a product that complies with the Interface, which are owned or controlled by DTLA, any Founder, Adopter or any Fellow Adopter, any Content Participant or any of their respective Affiliates. "Necessary Claims" do not include any claims relating to semiconductor manufacturing technology; claims relating to aspects of any technology, standard or product that is not itself part of the Specification (including, by way of example, CSS, MPEG, IEEE 1394 and analog copy protection systems) even though such technology, standard or product may otherwise be mentioned or required by the Specification or Compliance Rules; claims with regard to which it would be possible to build a product in compliance with the Interface without infringing such claim (even if in the same patent as Necessary Claims); or claims which, if licensed, would require a payment of royalties by the licensor to unaffiliated third parties.

1.24 **"Procedural Appendix"** means that document of the same name attached hereto which is hereby incorporated into this Agreement by reference, as may be amended by DTLA from time to time.

1.25 **"Proprietary Information"** means any and all information relating to the Specification made available to Adopter directly by DTLA or its designees or representatives, or by any Fellow Adopter including, without limitation, specifications, software, hardware, firmware, documentation, designs, flow charts, technical data, outlines, blueprints, notes, drawings, prototypes, templates, systems, manuals, know-how, processes and methods of operation.

1.26 "**Robust Inactive Product**" means a product or component that (i) does not contain a Device Key, (ii) is designed not to have its DTCP functions be activated except by an Update, and (iii) is no less secure from circumvention (including but not limited to modification and/or compromise of Confidential Information or Highly Confidential Information) than Licensed Products are required to be hereunder. By way of example, a product or component consisting of software object code manufactured by Adopter shall be deemed a Robust Inactive Product if (x) if the portions implementing DTCP (including any portion of DTCP) are encrypted using a commercially reasonable strength of encryption and the keys necessary to decrypt and use such portions are not made available to any person or entity other than Adopter and (y) the product or component does not contain a Device Key.

1.27 **"Robust Licensed Component"** means a Licensed Component that is designed to be modified via an Update to become, or designed to be incorporated via an Update into, a Licensed Product and that (i) complies with all applicable Robustness Rules and all other applicable Compliance Rules, (ii) is designed in such a way that unless such Robust Licensed Component is modified to become, or is incorporated into, a Licensed Product by means of Update, such Robust Licensed Component shall not be able to transmit via any digital output any content using DTCP or any components thereof, or decrypt or encrypt any content using DTCP, and (iii) shall upon distribution of such Robust Licensed Component and at such time as such Robust Licensed Component (as distributed) is modified to become, or is incorporated into, a Licensed Product, be no less secure from interception of Device Keys, Device Certificates and Decrypted DT Data, and from circumvention (including but not limited to modification and/or compromise of Confidential Information or Highly Confidential Information) than Licensed Products are required to be

hereunder. By way of example, Licensed Components consisting of software object code shall be deemed Robust Licensed Components if the object code is encrypted using a commercially reasonable strength of encryption and the keys necessary to decrypt and use such code are made available only to Fellow Adopters, DTCP Associates and Have Made Parties, or such Licensed Components are capable of being Updated and the DTCP functions are only activated when contained in a Licensed Product (i.e., the resultant product meets all of the requirements that a Licensed Product was required to meet at the time the Licensed Components were distributed).

1.28 **"Robustness Rules"** means the requirements set out in Exhibit C, as such exhibit may be amended by DTLA from time to time pursuant to Section 3.3.

1.29 **"Specification"** means the specification entitled "5C Digital Transmission Content Protection " release 1.2 as may be amended from time to time pursuant to Section 3.3.

1.30 **An "Update"** means, with respect to a Licensed Product or Robust Licensed Component or a Robust Inactive Product distributed by a Fellow Adopter (a "Distributed Adopter Product"), the distribution by a Fellow Adopter of a Licensed Product or Robust Licensed Component (the "Adopter Update") to modify or replace such Distributed Adopter Product (including but not limited to modifications that activate the DTCP functions in such Distributed Adopter Product, or replace the Device Certificate or Device Key in such Distributed Adopter Product), such that (i) the resultant product (i.e., the Distributed Adopter Product as modified or replaced by the Adopter Update) shall be a Licensed Product or Robust Licensed Component (i.e., shall comply with all of the requirements that Licensed Products or Robust Licensed Components, as the case may be, were required to meet at the time the Distributed Adopter Product was distributed) and (ii) upon distribution of the Adopter Update, and upon modification or replacement of the Distributed Adopter Product, such Adopter Update and Distributed Adopter Product shall be no less secure from interception of Device Keys, Device Certificates and Decrypted DT Data and from circumvention (including but not limited to modification and/or compromise of Confidential Information or Highly Confidential Information) than Licensed Products are required to be hereunder. By way of example but not limitation, an Update may take place by means of an on-line download of a Robust Licensed Component or the distribution of CD-ROM containing a Robust Licensed Component to end-users. For clarification, a " Distributed Adopter Product" and "Update" with respect thereto may be distributed at the same or different times.

2. FEES.

2.1 **Administration and Disclosure Fee**. Within thirty (30) days of the Effective Date, Adopter shall pay DTLA a nonrefundable sum in the amount of the Annual Administration Fee set out in the Procedural Appendix (the "Annual Administration Fee"). Adopter shall not be entitled to any refund thereof for any reason. Adopter shall pay DTLA the "Per Certificate Fees" set out on the Procedural Appendix in accordance with the procedures for ordering Device Certificates and Device Keys or Common Device Certificates and Common Device Keys specified in the Procedural Appendix. Upon each anniversary of the Effective Date, or such other date as specified in the Procedural Appendix (the "Annual Payment Date"), Adopter shall pay DTLA the Annual Administration Fee for the following year (or, in the final year of the Term, such portion of the Annual Administration Fee as is specified in the Procedural Appendix). DTLA may, upon at least thirty (30) days' notice to Adopter, modify the Annual Administration Fee and Per Certificate Fees payable for the period beginning on the next Annual Payment Date, provided that any increase in such fees shall not exceed an amount commensurate with any increase in DTLA's costs (including but not limited to the cost of inflation).

Without limiting the foregoing, where costs per Device Key or per Fellow Adopter decrease, DTLA shall use commercially reasonable efforts to reduce the Per Certificate Fee or Annual Administration Fee, respectively.

2.2 **Activation.** At any time after Adopter has paid the Annual Administration Fee for the initial year, or any subsequent year, of the Term for the "Small Adopter" or "Large Adopter" category (as selected by Adopter with reference to the Fee Schedule set forth in the Procedural Appendix), Adopter may execute the Activation Notice attached hereto as Exhibit D in accordance with the procedures set out in Exhibit D. Prior to Activation, Adopter is not licensed to distribute any products or components hereunder, and the provisions of Sections 5.2, 5.3, 5.4, 6.1, 6.2 and 6.3 shall only be applicable after Activation. Any Evaluation Fee (as set out in the Procedural Appendix) which Adopter has paid hereunder for the year in which Adopter elects Activation shall be credited as provided in such Activation Notice against the Annual Administration Fee for such year payable upon Activation.

2.3 **Device Certificate and Device Keys.** Device Certificates and Device Keys are necessary to manufacture Licensed Products. These are generated under the direction of DTLA and, except in the case that Adopter elects to use a Common Device Certificate and Common Device Key for certain devices as described in the Procedural Appendix and Compliance Rules, are generated uniquely per device. Without limiting any other provision of this Agreement, Adopter may not use the same Device Key or Device Certificate in more than one individual unit or copy of any product or component except for the use of Common Device Keys and Common Device Certificates in accordance with Section 2.2 of the Procedural Appendix. Following Activation, Device Keys and Device Certificates shall be made available according to the fee schedule set out in the Procedural Appendix, as updated from time to time in accordance with the terms of this Agreement. Prior to Activation, facsimile Device Certificates and facsimile Device Keys shall be issued to Adopter for development purposes. Adopter is cautioned that such facsimile cryptographic materials will not inter-operate with commercial devices. Without limiting any other provision of the Agreement, Adopter may replace or cause the replacement of Device Certificates and Device Keys by Update.

3. SPECIFICATION; COMPLIANCE RULES; USERS GROUP.

3.1 **Delivery**. Upon Adopter's execution hereof and DTLA's receipt of the applicable fee(s), DTLA shall cause to be distributed to Adopter the relevant portions of Proprietary Information and/or the Specification that Adopter has not previously received.

3.2 **Acknowledgement.** Adopter agrees to provide copies of the Specification, Compliance Rules and Robustness Checklist to those persons having supervisory responsibility for the design and manufacture of Licensed Products and Licensed Components for and on behalf of Adopter, in such manner and at such times as to promote Adopter's compliance with all applicable terms thereof.

3.3 **Changes.** The Specification and the Compliance Rules may be amended from time to time by DTLA only in accordance with this Section 3.3. Adopter shall be required to comply with all amendments (a) to the Compliance Rules and Section 2.2(i)(y) of the Procedural Appendix within twelve (12) months after notification of the changes has been sent as specified herein or, in extraordinary cases, within such shorter or longer period specified by DTLA and (b) to the Specification within eighteen (18) months after such notice. Changes in the Procedural Appendix, with the exception of changes to Section 2.2(i)(y), the Annual Administration Fees and Per Certificate Fees, shall be effective on no less than thirty (30) days' notice. Changes to the Annual

Administration Fees or Per Certificate Fees shall be permitted only as set out in Section 2.1. In the case of individual units or copies of Robust Licensed Components, Robust Inactive Products or of Licensed Products that are capable of being Updated and are shipped by Adopter after the effective date of such amendment, the requirements of this Section 3.3 may be met by ensuring that the required changes are implemented in such Robust Licensed Components, Robust Inactive Products and Licensed Products through an Update by or at the direction of Adopter before the DTCP functions of such Licensed Products, Robust Inactive Products and Robust Licensed Components may be used for the first time. Notwithstanding the foregoing, in the event Adopter issues, after the effective date of any such amendment, an Update to a Licensed Product or Robust Licensed Component or Robust Inactive Product that was distributed prior to the effective date of such amendment, the Update and the Licensed Product or Robust Licensed Component or Robust Inactive Product as Updated shall not be required to comply with such amendment, provided that it (a) is not a Different Licensed Product, (b) complies with all applicable provisions of the Specification and Compliance Rules in effect at the time such Licensed Product or Robust Licensed Component or Robust Inactive Product was distributed, and (c) where applicable, complies with Section 3.5.

For purposes of this Section 3.3, a "Different Licensed Product" means, with respect to an Update applied to a Licensed Product, a resulting Licensed Product that is the same as a Licensed Product that (x) is separately marketed by Adopter under a new product name or a higher numerical designation to the left of the decimal point (e.g., the change from Version 1.0 to Version 2.0, but not to Version 1.9), and (y) either--

(i) enables DTCP protection of a service that would not have been protectable with DTCP by the Licensed Product prior to the Update, or

(ii) performs the DTCP functions by substantially different means and in a substantially different way than was performed by the Licensed Product prior to the Update.

3.3.1 DTLA shall not make any material changes to the Specification (including any changes that would expand the Specification to require new technical features, not included in version 1.2 of the Specification or such later version of the Specification as may be in effect as of the Effective Date, that would create compatibility problems with Licensed Products manufactured prior to such changes); provided, however, that DTLA may make such limited changes, if any, in the Specification as would permit DTCP to be used with transports other than those permitted in version 1.2 of the Specification (or such later version of the Specification as may be in effect as of the Effective Date), which may include but are not limited to USB and MOST. Without limiting the foregoing, DTLA reserves the right to correct any errors or omissions in the Specification or to make changes that would clarify, but not materially amend, alter or expand the Specification, from time to time.

3.3.2 Adopter shall manufacture all Licensed Products that implement revocation with the capacity to store, in accordance with the provisions of this Agreement, a revocation list of no less than one kilobyte (1KB) as set forth in Section 7.1.2 of the Specification.

3.3.3 Except as DTLA, in consultation with owners of Commercial Entertainment Content, may conclude is necessary to ensure and maintain content protection, DTLA shall not make any revisions to the Compliance Rules that would materially increase the cost or complexity of implementations of Licensed Products. Without limiting the foregoing, DTLA shall provide the members of the CPIF (defined in Section 3.4) with at least thirty (30) days' notice of any material changes to the Compliance Rules.

3.4 **Content Protection Implementers Forum.** Adopter has the right to be a member of and to participate in a Content Protection Implementers Forum ("CPIF"), which DTLA shall convene, with which it may exchange views and information regarding DTCP. Members of the CPIF will have the right to participate in interoperability tests for DTCP and review and comment on proposed revisions to the Compliance Rules set forth in a notice from DTLA pursuant to Section 3.3.3.

3.5 **Most Current Update.** At any time that Adopter activates the DTCP functions of a unit or copy of a Licensed Product via an Update or replaces a Device Key of a unit or copy of a Licensed Product via an Update, Adopter shall issue one or more Updates to such unit or copy as necessary so as to cause the resulting product to include the changes that would have resulted if the copy or unit had received all sequential Updates designed for, and capable of properly functioning with, such copy or unit since the time the copy or unit was first distributed, provided, that if Adopter has, at any time, made available two or more versions of any such sequential Updates on different business terms (e.g., a free version and a fee-based version), the foregoing requirement shall apply with respect to the version of the Update(s) selected by the user of such unit or copy.

3.6 **Limitation for Licensed Products with Common Device Key.** Adopter shall not first activate the DTCP functions of a unit or copy of a Licensed Product that uses a Common Device Key more than eight (8) years after the particular version or model of such Licensed Product first was distributed, provided that a unit or copy of a particular version or model of such Licensed Product for which the DTCP functions were first activated during such eight-year period may be reactivated via an Update as permitted under Section 2.2(i)(y) of the Procedural Appendix. In the event that Adopter reasonably concludes that a software application containing or consisting of a copy of Licensed Product that uses a common Device Key and whose DTCP functions were first activated during such eight (8)-year period on a particular device was subsequently re-installed on the same device, the activation or re-activation of the DTCP functions of such re-installed copy shall not be deemed to be a "first activation" for purposes of this Section 3.6. If a software application containing or consisting of a copy of Licensed Product that uses a Common Device Key and whose DTCP functions were first activated during such eight (8)-year period on a particular device is subsequently installed and activated via an Update on a different device, such activation of the DTCP functions of such copy installed on the different device shall be deemed to be a "first activation" for purposes of this Section 3.6, subject to the reasonableness standard of the preceding sentence.

4. REVOCATION.

4.1 **Generally.** The Specification includes means by which the Device Certificates of certain devices may be invalidated, rendering such devices with invalidated Device Certificates unable to exchange data via DTCP with Licensed Products (generally, "Revocation" or "Revoked")

4.2 **Revocation.** DTLA may revoke a Device Certificate when it is required to do so pursuant to Section 4.2.3 or it has otherwise been determined, pursuant to the procedures set forth in the Procedural Appendix, that one or more of the Revocation Criteria have been satisfied or as provided in the last sentence of Section 4.3. The "Revocation Criteria" mean the criteria set forth in Sections 4.2.1, 4.2.2 or 4.2.3:

> 4.2.1 (a) a Device Key and corresponding Device Certificate (other than a Common Device Key and Common Device Certificate) have been cloned such that the same Device Key and corresponding Device Certificate are found in more than one device or product or (b) a

Common Device Key and corresponding Common Device Certificate are found in any product or component that is not manufactured by a Fellow Adopter or is not authorized by the Fellow Adopter that ordered such Common Device Key.

4.2.2 a Device Key and corresponding Device Certificate have been lost, stolen, intercepted or otherwise misdirected, or made public or disclosed in violation of an Adopter Agreement; or

4.2.3 DTLA is required to revoke a Device Certificate by the National Security Agency, court order, or other competent government authority.

4.2.4 Without limiting the foregoing, DTLA shall not Revoke a Device Certificate (a) based on Adopter's general implementations of the Specification in a model or product line that is not Compliant or otherwise based on Adopter's breach of this Agreement (except that if Adopter has caused any of the circumstances described in Sections 4.2.1 or 4.2.2, the Device Certificate of any device or product in which such a Device Key has been included may be Revoked) or (b) to disable products or devices where the general security of DTCP has been compromised (other than as described in Sections 4.2.1 and 4.2.2) by third parties.

4.2.5 Without limiting any other provision of this Agreement, Adopter shall be entitled to replace or cause the replacement of Revoked Device Certificates by Update.

4.2.6 **Procedure.** Except as set forth in this Section 4.2.6, the procedures set out in the Procedural Appendix shall govern Revocation and any rescission or cancellation thereof. Such procedures provide for notice and review of DTLA decisions and/or actions regarding Revocation where requested. At any time commencing forty-eight (48) months following the issuance to a Fellow Adopter of a Common Device Certificate, such Common Device Certificate may be Revoked without notice.

4.3 **Remedies**. Except as otherwise expressly provided in this Section 4.3, Adopter's sole recourse with respect to Revocation shall be the objection and arbitration procedures set out in the Procedural Appendix. The Founders, Generator and Eligible Content Participants (defined below) shall each have no liability whatsoever with respect to any Revocation. Without limiting the foregoing, DTLA and the Founders shall not have any liability with respect to any Revocation, and no compensation shall be made to Adopter, except that if DTLA determines that a Revocation was performed in error by DTLA, DTLA, at the request of Adopter shall, at DTLA's discretion, (a) rescind the Revocation through substantially the same means as were used to effect the Revocation, or (b) provide for compensation to Adopter (or Adopter's affected customers) for each of its affected devices in an amount equal to the least of (i) the fair market value of each device, (ii) the cost of reworking each device to incorporate a new Device Certificate and Device Keys, (iii) $25 per device, or, (c) in the case of Revocation of a Common Device Certificate, provide Adopter without charge with a new Common Device Key and Common Device Certificate at the same level of Unit Option or Blanket Option of the Revoked Common Device Certificate, or (d) provide for an alternative method of remedial action that DTLA determines appropriate to the particular circumstances of the Revocation.

5. LICENSES.

5.1 **Development**. Adopter may possess and use the Specification for development of Licensed Products or Licensed Components. Any distribution or disclosure of the Specification or of any product made with the use of the Specification must be in compliance with the other terms hereof.

5.2 **License**. Subject to the other provisions hereof, including payment of all fees required, DTLA grants to Adopter (including its Affiliates) a nonexclusive, nontransferable, nonsublicenseable, worldwide sublicense under the Necessary Claims of the Founders, as well as under any trade secrets or copyrights embodied in the Specification to make, have made, use, import, offer to sell and sell Licensed Products and Licensed Components; provided that such sublicense shall not extend to features of a product which are not required to comply with the Specification or for which there exists a noninfringing alternative, and further does not extend to Adopter if Adopter is in violation of Section 5.3 below.

5.3 **Reciprocal Non-Assertion Agreement**. Adopter, on behalf of itself and its Affiliates, promises not to assert or maintain against DTLA or Fellow Adopters and Affiliates thereof, and accepts Fellow Adopters' promise not to assert or maintain, any claim of infringement under its or their respective Necessary Claims, as well as under any trade secrets or copyrights embodied in the Specification for (a) with respect to Fellow Adopters, the making, having made, use, import, offering to sell and sale of Licensed Products and Licensed Components and (b) with respect to the Founders and DTLA, the use of DTCP; provided that in each case such promise shall not extend to features of a product which are not required to comply with the Specification or for which there exists a noninfringing alternative, and further does not extend to any person or entity which is asserting, or whose Affiliate is asserting, a Necessary Claim against Adopter if Adopter (x) is not willfully in material breach of its obligations under the Compliance Rules or Confidentiality Agreement , or (y) is not otherwise in material breach of the Compliance Rules or Confidentiality Agreement, which breach has not been cured or is not capable of cure within thirty (30) days of Adopter's receipt of notice thereof.

5.4 **Content Participant Non Assertion**. Adopter, on behalf of itself and its Affiliates, promises not to assert or maintain against Content Participants and Affiliates thereof any claim of infringement under its or their respective Necessary Claims, as well as under any trade secrets or copyrights embodied in the Specification for Content Participants' using or causing the use of DTCP to protect Commercial Entertainment Content in compliance with their Content Participant Agreements; and accepts Content Participants' promises not to assert or maintain any claim of infringement under their respective Necessary Claims, as well as under any trade secrets or copyrights embodied in the Specification for the making, having made, use, import, offering to sell and sale of Licensed Products and Licensed Components; provided that each such promise shall not extend to features of a product which are not required to comply with the Specification or for which there exists a noninfringing alternative, and further does not extend to any person or entity which is asserting, or whose Affiliate is asserting, Necessary Claims against Adopter if Adopter (x) is not willfully in material breach of its obligations under the Compliance Rules or Confidentiality Agreement, or (y)) is not otherwise in material breach of the Compliance Rules or Confidentiality Agreement, which breach has not been cured or is not capable of cure within thirty (30) days of Adopter's receipt of notice thereof.

5.5 **Scope of Use**. This license, and the promises of non-assertion extended or accepted pursuant to Sections 5.3 and 5.4, shall, in each case, extend only to Licensed Products and to Licensed Components, only for transmission of content that, when received by the Licensed Component or Licensed Product, was protected using a Commercially Adopted Access Control Method or otherwise constitutes Commercial Entertainment Content, and under a Device Certificate issued by or under the authority of DTLA following Activation. No license is granted, express or implied, and no promises of non-assertion extended or accepted pursuant to Sections 5.3 and 5.4, for (a) aspects of any technology, standard or product that is not itself part of the Specification (including, by way of

example, CSS, MPEG, IEEE 1394 and analog copy protection systems) even though such technology, standard or product may be otherwise mentioned or required by the Specification or Compliance Rules or (b) implementation of any portion of the Specification other than for enabling the implementation of DTCP in Licensed Products.

5.6 **Proper Use.** The licenses granted herein are subject to and conditioned on the requirements that Adopter shall not produce or sell devices or software (a) under color of this Agreement, or (b) using Confidential and Highly Confidential Information, where such devices or software are designed to circumvent the requirements or effectiveness of the Specification.

6. DISTRIBUTION OF PRODUCTS

6.1 **Licensed Products.** If fully Compliant, Licensed Products may be disposed of in any commercially reasonable manner.

6.2 **Licensed Components.** Except as otherwise expressly provided in Section 6.3, Licensed Components (Schedule 1) may only be furnished to Fellow Adopters and any person or entity that is providing services to Adopter pursuant to the right under Section 5.2 to "have made" Licensed Products or Licensed Components (a "Have Made Party"). Licensed Components (Schedule 2) may only be furnished to Fellow Adopters, DTCP Associates and Have Made Parties. Adopter shall contractually bind any Have Made Party to sell, distribute or otherwise dispose of Licensed Components furnished by or made for Adopter only to Adopter.

6.3 **Robust Licensed Components.** Robust Licensed Components may be disposed of in any commercially reasonable manner.

7. CONFIDENTIALITY.

7.1 **Treatment.** Adopter shall comply with the terms of Exhibit A ("the Confidentiality Agreement"). The portions of the Specification marked "Confidential" are to be treated as Confidential Information under the Confidentiality Agreement, and the materials designated by DTLA as "Highly Confidential" shall be treated as specified by the Confidentiality Agreement.

7.2 **Compliance with Laws, Export**. Adopter will comply with all applicable rules and regulations of the United States, Japan and other countries and jurisdictions, including those relating to the export or re-export of commodities, software and technical data insofar as they relate to the activities under this Agreement. Adopter agrees that commodities, software and technical data provided under this Agreement are subject to restrictions under the export control laws and regulations of the United States, Japan and other countries and jurisdictions, as applicable, including but not limited to the U.S. Export Administration Act and the U.S. Export Administration Regulations and the Japanese Foreign Exchange and Foreign Trade Law, and shall obtain any approval required under such laws and regulations whenever it is necessary for such export or re-export.

8. TERM/TERMINATION.

8.1 **Termination**. This Agreement shall be effective upon the Effective Date and, unless sooner terminated in accordance with this section 8, shall continue until the fifth anniversary of the Effective Date and shall thereafter automatically renew for successive one-year terms and remain in effect unless terminated in accordance with this section 8:

8.1.1 **Termination Without Cause**.

(a) By Adopter. Adopter shall have the right to terminate this Agreement at any time, with or without cause, upon ninety (90) days' prior written notice to DTLA.

(b) By DTLA. DTLA shall have the right to terminate this Agreement at any time, with or without cause, upon at least one hundred and eighty (180) days' prior written notice to Adopter, provided that, to the extent DTLA has the same or a similar termination right with other Fellow Adopters, DTLA exercises such right on a non-discriminatory basis with respect to Adopter and all such other Fellow Adopters.

8.1.2 **Termination for Cause.**

(a) Breach Capable of Cure. In the event that either party (i) materially breaches any of its obligations hereunder, which breach is not cured within thirty (30) days after written notice is given to the breaching party specifying the breach or (ii) repeatedly breaches any of its obligations hereunder and fails to cure and cease committing such repeated breaches within thirty (30) days after being given written notice specifying the breaches, then the party not in breach may, by giving written notice thereof to the breaching party, terminate this Agreement, upon the expiration of a thirty (30)-day period beginning on the date of such notice of termination. Notwithstanding the foregoing, DTLA shall not terminate this Agreement for reason that a Robust Inactive Product manufactured or distributed by Adopter would not comply with the Compliance Rules if its DTCP functions were activated, provided that, no later than thirty (30) days after receiving notice of breach from DTLA, Adopter prevents activation of the DTCP functions of such Robust Inactive Product until such time, if any, that an Update is applied to such Robust Inactive Product that causes it to be a Licensed Product in accordance with the terms of Section 3.3.

(b) Breach Not Capable of Cure. In the event of a material breach that is not capable of cure under the provisions of Section 8.1.2(a), the party not in breach may, by giving written notice of termination to the breaching party, terminate this Agreement. Such termination shall be effective upon receipt of such notice of termination.

8.2 **Effect of Termination.** Upon termination or expiration of this Agreement, Adopter shall immediately cease use of Device Certificates and Device Keys. Within thirty (30) days after termination or expiration of this Agreement, Adopter shall return such Device Certificates and Device Keys and shall as directed by DTLA: (i) return all other Proprietary Information to DTLA; or (ii) destroy all Proprietary Information in its possession, retaining no copies thereof, and certify such destruction in writing to DTLA. Within thirty (30) days after termination or expiration of this Agreement, Adopter shall discontinue all manufacture, sale, or distribution of Licensed Products and Licensed Components. Notwithstanding the foregoing, in the event that Adopter, prior to the date of such termination or expiration, manufactures, distributes or sells to persons or entities Robust Inactive Products, Adopter shall have the right to continue to manufacture, distribute and sell the same version of such Robust Inactive Products after such termination or expiration for a period of up to two (2) years, or such longer period as DTLA may, in extraordinary circumstances, approve in writing, provided that the DTCP functions in any such Robust Inactive Products sold or distributed after the date of such termination shall not be activated.

8.3 **Survival**. Following termination of this Agreement for any reason, the following Sections shall survive: 4.2.6, 4.3, 5.3 and 5.4 (both with respect to the Specification in effect as of the date of termination), 7, 8.2, this Section 8.3, 9, 10, and 11.

9. DISCLAIMER AND LIMITATION OF LIABILITY.

9.1 **Generally.** The following terms limit the ability of the Adopter to recover any damages from DTLA or the Founders in excess of fees actually paid to DTLA by Adopter. These provisions are an essential part of the bargain, without which DTLA would not be willing to enter into this Agreement, nor would the Founders be willing to license their Necessary Claims to DTLA.

9.2 **Disclaimer.** ALL INFORMATION, MATERIALS, KEYS, AND CERTIFICATES ARE PROVIDED "AS IS." DTLA AND THE FOUNDERS AND GENERATOR MAKE NO REPRESENTATIONS OR WARRANTIES, EXPRESS, IMPLIED, STATUTORY OR OTHERWISE, AND EXPRESSLY DISCLAIM IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE AND ANY EQUIVALENTS UNDER THE LAWS OF ANY JURISDICTION THAT MIGHT ARISE FROM ANY ACTIVITIES OR INFORMATION DISCLOSURES RELATING TO THIS AGREEMENT. DTLA, THE FOUNDERS AND GENERATOR FURTHER DISCLAIM ANY WARRANTY THAT ANY IMPLEMENTATION OF THE SPECIFICATION, IN WHOLE OR IN PART, WILL BE FREE FROM INFRINGEMENT OF ANY THIRD PARTY INTELLECTUAL PROPERTY OR PROPRIETARY RIGHTS.

9.3 **Limitation of Liability**. NEITHER DTLA NOR THE FOUNDERS NOR GENERATOR NOR ANY DIRECTOR, OFFICER, AGENT, MEMBERS, REPRESENTATIVES, EQUIVALENT CORPORATE OFFICIAL, OR EMPLOYEE OF ANY OF THEM ACTING IN THEIR CAPACITIES AS SUCH (COLLECTIVELY, THE "AFFECTED PARTIES") SHALL BE LIABLE TO ADOPTER FOR ANY DIRECT, INDIRECT, INCIDENTAL, CONSEQUENTIAL, SPECIAL OR PUNITIVE DAMAGES ARISING OUT OF ANY CAUSE OF ACTION RELATING TO THIS AGREEMENT, OR BASED ON MAKING, USING, SELLING OR IMPORTING ANY PRODUCTS OF ADOPTER THAT IMPLEMENT PROPRIETARY INFORMATION OR DTCP, WHETHER UNDER THEORY OF CONTRACT, TORT, INDEMNITY, PRODUCT LIABILITY OR OTHERWISE. TO THE EXTENT THAT ANY COURT OF COMPETENT JURISDICTION RENDERS JUDGMENT AGAINST DTLA NOTWITHSTANDING THE ABOVE LIMITATION, THE AFFECTED PARTIES' AGGREGATE LIABILITY TO ADOPTER IN CONNECTION WITH THIS AGREEMENT SHALL IN NO EVENT EXCEED THE AMOUNTS OF MONEY RECEIVED BY DTLA FROM ADOPTER UNDER THIS AGREEMENT IN ANY ONE YEAR PERIOD.

10. REMEDIES.

10.1 **Indemnification for Wrongful Acts of Adopter**. Adopter shall indemnify and hold DTLA, the Founders and Generator, and their officers, members, representatives, agents, directors, equivalent corporate officials, and employees, harmless from and against any and all any losses, claims, actions, suits, proceedings or litigation, and any losses, deficiencies, damages, liabilities, costs and expenses including without limitation, reasonable attorneys' fees and all related costs and expenses, to be paid or otherwise incurred in connection with the defense of any claim, action, suit, proceeding or litigation, which result from any material breach of any covenant, agreement, representation or warranty herein or negligent acts committed by Adopter.

10.2 **Records Audit and Inspection**. DTLA shall have the right, at reasonable times and intervals, to have audited Adopter's books and records to ascertain the propriety of any payment hereunder. Such audit shall be undertaken at the auditing party's sole expense, and the auditor, who shall be a Certified Public Accountant from a major accounting firm, shall only disclose those matters which

the auditing party has the right to know under this Agreement, and the results of the audit shall be deemed confidential.

10.3 **Device Inspection**. DTLA may acquire products distributed hereunder on the open market for examination. Adopter shall provide reasonable cooperation in affording DTLA an example of any product distributed hereunder if requested, and Adopter shall provide, once per model of product, and under the terms of a non-disclosure agreement equivalent to that document referred to by DTLA as the Evaluation NDA, the service manual for such product in order to assist in evaluation of it. Adopter may, at its option provide further information.

10.4 **Equitable Relief**. DTLA and Adopter agree and acknowledge that due to the unique nature of certain provisions hereof and the lasting effect of and harm from a breach of such provisions, including making available the means for widespread unauthorized copying of copyrighted content intended to be protected using the Specification, if Adopter breaches its obligations hereunder, money damages alone may not adequately compensate an injured party, and that injury to such party may be irreparable, and that specific performance or injunctive relief is an appropriate remedy to prevent further or threatened breaches hereof, provided, however, that injunctive relief shall not be available to prevent the distribution of a Robust Inactive Product that would not comply with the Compliance Rules if its DTCP functions were activated if, no later than thirty (30) days after receiving notice of breach from DTLA, Adopter prevents activation of the DTCP functions of such Robust Inactive Product until such time, if any, that an Update is applied to such Robust Inactive Product that causes it to be a Licensed Product in accordance with the terms of Section 3.3. Notwithstanding the preceding sentence, Adopter agrees that DTLA shall be entitled to seek injunctive relief to prevent further or threatened breaches of this Agreement if Adopter has engaged in a pattern of behavior involving the repeated release of non-compliant products or components for which Adopter received notice of the breach, whether or not Adopter corrected such repeated breaches following such notice.

10.5 **Damages Measure and Limitation.** The parties agree that it would be impossible to estimate the amount of damages in the event of certain breaches. In the event of a material breach by Adopter (1) of the Confidentiality Agreement, Adopter shall be liable for one million dollars; (2) that involves the manufacture or distribution of devices or software, including but not limited to an Update, that fail to protect Device Keys and Device Certificates as provided by the applicable Compliance Rules or as required by Section 6.2 or 6.3 or the requirements hereunder applicable to Updates, Adopter shall be liable in an amount equal to its profits on such devices or software, and in no event less than one million dollars nor more than eight million dollars; and (3) that involves any other provision of this Agreement, Adopter shall be liable in an amount equal to its profits on the affected devices or software, and in no event more than eight million dollars. The amounts payable by Adopter in accordance with this Section 10.5 shall be DTLA's exclusive monetary remedies available for any and all such breaches by Adopter, and such amounts shall be paid by Adopter in lieu of any and all other monetary damages to DTLA relating to such breaches. For purposes of this Section 10.5, a series of substantially related events shall constitute a single material breach. A breach shall be "material" only if it has resulted in or would be likely to result in commercially significant harm to other users of DTCP, including but not limited to Fellow Adopters and Content Participants, or constitute a threat to the integrity or security of DTCP. In addition, the following is a non-exclusive list of circumstances in which, standing alone, there is no material breach of the applicable provisions by Adopter: (1) if no Confidential Information or Highly Confidential Information was released to a third party not permitted hereunder to have such information or could reasonably have been expected to have been released to such third party as a result of the breach; (2) if Adopter maintains an internal

program to assure compliance herewith (including a program to assure maintenance of inventory, samples, and confidentiality of information for purposes in addition to compliance with this Agreement), the breach was inadvertent or otherwise unintentional, and the breach did not have a material adverse effect on the integrity or security of DTCP or the function of DTCP to protect Commercial Entertainment Content; (3) if Adopter brought the breach to DTLA's attention in a timely manner as required by this Agreement and such breach did not have a material adverse effect on the integrity or security of DTCP or the function of DTCP to protect Commercial Entertainment Content.

10.6 **Third-Party-Beneficiary Rights.** Compliance of Adopter and other licensees with the terms hereof is essential to maintain the value, integrity, security and performance of DTCP. As part of the consideration granted herein, upon Activation, Adopter agrees that each Content Participant that (i) distributes or transmits, or causes or authorizes the distribution or transmission of, its Commercial Entertainment Content in commercial quantities, or via mass distribution channels such as satellite or cable transmission, to the general public in a form that would, in the course of a transmission up to and including the display or other performance of such Commercial Entertainment Content, use a channel protected by DTCP ("Eligible Content") and (ii) at such time (x) is not willfully in material breach of any term or condition of its Content Participant Agreement, and (y) is not otherwise in material breach of any term or condition of its Content Participant Agreement, which breach has not been cured, or is not capable of cure, within thirty (30) days of Content Participant's receipt of notice thereof by DTLA or any Fellow Adopter (an "Eligible Content Participant"), shall be a third-party beneficiary of this Agreement and shall be entitled, during such period that such Content Participant is an Eligible Content Participant, to bring a claim or action to enforce rights against Adopter in accordance with the procedures set out in the Procedural Appendix with respect to Adopter's implementation of DTCP in any product that receives or transmits data in a format in which Content Participant has made Eligible Content available. Such rights shall be limited to seeking injunctive relief against the manufacture, distribution, commercial use and sale of Adopter's products that are in material breach of the Compliance Rules, and against disclosure of Highly Confidential Information in breach of this Agreement that affects the integrity or security of DTCP, except where such Adopter has willfully breached, or engaged in a pattern or practice of breaching, such obligations, as to which breach attorneys' fees and costs shall be awarded to each Eligible Content Participant that is a prevailing party. Notwithstanding the provisions of this Section 10.6, injunctive relief shall not be available to an Eligible Content Participant to prevent the distribution of a Robust Inactive Product that would not comply with the Compliance Rules if its DTCP functions were activated if, no later than thirty (30) days after receiving notice of breach from DTLA, Adopter prevents activation of the DTCP functions of such Robust Inactive Product until such time, if any, that an Update is applied to such Robust Inactive Product that causes it to be a Licensed Product. Notwithstanding the preceding sentence, Adopter agrees that an Eligible Content Participant shall be entitled to seek injunctive relief to prevent further or threatened breaches of this Agreement if Adopter has engaged in a pattern of behavior involving the repeated release of non-compliant products or components for which Adopter received notice of the breach, whether or not Adopter corrected such repeated breaches following such notice.

10.7 **Adopter Claims.** Following Activation, and while Adopter (i) is not willfully in material breach of any term or condition of this Agreement, and (ii) is not otherwise in material breach of any term or condition of this Agreement, which breach has not been cured, or is not capable of cure, within thirty (30) days of Adopter's receipt of notice thereof by DTLA, Adopter shall be a third-party beneficiary of each Content Participant Agreement and shall be entitled to bring a claim or action to

enforce rights against a Content Participant, in accordance with the third-party-beneficiary procedures set out in the Procedural Appendix, with respect to such Content Participant's compliance with its obligations under Section 5 of its Content Participant Agreement; provided that such rights, pursuant to such Content Participant Agreement, shall be limited to seeking equitable relief, except where such Content Participant has willfully breached, or engaged in a pattern or practice of breaching, such obligations, as to which breach attorneys' fees and costs shall be awarded to each Adopter that is a prevailing party.

11. MISCELLANEOUS.

11.1 **Ownership**. All Proprietary Information and media containing Proprietary Information as provided by DTLA to Adopter shall remain the property of DTLA or its suppliers. Except as expressly provided herein, this Agreement does not give Adopter any license or other right to the Proprietary Information.

11.2 **Entire Agreement**. This Agreement, the exhibits hereto and the Specification constitute the entire Agreement between the parties hereto with respect to the subject matter hereof and supersede all prior oral, written or other agreements. Except as otherwise provided herein, this Agreement may not be modified except by written agreement dated subsequent to the date of this Agreement and signed by both parties.

11.3 **Controlled Entities**. Adopter represents and warrants that it has, or will have, the authority to bind its Affiliates to the terms of this Agreement.

11.4 **Money.** All fees shall be paid to DTLA or to its order in United States dollars by wire transfer or such other means as DTLA may reasonably specify. If Adopter is required by law to make any withholding from fees due to DTLA, it may make such withholding but shall provide DTLA, at the time of payment, with evidence of such withholding adequate to permit DTLA or its assignee to claim relevant tax credits under applicable treaties.

11.5 **Assignment**. The licenses granted hereunder are personal to Adopter, and Adopter's rights under this Agreement shall not be assigned or otherwise transferred except (a) with the written approval of DTLA (which shall not be unreasonably withheld) or (b) to a corporation controlling, controlled by or under common control with Adopter or to the purchaser of all or substantially all of the outstanding capital stock or assets and obligations of Adopter or to the surviving entity in a merger, reorganization, or other business combination and where notice of such assignment has been provided in advance to DTLA and where the surviving or acquiring company agrees in writing to be bound by this Agreement. Subject to the limitations set forth in this Agreement, this Agreement will inure to the benefit of and be binding upon the parties, their successors and permitted assigns. DTLA may assign or transfer this Agreement to a party that agrees to assume DTLA's obligations hereunder, and will provide Adopter with written notice thereof.

11.6 **Presumptions**. In construing the terms of this Agreement, no presumption shall operate in either party's favor as a result of its counsel's role in drafting the terms or provisions hereof.

11.7 **Governing Law; Jurisdiction**. THIS AGREEMENT, AND ALL THIRD-PARTY-BENEFICIARY CLAIMS BROUGHT PURSUANT HERETO, SHALL BE GOVERNED BY AND CONSTRUED IN ACCORDANCE WITH THE LAWS OF THE STATE OF NEW YORK APPLICABLE TO AGREEMENTS MADE AND TO BE PERFORMED ENTIRELY IN SUCH

STATE AND WITH THE LAWS OF THE UNITED STATES AS WOULD BE CONSTRUED BY A COURT SITTING IN THE SOUTHERN DISTRICT OF NEW YORK.

11.7.1 IN CONNECTION WITH ANY LITIGATION BETWEEN THE PARTIES HERETO OR IN CONNECTION WITH ANY THIRD-PARTY-BENEFICIARY CLAIM BROUGHT HEREUNDER ARISING OUT OF OR RELATING TO THIS AGREEMENT, EACH PARTY IRREVOCABLY CONSENTS TO: (i) THE EXCLUSIVE JURISDICTION AND VENUE IN THE FEDERAL AND STATE COURTS LOCATED IN THE COUNTY OF NEW YORK, NEW YORK (EXCEPT THAT CLAIMS BROUGHT PURSUANT TO SECTION 10.6 OR 10.7 MAY BE BROUGHT IN A COURT SITTING IN LOS ANGELES COUNTY, CALIFORNIA); AND (ii) THE SERVICE OF PROCESS OF SAID COURTS IN ANY MATTER RELATING TO THIS AGREEMENT BY PERSONAL DELIVERY OR BY MAILING OF PROCESS BY REGISTERED OR CERTIFIED MAIL, POSTAGE PREPAID, AT THE ADDRESSES SPECIFIED IN THIS AGREEMENT, OR TO THE AGENT TO BE APPOINTED PURSUANT TO THE SECTION, BELOW;

11.7.2 ADOPTER SHALL APPOINT AN AGENT IN THE STATE OF NEW YORK FOR ACCEPTANCE OF SERVICE OF PROCESS PROVIDED FOR UNDER THIS AGREEMENT AND SHALL NOTIFY DTLA OF THE IDENTITY AND ADDRESS OF SUCH AGENT WITHIN THIRTY (30) DAYS AFTER THE EFFECTIVE DATE

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

11.8 **Notice**. All notices to be provided pursuant to this Agreement shall be given in writing and shall be effective when either served by personal delivery or upon receipt via certified mail, return receipt requested, postage prepaid, overnight courier service or sent by facsimile transmission with hard copy confirmation sent by certified mail, in each case to the party at the addresses set out herein.

11.9 **Severability; Waiver**. Should any part of this Agreement judicially be declared to be invalid, unenforceable, or void by any court of competent jurisdiction, the parties agree that the part or parts of this Agreement so held to be invalid, unenforceable, or void shall be reformed by such court without further action by the parties hereto but only to the extent necessary to make such part or parts valid and enforceable. A waiver by either of the parties hereto of any of the covenants to be performed by the other party or any breach thereof shall not be effective unless made in writing and signed by the waiving party and shall not be construed to be a waiver of any succeeding breach thereof or of any covenant herein contained.

11.10 **Most Favored Status.** DTLA will make available to Adopter its substantive commitments or clarifications regarding the standard Adopter Agreement through notice on the DTLA website or otherwise. DTLA also commits that the benefit of any of its clarifications or interpretations of

language in the standard Adopter Agreement will be extended to Adopter in accordance with this Section 11.10. Where DTLA agrees to make a change to a particular Fellow Adopter's standard Adopter Agreement, such change shall be reflected in the next regular revision of the standard Adopter Agreement and Adopter will be given the ability to upgrade to such revised Adopter Agreement. Prior to such time as it makes a revised or upgraded standard Adopter Agreement available to all Fellow Adopters that have executed a standard Adopter Agreement, where DTLA has agreed to include language in a particular Fellow Adopter's standard Adopter Agreement that is more favorable than that in the then-current version of the standard Adopter Agreement, DTLA will not enforce the language in Adopter's Adopter Agreement to the extent that such language is less favorable than that found in such Fellow Adopter's Adopter Agreement. For purposes of this Section 11.10, "standard Adopter Agreement" refers to an Adopter Agreement under which a Fellow Adopter receives a license with respect to activities that are the same as those activities licensed hereunder, but does not include, by way of example and not limitation, any Adopter Agreement in which a Fellow Adopter is not licensed to manufacture Licensed Products.

IN WITNESS WHEREOF, the parties have executed this Agreement as of the date first above written.

DTLA:	**Adopter:**
By:_____	**By:**_____
Name:_____	**Name:**_____
Title:_____	**Title:**_____
Date:_____	**Date:**_____

Addresses for notices:

DTLA:
c/o License Management International, LLC

380 Tennant Avenue, Unit #4

Morgan Hill, CA 95037

Adopter:

Procedural Appendix

Unless otherwise expressly stated in this Procedural Appendix, all section references in this Procedural Appendix are references to sections of this Procedural Appendix.

Fee Schedule

A. Annual Administration Fee

Adopter may select whichever category of license it prefers. Adopter is encouraged to select the category of license which it finds most financially efficient. Adopter may (i) downgrade its elected category not more than once per year upon providing DTLA thirty (30) days prior written notice, provided that, such Adopter shall not be entitled to any refund of the Annual Administration Fee paid for such period; or (ii) upgrade its elected category upon providing DTLA thirty (30) days prior written notice and the full Annual Administration Fee associated with such upgraded category. Future Annual Administration Fees owed by such Adopter shall be due on the anniversary of the effective date of Adopter's notice, provided that the Annual Administration Fee payable for the last year of the Term shall be pro-rated based on the number of months remaining in the Term.

Category	Annual Administrative Fee (US $)
Component Supplier Fee	$14,000
Evaluation Fee	$10,000
Adopter-Small	$14,000
Adopter-Large	$18,000

B. Certificate Fees

(i). Unique Device Certificates

An Adopter in the category of Adopter-Small or Adopter-Large may order Device Keys and Device Certificates as unique certificates (i.e., a different certificate for each device).

CATEGORY	Per Unique Certificate Fee	
	Order Format 1 Order Format 5 Full	Order Format 3 Restricted/Full
Small Adopter	.06	.07
Large Adopter	.05	.06

Shipping and Handling - $200.00 / order

(ii). Common Device Certificates

An Adopter in the category of Adopter-Large may order Common Device Keys and Common Device Certificates, in Unit Options or Blanket Options.

(a) Under the Unit Options, a particular Common Device Certificate may be used in no more than the number of units or copies, as specified below, of the same Licensed Product or Robust Licensed Component. Such "same" Licensed Product or Robust Licensed Component may include, for purposes of assessment of fees under this Fee Schedule, units or copies that are substantially identical but are marketed under different names or model designations, and units or copies that have different version numerical designations to the right of the decimal point. If within a given year Adopter wishes to use the same Common Device Certificate in a greater number of units or copies than would have been permitted under its original order, Adopter shall provide DTLA with an amended Order Form indicating the new desired maximum number of units or copies and, when invoiced by DTLA, shall pay the difference between the fees under the original and amended orders. However, Adopter may order no more than 4 sets of Common Device Keys and Common Device Certificates within a year under the option to obtain no more than 4 keys to be used in a maximum of 20,000 units or copies.

(b) Any Adopter that orders one or more Common Device Certificate(s) pursuant to a Unit Option shall maintain accurate records of the number of Devices into which each Common Device Certificate was implemented by or with the authorization of Adopter. Adopter agrees to permit DTLA to audit those records at Adopter's place of business during normal business hours within sixty (60) days of receipt of written notice from DTLA of DTLA's intent to conduct said audit, or at such other place and time as may be mutually agreed by DTLA and Adopter. Adopter shall not be required to undergo an audit more than once during a single calendar year. Such audit may cover the three-year period preceding the audit. During said audit, Adopter shall provide the auditor with complete access to the aforementioned records and to records of shipments and sales of all products that incorporate DTCP for the period covered by the audit, and shall provide all reasonable assistance to the auditors. Such audits shall be conducted by an independent auditor hired by DTLA and shall be conducted pursuant to generally accepted auditing standards. The costs to DTLA of the audit shall be borne by DTLA, except that if any such audit should reveal that any Common Device Certificate was implemented in more than the number of products covered by the selected Unit Option (other than by a de minimis amount), Adopter shall pay DTLA's costs of such audit, as well as pay the discrepancy in fees. Adopter's failure to comply with any provisions of this paragraph shall constitute a material breach of this Adopter Agreement.

(c) Under the Blanket Option, Adopter can order up to 5 Common Device Certificates for a flat annual fee, with an option to purchase additional Common Device Certificates for $1,000 each. Each Common Device Certificate can be used in an unlimited number of units or copies.

Per Common Certificate Fee (Large Adopter Only)
Unit Options Up to a maximum of 4 keys/total 20,000 units or copies -- $1,000 Up to 100,000 units or copies -- $2,000 Up to 200,000 units or copies -- $4,000 Up to 500,000 units or copies -- $6,000 Up to 1,000,000 units or copies -- $10,000 Up to 2,000,000 units or copies -- $12,000 Up to 5,000,000 units or copies -- $15,000 Up to10,000,000 units or copies -- $25,000 Up to 30,000,000 units or copies -- $50,000 Blanket Option Up to a maximum of 5 Common Device Keys and Common Device Certificates -- $100,000 Additional Common Device Keys and Common Device Certificates -- $1,000

Shipping and Handling - $200.00 / order

C. PGP key registration fee

The fee for replacing a PGP key is $3000.00

D. Fee for additional Hard Copies of the Specification

The fee for additional Hard Copies of the Specification which are Confidential Information or Highly Confidential Information is $500.00 per copy

1. PROCEDURES FOR HANDLING DEVICE CERTIFICATES AND DEVICE KEYS

Private Device Keys, keys associated with Restricted Authentication, and, random seed values associated with the keying material are Highly Confidential Information and Adopters must protect them from exposure and loss using methods that equivalent to or exceed that which is used by DTLA

to deliver them to the Adopter and at a minimum that they are kept in a secure controlled environment with controlled access.

2. PROCEDURE FOR ORDERING DEVICE CERTIFICATES AND DEVICE KEYS; REQUIREMENTS FOR USE OF COMMON DEVICE CERTIFICATES AND COMMON DEVICE KEYS

2.1 Adopter will be supplied with a form and associated tools for ordering Device Certificates and Device Keys. As set out in the Specification, such Device Certificates will reflect certain capabilities of the device into which they are intended to be installed. The number of Device Certificates and Device Keys which may be ordered will be constrained to the Adopter's reasonably anticipated production run rate.

2.2 Common Device Certificates and common Device Keys may be used only in Licensed Products or Robust Licensed Components

(i) where

(x) such common Device Keys and common Device Certificates are (a) implemented in software, firmware or a combination of software and firmware; and (b) are or will be capable of being replaced, via an Update, by valid Device Certificates and valid Device Keys, including if and when such original common Device Keys and common Device Certificates are Revoked; and

(y) the DTCP functions in each individual unit or copy of such Licensed Product or of a Licensed Product incorporating such Robust Licensed Component cease to function no later than one (1) year after the DTCP functions of such unit or copy first functioned, unless the common Device Key and corresponding common Device Certificate in such individual units or copies were sooner replaced via an Update, in which event the DTCP functions shall cease to function no later than one (1) year from the date of such replacement or any subsequent replacement via an Update. Without limiting the last sentence of Section 2.3 of the Agreement, in the event the DTCP functions of such individual units or copies so cease to function, Adopter may thereafter reactivate or cause the reactivation of such DTCP functions by an Update that replaces the Common Device Key and corresponding Common Device Certificate in such unit or copy with a new Device Key and corresponding Device Certificate, in which event the DTCP functions shall cease to function no later than one (1) year after such replacement or any subsequent replacement via an Update; and

(z) each such Common Device Certificate and Common Device Key is not used in connection with the activation of the DTCP functions of a Licensed Product more than one (1) year after the first activation of a Licensed Product using such Common Device Certificate and Common Device Key;

or

(ii) that are not capable of performing Sink Functions (and, in the case of Robust Licensed Components, not capable of becoming or being incorporated into Licensed Products that perform Sink Functions), that have Source Functions that are part of remotely-managed devices (e.g., set-top

boxes, smartcard-controlled devices or devices using renewable software), and that have Common Device Keys and Common Device Certificates that are capable of being replaced, via an Update, by valid Device Keys and valid Device Certificates if and when such original Common Device Keys and Common Device Certificates are revoked..

3. REVOCATION PROCEDURES

The procedures set forth in this Section 3 shall apply to Revocation other than Revocation of Common Device Certificates as contemplated in the last sentence of Section 4.2.6.

3.1 **Notice of Revocation.** In the event that Revocation is requested, DTLA shall provide any Fellow Adopter to whom DTLA or its designee had issued a Device Certificate for which Revocation has been requested with notice of such requested Revocation, provided, however, that DTLA may, in its sole discretion, reduce such notice period where it deems circumstances warrant. If Adopter notifies DTLA in writing that Adopter consents to such Revocation of any Device Certificate issued to it hereunder, or if DTLA is required to Revoke pursuant to Section 4.2.3 of the Agreement, DTLA may take steps to Revoke the applicable Device Certificate.

3.2 **Assent to Revocation/Dispute Resolution.**

3.2.1.1 No more than fifteen (15) calendar days after the date of notice from DTLA, Adopter shall notify DTLA whether Adopter desires to contest the grounds for such Revocation. If Adopter notifies DTLA that it does not wish to contest the requested Revocation, or if Adopter fails to respond timely to the notice from DTLA, the Revocation shall be deemed to be without objection and may proceed. If Adopter timely notifies DTLA of its intent to object to the requested Revocation, Adopter shall submit a written statement, under oath, which sets out any facts which disprove or contradict DTLA's stated grounds for Revocation ("Revocation Objection"). Within ten (10) business days after receipt of the Revocation Objection, DTLA shall provide notice of the Revocation Objection and the Revocation Objection itself to the entity that requested the Revocation. Within thirty (30) days after receipt from the DTLA of the notice of the Revocation Objection, the entity or entities that requested Revocation (the "Revocation Initiators") may initiate an arbitration in accordance with the provisions of Section 3.4 to determine whether the requested Revocation may proceed.

3.2.1.2 **Request for Revocation**. Adopter may seek Revocation by providing proof in a sworn affidavit (the "Adopter Affidavit") of any of the facts relating to any particular Device Certificate and/or associated Device Keys issued to Adopter hereunder that would warrant Revocation of such certificate and satisfy one or more of the Revocation Criteria. The Adopter Affidavit shall be sufficiently detailed that DTLA can determine solely on the basis of such affidavit whether the facts averred on their face would satisfy one or more of the Revocation Criteria.

3.3 **Indemnification.** If Adopter has sought Revocation, it shall indemnify and hold harmless and, at DTLA's option, defend DTLA, the Founders, Generator, any Content Participant that carries the Revocation Information applicable to such Revocation and each of their officers, directors, equivalent corporate officials, employees, representatives and agents ("Indemnified Parties") from and against any and all (i) claims, actions, suits, proceedings or litigation and any losses, deficiencies, damages, liabilities, costs and expenses associated therewith, including but not limited to reasonable

attorneys' fees and expenses, arising out of the Revocation or rescission of Revocation of any Device Certificate for which Adopter had sought Revocation and (ii) other costs or expenses incurred by DTLA and/or such Content Participant in connection with such Revocation or rescission of Revocation, including but not limited to any costs and expenses associated with the generation and distribution of information necessary to effect such revocation or rescission and any amounts paid by DTLA to Adopters (or to Adopters' affected customers) or any other party on account of such Revocation. DTLA may require a bond or security reasonably anticipated for such costs.

3.4 **Arbitration Procedures.**

3.4.1 The parties to the arbitration shall be the Revocation Initiators, the affected Fellow Adopter(s), if any, that objected to the Revocation in accordance with their respective Adopter Agreement and/or any affected person or entity that such Fellow Adopter(s) may designate (such Fellow Adopters and designees, collectively, the "Affected Adopters") and/or at its election, DTLA (collectively, the "Arbitrating Parties"). The Revocation Initiators shall bear the burden of proof in demonstrating, by a preponderance of the evidence, that one or more of the Revocation Criteria have been satisfied.

3.4.2 There shall be a sole arbitrator, who shall be selected by the Arbitrating Parties from the National Panel of Commercial Arbitrators of the American Arbitration Association within fourteen (14) days of the initiation of arbitration; provided, however, that in the event the Arbitrating Parties cannot agree on a sole arbitrator within such fourteen (14)-day period, the Revocation Initiators, on the one hand, and the other Arbitrating Parties, on the other hand, shall each, promptly thereafter, select one arbitrator from the National Panel of Commercial Arbitrators of the American Arbitration Association and those two arbitrators shall jointly select a third arbitrator from the National Panel of Commercial Arbitrators of the American Arbitration Association, who shall serve as the presiding arbitrator and chairperson of such arbitration.

3.4.3 The arbitration shall be conducted in Los Angeles, California, in accordance with the International Arbitration Rules of the American Arbitration Association. The language of the arbitration shall be English.

3.4.4 The arbitrator(s) may conduct the arbitration in such manner as he, she or they shall deem appropriate, including the imposition of time limits that he, she or they consider(s) reasonable for each phase of the proceeding, but with due regard for the need to act, and make a final determination, in an expeditious manner. The arbitrator(s) shall set a schedule to endeavor to complete the arbitration within one (1) month.

3.4.5 The arbitrator(s) shall permit and facilitate such limited discovery as he, she or they shall determine is reasonably necessary, taking into account the needs of the Arbitrating Parties and the desirability of making discovery as expeditious and cost-effective as possible, recognizing the need to discover relevant information and that only one party may have such information.

3.4.6 The Arbitrating Parties and the arbitrator(s) shall treat the arbitration proceedings, any related discovery, documents and other evidence submitted to, and the decision of, the arbitrator(s) as Confidential Information. In addition, and as necessary, the arbitrator(s) may issue orders to protect the confidentiality of proprietary information, trade secrets and other sensitive information disclosed in discovery or otherwise during the arbitration.

3.4.7 Any decision by the arbitrator(s) shall be final and binding on the Arbitrating Parties, except that whether the arbitrator(s) exceeded his, her or their authority, as specifically described in this Agreement, shall be fully reviewable by a court of competent jurisdiction. Judgment upon any award shall be entered in a court of competent jurisdiction.

3.4.8 The arbitrator(s) shall be compensated at his, her or their hourly rates, determined at the time of appointment, for all time spent in connection with the arbitration, and shall be reimbursed for reasonable travel and other expenses. The arbitrator(s) shall determine all costs of the arbitration, including the arbitrator(s)' fees and expenses, the costs of expert advice and other assistance engaged by the arbitrator(s), the cost of a transcript and the costs of meeting and hearing facilities.

3.4.9 The arbitrator(s) is (are) empowered solely to determine (a) whether one or more of the Revocation Criteria have been satisfied and (b) if so, only in the circumstance set forth in clause (x) of this Section 3.4.9, whether Revocation is warranted. Any such determination by the arbitrator(s) shall be final and binding on the parties to the arbitration and on DTLA if it is not a party to the arbitration, except that whether the arbitrator(s) exceeded his, her or their, authority as specifically described in this Section 3.4.9, shall be fully reviewable by a court of competent jurisdiction. In any such arbitration, the Affected Adopter(s), if any, may introduce evidence solely to support the position that one or more of the Revocation Criteria have not been satisfied. In the event that the Arbitrator(s) determine(s) that the Revocation Criteria set forth in Section 4.2.2 of the Agreement have been satisfied, (x) if DTLA is a party to the arbitration and objects to Revocation, it shall have the burden of demonstrating, by a preponderance of the evidence, that Revocation is not warranted, and if DTLA fails to meet such burden, Revocation shall be deemed warranted and (y) if DTLA is not a party to the arbitration, Revocation shall be deemed to be warranted. In the event that the arbitrator(s) determine(s) that the Revocation Criteria set forth in Section 4.2.1 of the Agreement have been satisfied, Revocation shall be deemed warranted.

3.4.10 All costs and fees shall be shared equally as between the Revocation Initiators, on the one hand, and the Affected Adopters, if any, that participate in the arbitration, on the other, provided, however, the arbitrator(s) may otherwise apportion such costs and fees among such Revocation Initiators and Affected Adopters, if any, as the arbitrator(s) may determine.

3.4.11 The prevailing party in such arbitration shall provide to DTLA a copy of the arbitrator(s) decision. If, pursuant to this Section 3.4, Revocation is warranted, DTLA may, after it receives such decision, take steps to cause such Revocation.

4. PROCEDURES FOR THIRD PARTY BENEFICIARY CLAIMS

4.1 Prior to initiating or instituting any third-party-beneficiary claim by a Fellow Adopter ("Adopter Beneficiary Claim" or by a Content Participant ("Content Participant Beneficiary Claim") (each, a "Beneficiary Claim") against Adopter, any other Fellow Adopter or a Content Participant, as the case may be (each, a "Defendant"), a Content Participant Beneficiary (defined below) or Adopter Beneficiary (defined below) (each, a "Third-Party Beneficiary") shall provide DTLA notice and consultation reasonable under the circumstances regarding a proposed Beneficiary Claim; provided that such consultation with DTLA shall not affect such Third-Party Beneficiary's discretion in initiating such a Beneficiary Claim. Such Third-Party Beneficiary shall further provide DTLA with notice of actual filing of a Beneficiary Claim and, upon DTLA's request, any copies of material documents to be filed in such Third-Party Beneficiary's initiation or pursuit of such Beneficiary Claim. DTLA shall cooperate reasonably with such Third-Party Beneficiary in providing appropriate

and necessary information in connection with the Beneficiary Claim to the extent that such cooperation is consistent with the preservation of the integrity and security of DTCP and to the extent such cooperation does not involve release of information provided to DTLA by a Content Participant or Fellow Adopter that such Content Participant or Fellow Adopter has designated to DTLA to be its confidential and proprietary information. Documents provided to DTLA under these third-party-beneficiary procedures shall not include any documents filed or to be filed under seal in connection with such Beneficiary Claim.

4.1.1 "Adopter Beneficiaries" means Adopter (for so long as Adopter is in compliance with all of the terms and conditions of this Agreement), together with any one (or more) other Fellow Adopters that is (or are) eligible to bring third-party-beneficiary claims in accordance with a Content Participant Agreement.

4.1.2 "Content Participant Beneficiaries" means any one (or more) Content Participant(s) that is (or are) eligible to bring third-party-beneficiary claims against Adopter in accordance with Section 10.6 of the Agreement or against other Fellow Adopters in accordance with comparable provisions of their respective Adopter Agreements.

4.2 DTLA shall provide all Fellow Adopters (in the case of an Adopter Beneficiary Claim) and all Content Participants (in the case of a Content Participant Beneficiary Claim) with prompt notice of DTLA's receipt of any notice of a Beneficiary Claim against a Defendant (a "Claim Notice"). Within thirty (30) days of the date of mailing of a Claim Notice, all Adopter Beneficiaries (in the case of an Adopter Beneficiary Claim), or all Content Participant Beneficiaries (in the case of a Content Participant Beneficiary Claim), shall elect whether to join such Beneficiary Claim, and the failure of any Fellow Adopter or Content Participant to provide written notice to DTLA of such election and to move to join such Beneficiary Claim within such thirty (30)-day period shall be deemed a waiver of such Fellow Adopter's or Content Participant's third-party-beneficiary right under its respective Adopter Agreement or Content Participant Agreement, as the case may be, with respect to all Beneficiary Claims against Defendant arising out of the alleged breach by Defendant raised in such Beneficiary Claim asserted by the Third-Party Beneficiary. The Third-Party Beneficiary instituting or initiating a Beneficiary Claim shall support, and Defendant shall not object to, any motion to so join by such Third-Party Beneficiaries electing to join such Beneficiary Claim within such thirty (30)-day period. Any judgment entered upon such Beneficiary Claim shall be binding on all Fellow Adopters and Content Participants that failed to join such Beneficiary Claim as if they had joined such Beneficiary Claim. Neither any Fellow Adopter's or Content Participant's failure to notify or consult with or to provide copies to DTLA, nor DTLA's failure to give notice to any Fellow Adopter or Content Participant pursuant to these third-party-beneficiary procedures, shall be a defense against any Beneficiary Claim or grounds for a request to delay the granting of any preliminary relief requested.

4.3 Third-Party Beneficiaries shall have no right to, and Adopter agrees that it will not, enter into any settlement that: (i) amends any material term of any Adopter Agreement or Content Participant Agreement; (ii) has an adverse effect on the integrity, performance and/or security of DTCP or on the operation of DTCP with respect to protecting Commercial Audiovisual Content from any unauthorized output, transmission, interception or copying, or the rights of Content Participants with respect to DTCP; or (iii) affects any of DTLA's or the Founders' rights in and to DTCP or any

intellectual property right embodied therein, unless DTLA shall have provided prior written consent thereto.

4.4 Nothing contained in these third-party-beneficiary procedures is intended to limit remedies or relief available pursuant to statutory or other claims that a Third-Party Beneficiary may have under separate legal authority.

EXHIBIT "A"
CONFIDENTIALITY AGREEMENT

1. PERMITTED USE.

1.1 For avoidance of doubt, all references to "Proprietary Information" in this Agreement shall be deemed to include Confidential Information and Highly Confidential Information.

1.2 **Use Restrictions**.

1.2.1 Adopter shall use Proprietary Information (and tangible embodiments thereof) solely for purposes of its own implementation of DTCP in accordance with the terms of this Agreement, and shall not intentionally copy, and shall not intentionally memorize, Proprietary Information in order to copy the methods disclosed therein.

1.2.2 Adopter shall not use any mentally-retained recollections of Proprietary information to circumvent the methods disclosed in Proprietary Information or to circumvent any obligations under this Agreement.

1.3 The use restrictions contained in Section 1.2.1 of this Confidentiality Agreement shall not apply to Proprietary Information that Adopter can demonstrate is or becomes or has become generally known to the public through no breach of Adopter's obligations owed to DTLA hereunder or the Founders and which DTLA failed to remove from public availability or to enjoin such public disclosure within 120 days after the date such information is or becomes generally known as set forth above; provided, that nothing in this Section 1.3 shall be deemed to create a license (express, implied, or otherwise) under any intellectual property right of DTLA or the Founders with respect to the use of such Proprietary Information.

2. CONFIDENTIALITY.

2.1 **Highly Confidential Information.** Adopter shall maintain the confidentiality of Highly Confidential Information in the following manner:

2.1.1 Adopter shall employ procedures for safeguarding Highly Confidential Information at least as rigorous as Adopter would employ for its own most highly confidential information, such procedures to include, at a minimum: (1) maintaining on Adopter's premises a secure location in which any and all Highly Confidential Information shall be stored; (2) such secure location shall be accessible only by authorized employees; (3) employees shall sign in and out each time such employees visit such secure location; and (4) when Highly Confidential Information is not in use, such information shall be stored in a locked safe at such secure location.

2.1.2 Adopter may disseminate Highly Confidential Information only to (a) the strictest minimum possible number of regular employees and individuals retained as regular independent contractors subject to confidentiality obligations equivalent to those applicable to regular employees of Adopter: (1) who have an absolute need to know such Highly

Confidential Information in order to enable Adopter to implement DTCP in compliance with the Specification; and, (2) who are bound in writing by obligations of confidentiality sufficient to protect the Highly Confidential Information in accordance with the terms of this Agreement; provided that Adopter shall be liable to DTLA for any failure by any such employee or individual to maintain the confidentiality of Confidential Information in accordance with the terms of this Confidentiality Agreement; and, (b) a third party that is providing services to Adopter pursuant to the right under Section 5.2 of the Agreement to "have made" Licensed Products or Licensed Components, provided that such third party is either a Fellow Adopter or has executed a nondisclosure agreement with DTLA consistent with the provisions hereof that authorizes such third party to receive such Highly Confidential Information.

2.1.3 Adopter shall not make any copies of any Highly Confidential Information, except where (i) copying of Cryptographic Constants which are Highly Confidential Information is necessary for the production process of Licensed Component or Licensed Product, or (ii) Adopter has a secure document access control system which provides security level equivalent to what is required in this section 2.1, in which case Adopter may scan the DTLA Highly Confidential Information into their system. Adopters may also request additional copies of Specification documents which are Highly Confidential Information, and DTLA may in its sole discretion fulfill any such request.

2.2 **Confidential Information**. Adopter may disclose Confidential Information only to (i) regular employees and individuals retained as independent contractors subject to confidentiality obligations equivalent to those applicable to regular employees of Adopter who have a reasonable need-to-know and are bound in writing by obligations of confidentiality sufficient to protect the Confidential Information in accordance with the terms of this Agreement, (ii) Fellow Adopters, (iii) entities subject to a non-disclosure agreement with DTLA or Adopter that includes provisions substantially in the form of the provisions of this Confidentiality Agreement that relate to Confidential Information, provided that Adopter may disclose to such parties only information that such parties are entitled to receive under their Adopter Agreement or nondisclosure agreement and, in the event that any such entity is not a Fellow Adopter, Adopter shall be liable for any failure by such entity to maintain the confidentiality of Confidential Information in accordance with the terms of this Confidentiality Agreement; or (iv) Adopter's attorneys, auditors or other agents who owe Adopter a duty of confidentiality and are bound to maintain such information in confidence as a result of a fiduciary relationship. Adopter shall use the same degree of care, but no less than a reasonable degree of care, to avoid unauthorized disclosure or use of Confidential Information as such party employs with respect to its comparably important confidential information. Notwithstanding the foregoing, Adopter and DTLA may disclose Adopter's status (or lack of it) as a licensee of DTCP, and such disclosure shall not constitute Confidential Information.

3. GENERAL.

3.1 Adopter shall make all reasonable efforts to assist DTLA in relation to any claim, action, suit, proceeding, or litigation with respect to any improper or unauthorized acts of any of its former employees or of such third parties identified in Section 2.1 and 2.2 of this Confidentiality Agreement.

3.2 Contact Person and Provision of DTCP Information. Adopter shall designate a single main employee contact and an alternate employee license contact who shall receive all Confidential Information and Highly Confidential Information (the "Adopter Contact(s)") disclosed by DTLA.

3.3 Notification of Unauthorized Use or Disclosure. Adopter shall notify DTLA in writing immediately upon discovery of any unauthorized use of Proprietary Information and any unauthorized disclosure of Confidential Information or Highly Confidential Information, and will cooperate with DTLA in every reasonable way to regain possession of Confidential Information and Highly Confidential Information and prevent its further unauthorized disclosure and to prevent further unauthorized use of Proprietary Information.

3.4 **Disclosure Required by Law.** If Adopter is required by law, regulation or order of a court or other authority of competent jurisdiction to disclose Confidential Information or Highly Confidential Information, Adopter shall notify DTLA as promptly as possible, and shall, upon such DTLA's request, reasonably cooperate in challenging or restricting the scope of such required disclosure.

3.5 **Confidentiality Exceptions**. The confidentiality restrictions contained in Section 2.10 and 2.2 of this Confidentiality Agreement shall not apply to information that Adopter can demonstrate: (i) is either Confidential or Highly Confidential Information which is or becomes or has become generally known to the public through no breach of Adopter's obligations owed to DTLA hereunder or the Founders and which DTLA failed to remove from public availability or to enjoin such public disclosure within 120 days after the date such information is or becomes generally known as set forth above; or (ii) is or has been developed by Adopter's employees (whether independently or jointly with others) without having reliance on or use of (whether directly or through any intermediaries) to any such Confidential Information or Highly Confidential Information (or any translation, derivation or abstractions of Confidential Information or Highly Confidential Information) and without any breach of Adopter's obligations to DTLA or the Founders, provided that the confidentiality restrictions shall continue to apply to Device Keys provided to Adopter; or (iii) is or has been disclosed to Adopter by a third party which had developed (whether independently or jointly with others) such information without reliance on or use of (whether directly or through any intermediaries) to any Confidential Information or Highly Confidential Information and without any breach of any such third party's obligations to DTLA or the Founders.

4. PERIOD.

The confidentiality obligations set forth herein shall continue until the later of (i) three (3) years after the last commercial use of DTCP by DTLA or any Fellow Adopter; or (ii) the expiration of the last copyright that protects any DTCP-encrypted/scrambled content which then exists in any country adhering to the Agreement on Trade Related Aspects of Intellectual Property Rights of the World

Trade Organization dated April 15, 1994.

5. OTHER TERMS.

Nothing herein shall be construed as an inducement or license for Adopter to reverse engineer any products of any Adopter or third party.

EXHIBIT "B": COMPLIANCE RULES

This Exhibit B is divided into two portions: "Exhibit B Audiovisual" and "Exhibit B Audio."

EXHIBIT B AUDIOVISUAL: COMPLIANCE RULES
INTRODUCTION

1. GENERALLY

1.1 This Exhibit B Audiovisual (the "Compliance Rules Audiovisual") is divided into separate Parts, which may be applicable, depending on the nature of the Licensed Product, and, in particular, on whether it has Sink Functions or Source Functions. The definitions in this Introduction to Exhibit B Audiovisual apply to each Part of this Exhibit B Audiovisual. Unless otherwise expressly provided, for purposes of this Exhibit B Audiovisual, all section references in any Part of this Exhibit B Audiovisual shall be deemed references to sections in such Part. For purposes of this Exhibit B Audiovisual, all references below to "Exhibit B" shall be deemed references to this Exhibit B Audiovisual.

1.2 **Implementation and Robustness.** Licensed Products shall comply with the requirements of the Specification, this Exhibit B and Exhibit C.

1.3 **Types of Functions**

1.3.1 "**Sink Function**" means the function of a Licensed Product to use DTCP to receive and decrypt Commercial Entertainment Content.

1.3.2 "**Source Function**" means the function of a Licensed Product to use DTCP to encrypt and transmit Commercial Entertainment Content.

1.3.3 A Licensed Product may have both Source Functions and Sink Functions. In such a case, the requirements applicable to Source Functions and Sink Functions shall apply to the respective portions of such Licensed Product.

1.4 For purposes of this Exhibit B Audiovisual, "Localization" shall mean implementation of RTT as specifically required by the Specifications.

1.4.1 Notwithstanding anything to the contrary in the Specifications, Adopter is not required to implement Localization for DTCP for IEEE1394 (a) in any Licensed Product manufactured prior to June 30, 2010, or (b) for any DTCP Source Devices made pursuant to government or quasi-government regulation in effect on October 1, 2005, where such regulation does not require implementation of Localization for DTCP for IEEE1394.

2. DEFINITIONS

Harmonization. Where a capitalized term is used but not otherwise defined in this Exhibit B, the meaning ascribed thereto elsewhere in the Agreement shall apply.

2.1 "Analog Sunset Content" shall mean Decrypted AACS Content and Decrypted AACS2 Content.

2.2 "Analog Sunset Token" shall mean the Analog Sunset Token defined in the Specification, used to trigger certain restrictions on the analog output of Analog Sunset Content in Licensed Products having Sink Functions.

2.3 "Analog Sunset Token Content" shall mean Decrypted DT Data for which the Analog Sunset Token has been asserted.

2.4 "BF Eligible Broadcast Television" shall mean the transmission of any service, Program or schedule of Programs, via an unencrypted digital terrestrial broadcast television transmission originating in any Broadcast Flag Jurisdiction and any substantially simultaneous re-transmission thereof made by an entity located within the country or territory in which the broadcast originated, regardless of whether such entity subjects such further transmission to an access control method.

2.5 "Bound CC Recording" shall have the meaning given in Section 2.8.2 of Part 1 of this Exhibit B.

2.6 "Broadcast Flag" shall mean, (i) for unencrypted digital terrestrial broadcast television transmissions originating in the United States, its territories and possessions, and associated commonwealths under the jurisdiction of the Federal Communications Commission, the Redistribution Control descriptor (rc_descriptor()) described in ATSC Standard A/65B: "Program and System Information Protocol for Terrestrial Broadcast and Cable" and (ii) for unencrypted digital terrestrial broadcast television transmissions originating in any other jurisdiction in which a similar law or regulation requires consumer electronics products and information technology products to respond to a flag or trigger associated with such transmissions so as to restrict unauthorized redistribution of such transmissions (such jurisdictions referenced in clauses (i) and (ii), collectively, "Broadcast Flag Jurisdictions"), such flag or trigger so identified in such law or regulation.

2.7 "Broadcast Flag Jurisdiction" shall have the meaning set forth in the definition of "Broadcast Flag."

2.8 "CC Content" shall mean an instance of Digital Entertainment Content that is associated with information indicating the Number of Permitted CC Copies for such instance of content. For the avoidance of doubt, CC Content includes content that, when Transferred from a Source Device to a Sink Device, is associated with a valid CC Field.

2.9 "CC Field" shall mean the field set out in the Specification for the Copy Count function indicating, with respect to CC Content when Transferred from a Source Device to a Sink Device, the Number of Permitted CC Copies for such content. For purposes of these Compliance Rules, a setting of the CC Field to "invalid" (0000) indicates the Number of Permitted CC Copies is not being sent to the Sink Function, and a "valid" setting of the CC Field means a setting greater than or equal to 1.

2.10 "Commercial Advertising Messages" shall mean, with respect to any service, Program, or schedule or group of Programs, commercial advertising messages other than advertising relating to such service itself or the programming contained therein, or the programming of Content Participant, or any of its Affiliates, or any advertising which is displayed concurrently with the display of any part of such Program(s), including but not limited to "bugs," "frames" and "banners."

2.11 "Commercial Audiovisual Content" shall mean Commercial Entertainment Content in the form of audiovisual works, as defined in 17 U.S.C. § 101.

2.12 "Commercial Entertainment Content" shall mean works, including audio, video, text and/or graphics, that are (a) not created by the user of the Licensed Product; (b) offered for transmission, delivery or distribution, either generally or on demand, to subscribers or purchasers or the public at large, or otherwise for commercial purposes, not uniquely to an individual or a small, private group; and (c) received (i) by a Commercially-Adopted Access Control Method or (ii) as BF Eligible Broadcast Television marked with the applicable Broadcast Flag for the Broadcast Flag Jurisdiction in which such broadcast originated, or (iii) over a Protected Free-to-Air System.

2.13 "Commercially-Adopted Access Control Method" shall mean any commercially-adopted access control method, such as CSS, Digicypher, Harmony, DBS and other commercially-adopted access control technology, including digitally-controlled analog scrambling systems, whether now or hereafter in commercial use.

2.14 "Computer Product" shall mean a device which is designed for or permits the end user to install a wide variety of commercially available software applications thereon including, but not limited to, personal computers, handheld "Personal Digital Assistants," and the like and further includes a subsystem of such a device, such as a graphics card.

2.15 "Conditional Access Delivery" shall mean any delivery of a service, Program, or schedule or group of Programs via a Commercially-Adopted Access Control Method. Without limitation, "Conditional Access Delivery" includes Prerecorded Media; a Pay Television Transmission; Pay-Per-View; Video-on-Demand; Subscription-on-Demand; Non-Premium Subscription Television and Free Conditional Access Delivery. Notwithstanding the foregoing, "Conditional Access Delivery" does not include any service, Program, or schedule or group of Programs, that is a further transmission of a broadcast transmission (i.e., an over-the-air transmission for reception by the general public using radio frequencies allocated for that purpose) that, substantially simultaneously, is made by a terrestrial television broadcast station located within the country or territory in which the entity further transmitting such broadcast transmission also is located, where such broadcast transmission is not subject to a Commercially-Adopted Access Control Method (e.g., is broadcast in the clear and supported by advertising revenues or government mandated fees, without any other charge to members of the public receiving such broadcasts), regardless of whether such entity subjects such further transmission to an access control method. Notwithstanding the foregoing, Conditional Access Delivery shall include any service, Program, or schedule or group of Programs, that both (a) was primarily authored in a format with a resolution equal to or greater than 1000i or 700p ("High Definition") and (b) is transmitted via a Commercially-Adopted Access Control Method in High Definition, provided that such service, Program, or schedule or group of Programs, is not, substantially simultaneously, transmitted in High Definition by a terrestrial broadcast station located within the same country or territory, where such broadcast transmission is not subject to a Commercially-Adopted Access Control Method.

2.16 "Consensus Watermark" shall mean the watermark technology designated as the "Consensus Watermark" by DTLA.

2.17 "Constrained Image" shall mean an image having the visual equivalent of no more than 520,000 pixels per frame (e.g., an image with resolution of 960 pixels by 540 pixels for a 16:9 aspect ratio). A Constrained Image may be attained by reducing resolution, for example, by discarding, dithering, or averaging pixels to obtain the specified value. A Constrained Image can be displayed

using video processing techniques such as line doubling or sharpening to improve the perceived quality of the image. By way of example, a Constrained Image may be stretched or doubled, and displayed full-screen, on a 1000-line monitor.

2.18 "Copy Freely" refers to Commercial Entertainment Content which, as set out in the Specification, has been encoded so that copy control using DTCP is not asserted, but which remains subject to the rights of the copyright owner.

2.19 "Copy Never" refers to Commercial Entertainment Content which, as set out in the Specification, has been encoded as "Copy Never" indicating that it is not to be reproduced.

2.20 "Copy One Generation" refers to Commercial Entertainment Content which, as set out in the Specification, has been encoded as "Copy One Generation" indicating that only one generation of copies is to be made of it.

2.21 "Decrypted AACS Content" shall mean audiovisual content that was protected by AACS and is received by a Licensed Product's Source function directly from the AACS decryption function or from a bound copy of such content made in accordance with the "Compliance Rules" of the AACS Adopter Agreement.

2.22 "Decrypted AACS2 Content" shall mean audiovisual content that was protected by AACS2 and is received by a Licensed Product's Source function directly from the AACS2 decryption function or from a bound copy of such content made in accordance with the "Compliance Rules" of the AACS2 Adopter Agreement.

2.23 "Decrypted DT Data" shall mean, with respect to any Licensed Product, DT Data that has been received by such Licensed Product's Sink Function and decrypted by such Licensed Product according to DTCP but has not been (a) protected by a one-generation copy protection technology identified or approved by DTLA pursuant to Sections 2.2.1.1 or 2.2.1.3 of Part 1 of this Exhibit B; (b) protected by a technology approved by DTLA pursuant to Section 4.4.4 of Part 1 of this Exhibit B or (c) passed to an output permitted by Part 1 of this Exhibit B.

2.24 "Digital Only Token" or "DOT" shall mean the Digital Only Token field as described in the Specification, used to trigger the limitation of output or recording of Decrypted DT Data.

2.25 "Digital Only Token Content" shall mean Decrypted DT Data for which the DOT field is asserted.

2.26 "DT Data" shall mean Commercial Entertainment Content that has been encrypted and transmitted using DTCP. For avoidance of doubt, DT Data includes Decrypted DT Data.

2.27 "EPN Field" shall mean the field or bits, described in the Specification, used to indicate that Commercial Audiovisual Content is to be protected using DTCP but that copy control restrictions are not being asserted over such content.

2.28 "Existing Model" shall mean (i) a Licensed Product or product into which a Licensed Product is integrated, all aspects of which are exactly the same in all respects (including branding and consumer model number indication assigned to such integrated device), as any Licensed Product (or

product into which a Licensed Product is integrated) manufactured and sold prior to December 31, 2010; or (ii) a software Licensed Product, all aspects of which are exactly the same in all respects (including branding and version number) as any software Licensed Product manufactured prior to December 31, 2010; provided, that changes to a product made solely for one or more of the following purposes shall be permitted: (w) to comply with the Compliance Rules or the compliance or robustness rules of another content protection technology, (x) to implement changes solely of device keys and device certificate sets, (y) to implement security patches or (z) to implement bug fixes of failures of a product to operate in accordance with such product's pre-existing product specification, shall be permitted.

2.29 "FCC Waiver Order" shall mean the Memorandum Opinion and Order of the Media Bureau of the Federal Communications Commission in In the Matter of Motion Picture Association of America, Petition for Expedited Special Relief; Petition for Waiver of the Commission's Prohibition on the Use of Selectable Output Control (47 C.F.R. § 76.1903), CSR-7947-Z, MB Docket No. 08-82 (May 7, 2010).

2.30 "Free Conditional Access Delivery" shall mean a Conditional Access Delivery, as to which viewers are not charged any fee (other than government-mandated fees) for the reception or viewing of the programming contained therein.

2.31 "High Definition Analog Form" shall mean a format that is an analog video signal which has a resolution greater than a Constrained Image.

2.32 "High Definition Analog Output" shall mean an output capable of transmitting Commercial Audiovisual Content in High Definition Analog Form.

2.33 "Image Constraint Token" shall mean the field or bits, as described in the Specification, used to trigger the output of a "Constrained Image" in Licensed Products having Sink Functions.

2.34 "Move" shall mean the transmission of Decrypted DT Data from a Licensed Product that has a Source Function to a Licensed Product that has a Sink Function pursuant to and in accordance with Section 3 of Part 1 and Section 3 of Part 2 of this Exhibit B.

2.35 "No More Copies" refers to Commercial Entertainment Content which, as set out in the Specification, has been encoded as "No More Copies," indicating that it may have originated as Copy One Generation, but that the version being transmitted is from that first generation copy and that therefore no more copies are permitted.

2.36 "Non-Premium Subscription Television" shall mean a Conditional Access Delivery of a service, or schedule or group of Programs (which may be offered for sale together with other services, or schedule or group of Programs), for which subscribers are charged a subscription fee for the reception or viewing of the programming contained therein, other than Pay Television Transmission and Subscription-on-Demand. By way of example, "basic cable service" and "extended basic cable service" in the United States (other than such programming contained therein that does not fall within the definition of Conditional Access Delivery) are "Non-Premium Subscription Television.

2.37 "Number of Permitted CC Copies" shall mean, with respect to a particular instance of content, the total number of copies that are associated with and permitted to be made of that instance of content, which number, when associated with a Bound CC Recording or other static copy of such content, shall include such Bound CC Recording or copy. By way of example, when a Sink Device receives CC Content with an associated valid CC Field indicating a Number of Permitted CC Copies of 4 and makes a Bound CC Recording thereof pursuant to Section 2.8 of Part 1 of this Exhibit B, the Number of Permitted CC Copies for such Bound CC Recording shall be 4, indicating that 3 additional copies are permitted.

2.38 "Other EPN Eligible Broadcast Television" shall mean the delivery or transmission of any service, Program, or schedule or group of Programs, that (a) is delivered or transmitted via a Commercially-Adopted Access Control Method and (b) does not fall within the definition of "Conditional Access Delivery" or "BF Eligible Broadcast Television."

2.39 "Pay-Per-View" shall mean a delivery of a single Program or a specified group of Programs, as to which each such single Program is generally uninterrupted by Commercial Advertising Messages and for which recipients are charged a separate fee for each Program or specified group of Programs. The term "Pay-Per-View" shall also include delivery of a single Program as described above for which multiple start times are made available at time intervals which are less than the running time of such Program as a whole. If a given delivery qualifies both as Pay-Per-View and a Pay Television Transmission, then, for purposes of this Agreement, such delivery shall be deemed Pay-Per-View rather than a Pay Television Transmission.

2.40 "Pay Television Transmission" shall mean a transmission of a service or schedule of Programs, as to which each individual Program is generally uninterrupted by Commercial Advertising Messages and for which service or schedule of Programs subscribing viewers are charged a periodic subscription fee, such as on a monthly basis, for the reception of such programming delivered by such service whether separately or together with other services or programming, during the specified viewing period covered by such fee. If a given delivery qualifies both as a Pay Television Transmission and Pay-Per-View, Video-on-Demand, or Subscription-on-Demand then, for purposes of this Agreement, such delivery shall be deemed Pay-Per-View, Video-on-Demand or Subscription-on-Demand rather than a Pay Television Transmission

2.41 "Prerecorded Media" shall mean the delivery of one or more Programs, in prerecorded and encrypted or scrambled form, on packaged media, such as DVD discs.

2.42 "Program" shall mean any work of Commercial Audiovisual Content.

2.43 "Protected Free-to-Air System" shall mean the United Kingdom High Definition Digital Terrestrial Transmission service and the Freeview New Zealand service. Licensee is advised that DTLA may from time to time amend the Encoding Rules and these Compliance Rules to add additional services to this definition.

2.44 "Remote Access" shall mean the Remote Access function as set out in the Specification that permits the use of DTCP to protect transmissions of DT Data to a DTCP Sink Function located outside the physical home network.

2.45 "Retention State Field" shall mean the field or bits, as described in the Specification, used to specify the retention period that is associated with a Program received by a Sink Function.

2.46 "SD Interlace Modes" shall mean composite video, s-video, 480i component video and 576i video.

2.47 "Subscription-on-Demand" shall mean the delivery of a single Program or a specified group of Programs for which (i) a subscriber is able, at his or her discretion, to select the time for commencement of exhibition thereof; (ii) where each such single Program is generally uninterrupted by Commercial Advertising Messages; and (iii) for which Program or specified group of Programs subscribing viewers are charged a periodic subscription fee for the reception of programming delivered by such service during the specified viewing period covered by the fee. In the event a given delivery of a Program qualifies both as a Pay Television Transmission and Subscription-on-Demand, then for purposes of this Agreement, such delivery shall be deemed Subscription-on-Demand rather than a Pay Television Transmission.

2.48 "Transfer" shall mean (a) where used as a noun, the transmission of CC Content from a Source Device to one or more Sink Devices that make or enable the making of a persistent copy thereof pursuant to and in accordance with Section 2.8 of Part 1 and Section 4.1 and 4.2 of Part 2 of this Exhibit B, and (b) where used as a verb, the act of making a transmission as described in clause (a).

2.49 "Transitory Image" shall mean data which has been stored temporarily for the sole purpose of enabling the immediate display of content but which (a) does not persist materially after the content has been displayed and (b) is not stored in a way which permits copying or storing of such data for other purposes.

2.50 "Video-on-Demand" shall mean a delivery of a single Program or a specified group of Programs for which (i) each such individual Program is generally uninterrupted by Commercial Advertising Messages; (ii) recipients are charged a separate fee for each such single Program or specified group of Programs; and (iii) a recipient is able, at his or her discretion, to select the time for commencement of exhibition of such individual Program or specified group of Programs. In the event a delivery qualifies as both Video-on-Demand and a Pay Television Transmission, then for purposes of this Agreement, such delivery shall be deemed Video-on-Demand.

EXHIBIT B AUDIOVISUAL, PART 1: COMPLIANCE RULES FOR SINK FUNCTIONS

1. INTRODUCTION

1.1 **Applicability.** This Part 1 of this Exhibit B is applicable to Licensed Products that have a Sink Function.

2. SINK FUNCTION OBLIGATIONS REGARDING PERSISTENT STORAGE OF CONTENT

2.1 **Copy Never.** Licensed Products shall be constructed such that Copy Never DT Data received via their Sink Functions may not, once decrypted, be stored except as a Transitory Image or as otherwise permitted in Section 2.1.1:

2.1.1 Copy Never DT Data may be retained (i.e., stored) for such period as is specified by the Retention State Field, solely for purposes of enabling the delayed display of such DT Data. Such retained DT Data shall be stored using a method set forth in Section 2.2. and shall be obliterated or otherwise rendered unusable upon expiration of such period.

2.2 **Permitted Copy One Generation Copies.** Subject to the requirements of Sections 2.5-2.7, a Licensed Product may not make, or cause to be made, a copy of Copy One Generation Decrypted DT Data unless each copy (a) is made as a Transitory Image or (b) is made using a method set out in Section 2.2.1. A Licensed Product may, alternatively, treat such Decrypted DT Data as Copy Never, provided that no retention under Section 2.1.1 of this Part 1 is permitted.

2.2.1 Subject to the requirements of Sections 2.5-2.7, and except as set forth in Sections 2.2.2 and 2.2.3, a Licensed Product may make, or cause to be made, no more than two (2) first-generation copies of Decrypted DT Data, in different formats of storage device or media, by using only the methods described in Section 2.2.1.1 and Section 2.2.1.2:

2.2.1.1 The copy is made using a copy protection technology (such as scrambling or encryption) that is approved by DTLA now or in the future, as specified on the DTLA website or in a notice to Adopter;

2.2.1.2 The copy is stored using an encryption protocol that uniquely associates such copy with a single Licensed Product so that it cannot be played on another device or that no further usable copies may be made thereof (other than copies made from an output permitted by this Agreement or as otherwise permitted under Section 2.3 of this Part 1 or Section 3 or 4 of Part 2); or

2.2.1.3 Copy One Generation Decrypted DT Data that is copied in a personal video recorder or other bound recording medium pursuant to Section 2.2.1.2 may continue to be treated as Copy One Generation for a period of up to ninety (90) minutes from initial reception of each unit of such data (e.g., frame-by-frame, minute-by-minute, megabyte-by-megabyte, etc.), but in no event shall such unit of data exceed one minute of a Program.

2.2.2 In the event that a Licensed Product supports one (1) or more format(s) of storage devices or media in addition to those in which a copy or copies of Decrypted DT Data are

made pursuant to Section 2.2.1, a Licensed Product may make, or cause to be made, one (1) additional first-generation copy of Decrypted DT Data, using any of the methods described in Sections 2.2.1.1 and 2.2.1.2, provided that (a) such DT Data is received by one separate Sink Function having a separate Device Certificate for such additional format of storage device or media and (b) such single copy is made in a format of storage device or media other than a format in which a copy has been made by a recording device supported by another Sink Function in such Licensed Product.

By way of example and not limitation, for purposes of this Section 2.2, the following constitute different formats of storage devices or media: MPEG4 HDD recorder; MPEG2 HDD recorder; DVHS; all DVD-recordable having less than 20GB capacity (for example, DVD-RAM, DVD-RW, DVD+RW or DVD-R); SD Card; Memory Stick; Compact Flash; non-removable RAM; and non-removable flash memory.

2.2.3 Each copy made pursuant to Sections 2.2.1, 2.2.2 or 2.4 may be stored on one or more physical storage devices or media, and may include a back-up copy, so long as all such devices, media and back-up copy constitute only a single usable copy (e.g., a back-up copy may be made on HDD or other media and the copy may be stored on RAID-type devices).

2.3 **No More Copies**. A Licensed Product may not make, or cause to be made, an analog copy of Decrypted DT Data that is encoded as No More Copies. A Licensed Product may not make, or cause to be made, a digital copy of any copy of Decrypted DT Data that is encoded as No More Copies except (a) as a Transitory Image, or (b) if the Licensed Product deletes or otherwise renders unusable the original copy such that, at any point in time, only a single useable copy persists as between such original and copy thereof, or (c) in the event that a Licensed Product that has a Sink Function receives DT Data via its Sink Function that was transmitted by a Licensed Product that has a Source Function pursuant to Section 3.1 (b) or 4.2.2 (b) of Part 2 of this Exhibit B.

2.4 **EPN Encoded Content**. Subject to the requirements of Sections 2.5-2.7, a Licensed Product may not make, or cause to be made, a digital copy of Decrypted DT Data for which the associated EPN Field is asserted except (a) as a Transitory Image or (b) if such copy is made using one or more of the methods set out in Section 2.2.1.1 and Section 2.2.1.2. Consistent with the assertion of EPN and with the preceding sentence, a Licensed Product may, subject to the requirements of Sections 2.5-2.6, make, or cause to be made, additional digital copies of Decrypted DT Data for which the associated EPN field has been asserted, provided that each such copy (a) is a Transitory Image or (b) is made using one or more of the methods set out in Section 2.2.1.1 and Section 2.2.1.2. For clarification, Section 2.2.1.2 shall not be read to limit the number of copies that may be made of EPN encoded content, so long as each copy is made using a method set out in Section 2.2.1.1 and Section 2.2.1.2.

2.5 **Analog Sunset Token Content.** Notwithstanding the terms of Section 2.2-2.4, with respect to Analog Sunset Token Content, the copy protection technologies referenced in Section 2.2.1.1 shall be deemed further restricted to only those copy protection technologies, if any, approved by DTLA for Analog Sunset Token Content, now or in the future, as specified on the DTLA website or in a notice to Adopter.

2.6 **Digital Only Token Content.** Notwithstanding the terms of Section 2.2-2.4, with respect to Digital Only Token Content, the copy protection technologies referenced in Section 2.2.1.1 shall be deemed further restricted to only those copy protection technologies, if any, approved by DTLA for Digital Only Token Content, now or in the future, as specified on the DTLA website or in a notice to Adopter.

2.7 **Remote Access Content.** Notwithstanding the terms of Sections 2.2-2.4, a Licensed Product may not make, or cause to be made, a digital copy of Decrypted DT Data received via Remote Access except (i) as a Transitory Image, or (ii) where a Sink Function receives DT Data that was transmitted by a Licensed Product that has a Source Function pursuant to Section 3.1(b) or 4.2.2(b) of Part 2 of this Exhibit B.

2.8 **Copy Count Content.** Notwithstanding the terms of Sections 2.2-2.4, and except as provided in Section 2.1, a Licensed Product may not make, or cause to be made, a copy of CC Content except in compliance with Section 2.9 using one of the methods set forth in Sections 2.8.1-2.8.3:

2.8.1 via a recording technology approved by DTLA for CC Content, now or in the future, as specified on the DTLA website or in a notice to Adopter, and the Sink Device passes to such technology the Number of Permitted CC Copies to be associated with such content passed to such technology;

2.8.2 if the copy is stored pursuant to Section 2.2.1.2, provided that the Sink Device associates such stored copy with a persistent indicator of the Number of Permitted CC Copies (such copy, a "Bound CC Recording"); or

2.8.3 if the copy is made using a copy protection technology pursuant to 2.2.1.1, provided that (a) the Number of Permitted CC Copies is not passed to the downstream technology and (b) the Number of Permitted CC Copies made by such copy protection technology shall be deemed one.

2.9 **Additional Obligations Regarding Recording and Output of Copy Count Content.** For each CC Content received by the Sink Function, the Sink Function shall keep track of the Number of Permitted CC Copies for all recordings made pursuant to Sections 2.8.1-2.8.3 (collectively, the "Downstream Recording CC Copies") as well as the Number of Permitted CC Copies for all Downstream Output CC Copies (as defined in Section 4.9.1), provided that the total Number of Permitted CC Copies for all such Downstream Recording CC Copies and for all Downstream Output CC Copies shall be no greater than the Number of Permitted CC Copies associated with such CC Content received by the Sink Device having such Sink Function or, where the cop(y)(ies)/output(s) is/are being made from a Bound CC Recording, no greater than the Number of Permitted CC Copies associated with such Bound CC Recording immediately prior to Transfer. Further, if any such output or copy is made from a Bound CC Recording on the Sink Device, the Sink Device shall decrement the Number of Permitted CC Copies associated with such Bound CC Recording by the number of all Downstream Recording CC Copies and all Downstream Output CC Copies, provided that if the decremented count would be zero, such Bound CC Recording shall be deleted or rendered unusable on the Sink Device.

3. SINK FUNCTION OBLIGATIONS REGARDING MOVE

3.1 **Move.** In the event that a Licensed Product that has a Sink Function receives DT Data via its Sink Function that was transmitted by a Licensed Product that has a Source Function pursuant to Section 3 or 4.2 of Part 2 of this Exhibit B, such Sink Function shall ensure that such DT Data is encoded as No More Copies and, for avoidance of doubt, in the event that DT Data was transmitted pursuant to section 3.1 (a) of Part 2 of this Exhibit B, such DT Data received by such Sink Function may not be treated as Copy One Generation pursuant to Section 2.2.1.3. Any Sink Function that receives DT Data pursuant to this Section 3 shall make or enable the making of only a single copy of such DT Data.

4. SINK FUNCTION PERMITTED OUTPUTS.

4.1 **Generally.** As set forth in more detail below, a Licensed Product shall not pass Decrypted DT Data, whether in digital or analog form, to an output except as permitted below.

4.1.1 **Outputs, Video.** A Licensed Product shall not pass any representation or conversion of the video portion of Decrypted DT Data to any output except:

4.1.1.1 Where Decrypted DT Data is output via an approved standard definition analog output in a manner pursuant to Section 4.2 of this Part of this Exhibit B;

4.1.1.2 Where Decrypted DT Data is output in a High Definition Analog Form in a manner pursuant to Section 4.3 of this Part of this Exhibit B;

4.1.1.3 Where Decrypted DT Data is output via a digital output in a manner pursuant to Section 4.4 of this Part of this Exhibit B; or

4.1.1.4 Where the Decrypted DT Data is encoded Copy Freely with the EPN Field unasserted, in which case there are no restrictions on output.

4.2 **Standard Definition Analog Output.** Subject to the requirements of Section 4.7, a Licensed Product shall not pass Decrypted DT Data to an NTSC, YUV, SECAM, PAL, or consumer RGB format analog output (including an S-video output for the listed formats) unless (a) the Decrypted DT Data is other than No More Copies, Copy Never, or Copy One Generation or (b) the Licensed Product is incorporated into a Computer Product and the output is either a VGA output or a similar output that was widely implemented as of May 1, 2001 that carries uncompressed video signals with a resolution less than or equal to a Constrained Image to a computer monitor or (c) the Licensed Product generates copy control signals according to the information provided in either such Decrypted DT Data or PCP-UR and E-EMI in accordance with the Specification. A Licensed Product may, as follows, pass Decrypted DT Data to an output pursuant to clause (c) if it uses the following technologies:

4.2.1 For NTSC analog outputs, however transmitted, the specifications for the Automatic Gain Control and Colorstripe copy control systems (contained in the document entitled "Specification of the Macrovision Copy Protection Process for DVD Products, Revision 7.1.D1, September 30, 1999") and the CGMS-A specifications contained in IEC 61880 (for inclusion on Line 20) or in EIA-608-B (for inclusion on Line 21), provided that, except as otherwise expressly provided in Section 4.2.5, all of such technologies must be utilized in order to meet this requirement.

4.2.2 For PAL, SECAM or YUV outputs, the appropriate specifications (i) for the Automatic Gain Control copy control system (contained in the document entitled

"Specification of the Macrovision Copy Protection Process for DVD Products, Revision 7.1.D1, September 30, 1999") and (ii) for the CGMS-A copy control system (contained in IEC 61880 (for inclusion on Line 20) or in EIA-608-B (for inclusion on Line 21) or in EIA-805 (for inclusion on Line 41) for YUV (525/60 systems) outputs or in ETS 300294 for PAL, SECAM, and YUV (625/50 systems) outputs), provided that, except as otherwise expressly provided in Section 4.2.5, both of these technologies must be utilized in order to meet this requirement. (Note; "YUV as used herein means a component video output comprised of a luminance signal (Y) and two color difference signal (U and V) and specifically includes the following component video signals (Y,Pb,Pr), (Y,Cb,Cr), (Y, Db, Dr), and (Y, B-Y, R-Y).)

4.2.3 For 480p progressive scan outputs, the appropriate specification for (i) the Automatic Gain Control copy control system (contained in the document entitled "Specification of the Macrovision AGC Copy Protection Waveforms for DVD Applications with 525p (480p) Progressive Scan Outputs, Revision 1.03 (December 22, 1999)") and (ii) CGMS-A copy control system (contained in, or adapted without material change from, EIAJCPR1204-1 (defining the signal waveform carrying the CGMS-A) and IEC61880 (defining the bit assignment for CGMS-A)).

4.2.4 For SCART connectors, the Automatic Gain Control specifications for the PAL and SECAM signal carried by that connector, provided that the connector must be configured so that the component signal carried by the connector must always be accompanied by a composite signal and such composite signal must provide the only synchronization reference for the component signal.

4.2.5 A Licensed Product shall not apply Analog Protection System (APS) to Copy One Generation Decrypted DT Data, but it shall pass through, without alteration, the value of any APS trigger bits (as described in the Specification) in accordance with the specifications relating to APS contained in (a) IEC 61880 (for inclusion of such value on Line 20) or EIA-608-B (for inclusion of such value on Line 21) for NTSC outputs or (b) IEC 61880 (for inclusion of such value on Line 20) or EIA-608-B (for inclusion of such value on Line 21) for YUV (525/60 systems) outputs. Notwithstanding the foregoing, the requirements to comply with the CGMS-A specification and to pass any values of APS trigger bits set forth in this Section 4.2 shall not apply to a Licensed Product incorporated into a Computer Product.

4.2.6 DTLA may amend certain obligations set out in this Section 4.2, or specify alternative means to comply, if DTLA finds that the required technologies are not available on fair, reasonable and nondiscriminatory terms.

4.3 **High Definition Analog Output.** Subject to the requirements of Section 4.7, Licensed Products shall not pass Decrypted DT Data to a High Definition Analog Output, except as set forth in this Section 4.3:

4.3.1 Licensed Products may pass Decrypted DT Data to a High Definition Analog Output as a Constrained Image.

4.3.2 Licensed Products that recognize and respond to the Image Constraint Token in accordance with the Specification may pass Decrypted DT Data to an output in High Definition Analog Form when authorized by the setting of the Image Constraint Token.

4.3.3 Licensed Products incorporated into Computer Products may pass Copy One Generation or No More Copies Decrypted DT Data without image constraint to SVGA (1024x768 and greater), XGA (1024x768), SXGA and UXGA or similar computer video

outputs that were widely implemented as of May 1, 2001 (but not to such typical consumer electronics outputs as NTSC, PAL, SECAM, SCART, YUV, S-Video and consumer RGB, whether or not such outputs are found on any Computer Product) in High Definition Analog Form for devices manufactured prior to December 31, 2010, unless otherwise notified by DTLA.

4.3.4 Licensed Products may pass Decrypted DT Data in High Definition Analog Form to a High Definition Analog Output where such Decrypted DT Data is encoded Copy Freely.

4.4 **Digital Outputs.** Subject to the requirements of Section 4.8-4.9, Licensed Products may only pass Decrypted DT Data to a digital output as follows:

4.4.1 To DTCP-protected outputs according to the Specification;

4.4.2 In the case of Licensed Products incorporated into Computer Products, as a Constrained Image to DVI outputs of devices manufactured on or prior to December 31, 2005, unless otherwise notified by the DTLA. Such Licensed Products may pass Decrypted DT Data to outputs other than as a Constrained Image (a) for content encoded other than Copy Never, for devices manufactured on or prior to December 31, 2003, unless otherwise notified by the DTLA or (b) for devices manufactured on or prior to December 31, 2010, when such Licensed Products recognize and respond to the Image Constraint Token in accordance with the Specification and are authorized by the setting of the Image Constraint Token;

4.4.3 To any digital output where the Decrypted DT Data is encoded Copy Freely with the EPN Field unasserted; or

4.4.4 Via other methods that may be approved by DTLA in the future.

4.5 **Audio, Analog.** There are no prohibitions relating to analog audio outputs.

4.6 **Audio, Digital.** Except as otherwise provided in Section 4.4, Licensed Products shall not output the audio portions of Decrypted DT Data in digital form except in compressed audio format (such as AC3) or in Linear PCM format in which the transmitted information is sampled at no more than 48 kHz and no more than 16 bits. Adopter is cautioned and notified that the requirements relating to audio may be revised.

4.7 **Analog Sunsets.** Notwithstanding the provisions of Sections 4.2 and 4.3, analog output of Decrypted DT Data marked with the Analog Sunset Token shall be subject to the following requirements:

4.7.1 **Analog Sunset – 2010.**

4.7.1.1 With the exception of Existing Models and as otherwise provided in Section 4.7.1.2, Licensed Products that are manufactured after December 31, 2010 but before December 31 2013 shall not pass Decrypted DT Data marked with the Analog Sunset Token to any analog video output except in SD Interlace Modes. Existing Models that do not so restrict such analog output of Decrypted DT Data to SD Interlace Modes may be manufactured and sold by Adopter until December 31, 2011. Notwithstanding the foregoing, Adopter may continue to manufacture and sell an Existing Model in which the

implementation of DTCP is a Robust Inactive Product after December 31, 2010 provided that when such Robust Inactive Product is activated through an Update, such Update results in a Licensed Product that, in response to the Analog Sunset Token, limits analog video output of such content to SD Interlace Modes only.

4.7.1.2 Until September 30, 2011, Licensed Products may continue to be manufactured in accordance with the existing Specification in lieu of responding to the Analog Sunset Token as described in Section 4.7.1.1.

4.7.2 **Analog Sunset – 2013.** No Licensed Product manufactured or sold by Adopter after December 31, 2013 may pass Decrypted DT Data marked with the Analog Sunset Token to any analog video output.

4.8 Digital Only Token Content. Notwithstanding the terms of Sections 4.1-4.4 and 4.7, and except as provided in Sections 4.5 and 4.6, a Licensed Product shall not pass Digital Only Token Content to any output except:

4.8.1 To DTCP-protected outputs according to Specification Revision 1.7 or higher, setting DOT field to DOT-asserted; or

4.8.2 Via other methods approved by DTLA for Digital Only Token Content, now or in the future, as specified on the DTLA website or in a notice to Adopter.

4.9 Copy Count Content. Notwithstanding the terms of Sections 4.1-4.4 and 4.7-4.8, and except as provided in Sections 4.5 and 4.6, a Licensed Product shall not pass CC Content to any output except as provided in Sections 4.9.1 or 4.9.2:

4.9.1 A Licensed Product may pass CC Content using a method described in Section 4.9.1.1 or 4.9.1.2:

4.9.1.1 To DTCP-protected outputs according to Specification Volume 1 Revision 1.7 or higher that implement the requirements pertaining to CC Content in Part 2 of this Exhibit; or,

4.9.1.2 Via other methods approved by DTLA for CC Content, now or in the future, as specified on the DTLA website or in a notice to Adopter.

When passing CC Content pursuant to Section 4.9.1.1 or 4.9.1.2, a Sink Function also shall pass the Number of Permitted CC Copies for each output (collectively, the "Downstream Output CC Copies"), and shall comply with the requirements of Section 2.9.

4.9.2 In addition to outputs permitted under Section 4.9.1, in the case that the CC Content being output is made from a Bound CC Recording, a Licensed Product may pass such CC Content to any output permitted under Sections 4.1-4.4 if no copies can be made from such output; the content is treated as No More Copies content; and no Number of Permitted CC Copies is passed to such output.

5. INTERNET RETRANSMISSION.

5.1 **Generally.** The parties acknowledge that Licensed Products shall not permit retransmission of Decrypted DT Data to the Internet except as permitted in Section 4.4.3.

6. CONSENSUS WATERMARK NON-INTERFERENCE.

6.1 **Phase-in Period.** During the period commencing on the Effective Date and ending (i) with respect to the Consensus Watermark, eighteen (18) months after the date DTLA declares the Consensus Watermark, and (ii) with respect to all other Presently Known Watermark Technologies, on the date DTLA declares the Consensus Watermark, Adopter shall not knowingly design or knowingly develop a Licensed Product or a component thereof for the primary purpose of stripping, interfering with or obscuring such Consensus Watermark or other Presently Known Watermark Technologies in DT Data received by such Licensed Product's Sink Function or knowingly promote or knowingly advertise or knowingly cooperate in the promotion or advertising of Licensed Products or components thereof for the purpose of stripping, interfering or obscuring such watermarks in such DT Data. For purposes of this Section 6.1, a "Presently Known Watermark Technology" shall mean each of the technologies submitted by the Galaxy group of companies and by the Millennium Group to the DVD Copy Control Association, Inc. in August 1999, and the technology defined as "ARIS/SOLANA-4C," as required by the SDMI Portable Device Specification, Part 1, Version 1.0 (July 8, 1999).

6.2 **Protection of the Watermark**. Without limiting the terms of Section 6.1,

6.2.1 Commencing on the date that DTLA declares the Consensus Watermark, Adopter:

6.2.1.1 Shall, when selecting among technological implementations for product features of Licensed Products designed after such date, take commercially reasonable care (taking into consideration the reasonableness of the costs of implementation, as well as the comparability of their technical characteristics, of applicable commercial terms and conditions, and of their impact on Decrypted DT Data and on the effectiveness and visibility of the Consensus Watermark) that Licensed Products and components thereof do not strip, interfere with or obscure the Consensus Watermark in DT Data received by their Sink Functions;

6.2.1.2 Shall not design new Licensed Products or components thereof for which the primary purpose is to strip, interfere with or obscure the Consensus Watermark in DT Data received by their Sink Functions; and

6.2.1.3 Shall not knowingly promote or knowingly advertise or knowingly cooperate in the promotion or advertising of Licensed Products or components thereof for the purpose of stripping, interfering with or obscuring the Consensus Watermark in DT Data received by their Sink Functions.

6.2.2 Commencing eighteen (18) months after DTLA declares the Consensus Watermark, Adopter:

6.2.2.1 Shall not produce Licensed Products or components thereof for which the primary purpose is to strip, interfere with or obscure the Consensus Watermark in DT Data received by their Sink Functions; and

6.2.2.2 Shall not knowingly distribute or knowingly cooperate in distribution of Licensed Products or components thereof for the purpose of stripping, interfering with or obscuring the Consensus Watermark in DT Data received by their Sink Functions.

6.3 **Product Features.** This Section 6 shall not prohibit a Licensed Product or Licensed Component from incorporating legitimate features (i.e., zooming, scaling, cropping, picture-in-picture, compression, recompression, image overlays, overlap of windows in a graphical user interface, audio mixing and equalization, video mixing and keying, downsampling, upsampling, and line doubling, or conversion between widely-used formats for the transport, processing and display of audiovisual signals or data, such as between analog and digital formats and between PAL and NTSC or RGB and YUV formats, as well as other features as may be added to the foregoing list from time to time by DTLA by amendment to these Compliance Rules Audiovisual) that are not prohibited by law, and such features shall not be deemed to strip, interfere with or obscure the Consensus Watermark in DT Data, provided that (a) Adopter shall, at all times after DTLA declares the Consensus Watermark, take commercially reasonable care, in accordance with Section 6.2.1, that such features in a Licensed Product do not strip, obscure, or interfere with the Consensus Watermark in DT Data received by such Licensed Product's Sink Function, and (b) Adopter shall not knowingly market or knowingly distribute, or knowingly cooperate in marketing or distributing, such Licensed Products or Licensed Components for the purpose of stripping, obscuring or interfering with the Consensus Watermark in DT Data.

6.4 Adopter is alerted that the requirements of this Section 6, and the declaration of the Consensus Watermark, may be rescinded by DTLA if, during the two (2)-year period immediately preceding the fourth anniversary of such declaration, the Consensus Watermark has not been implemented by major Content Participants in more than thirty-three percent (33%) of DVD discs of new theatrical motion pictures produced for DVD release by such Content Participants in the United States of America and Canada during such period.

7. REQUIREMENTS WITH CERTAIN OPERATING SYSTEMS.

7.1 **TTL Exception**. The requirement in section 10.2 of Specification Volume 1 Supplement E that "receiving devices shall discard such received IP datagrams which have a TTL value greater than 3" shall not apply where it is not technically feasible and commercially reasonable for a Licensed Product to determine from its operating system the TTL value of a received IP datagram.

7.2 **Wireless LAN Security Exception**. The first sentence of section 10.3 of Specification Volume 1 Supplement E shall not apply where it is not technically feasible and commercially reasonable for a Licensed Product to determine from its operating system whether Wireless LAN security is engaged.

7.3 Eighteen (18) months after it becomes technically feasible and commercially reasonable for a Licensed Product to conform to 10.2 and/or 10.3 of Specification Volume 1 Supplement E, the exceptions 7.1 and/or 7.2 respectively will cease to apply to such device.

EXHIBIT B AUDIOVISUAL, PART 2: COMPLIANCE RULES FOR SOURCE FUNCTIONS

1. SOURCE FUNCTION OBLIGATIONS

1.1 **Applicability.** This Part 2 of this Exhibit B is applicable to Licensed Products that have a Source Function.

2. VIDEO CONTENT

2.1 **Encoding Rules.** Adopter acknowledges that Content Participants may only encode Commercial Audiovisual Content using DTCP to prevent or limit copying as set out Sections 2.1.1 and 2.1.2.

2.1.1 **Copy Never.** Commercial Audiovisual Content delivered as follows may be encoded and transmitted as Copy Never Content:

2.1.1.1 Prerecorded Media,

2.1.1.2 Pay-Per-View,

2.1.1.3 Subscription-On-Demand,

2.1.1.4 Video-on-Demand,

2.1.1.5 New business models that are comparable to 2.1.1.1 - 2.1.1.4.

For the avoidance of doubt, content delivered over a Protected Free-to-Air System may not be encoded and transmitted as Copy Never.

2.1.2 **Copy One Generation.**

2.1.2.1 Commercial Audiovisual Content delivered as follows may be encoded and transmitted on such system as Copy One Generation Content:

2.1.2.1.1 Prerecorded Media,

2.1.2.1.2 Pay-Per-View,

2.1.2.1.3 Subscription-On-Demand,

2.1.2.1.4 Video-on-Demand,

2.1.2.1.5 Pay Television Transmission,

2.1.2.1.6 Non-Premium Subscription Television,

2.1.2.1.7 Free Conditional Access Delivery,

2.1.2.1.8 New business models that are comparable to 2.1.2.1.1.1 – 2.1.2.1.7.

2.1.2.2 Content delivered over a Protected Free-to-Air System may be encoded and transmitted as Copy One Generation Content as follows:

a. content that previously has been available only in theatrical release and/or on Prerecorded Media in any country of the world, and has not previously been licensed for television broadcast in any country of the world; or,

b. content that --

i. was transmitted in North America, Japan, any Western European country, Australia, or in any country constituting a major market for such audiovisual programming (each a "Major Market"), by or under license from a person or entity authorized to license such transmission, and each such

transmission has been made over Video on Demand, Pay-Per-View, Subscription-on-Demand, or Undefined Business Models that are comparable to the foregoing, or Pay Television Transmissions, and

ii. either—

A. has not been lawfully transmitted in any Major Market in greater than Standard Definition format without using one or more digital copy protection methods (*i.e.*, methods that impose numerical copy restrictions), including by way of example DTCP encoding and display-only methods, or,

B. is a version created specifically for the market covered by a Protected Free-to-Air System, other than by minor editing processes typically performed for English-speaking foreign-produced programs re-broadcast in such market, of a program that was broadcast or is scheduled to be broadcast in another country; or,

c. content that is co-produced by Content Participant and one or more other entities and is scheduled to be transmitted in a Major Market by or under license from one or more of the other co-production partners using a method of delivery set out in b(i) above and satisfies the condition set out in b(ii)(A), or,

d. content that was permitted to be transmitted, and was transmitted, using DTCP Copy One Generation encoding in accordance with this Section 2.1.2.2.

2.1.3 **No More Copies.** Licensed Products shall only encode as "No More Copies" content received as Copy One Generation and stored via a method set out in, or approved pursuant to, Exhibit B, Part 1, Section 2.2.

2.1.4 **Encryption Plus Non-assertion Encoding.** Content that is broadcast over the Protected Free-to-Air System may be encoded and transmitted as EPN, except that EPN encoding may not be applied to content that is broadcast (a) over another service, in the same market as the Protected Free-to-Air System, in High Definition, (b) at or about the same date as the broadcast over the Protected Free-to-Air System, (c) without using one or more digital protection methods (*i.e.*, methods that impose numerical copy restrictions, restrictions upon retransmission, or both), including by way of example DTCP EPN encoding. Adopter acknowledges that EPN Encoding may not be asserted by Content Participants with respect to Other EPN Eligible Broadcast Television, except by such eligible Content Participants that are identified by DTLA. "EPN Encoding" means such encoding used by or at the direction of a Content Participant so as to cause a service or Program to be encrypted with DTCP but not to be subject to copy control restrictions.

2.1.5 **DOT and AST.** Adopter acknowledges that Content Participant may not encode, or direct to be encoded, using the Digital Only Token or the Analog Sunset Token, Commercial Audiovisual Content except--

(a) in the case of Video-on-Demand in a particular country, any Program until the earlier of (x) 120 days from the first application of DOT by any Video-on-Demand service for such Program or (y) the retail release in such country of such Program in any pre-recorded format except if such pre-recorded format both (i) is designed to prevent all products from outputting such Program in analog format (whether output from a product then- manufactured or distributed or from any legacy product) and (ii) includes an indicator requiring the Source

Device to set the DOT to asserted for such Program, if such Program can be output via DTCP,

(b) to the same extent in any country of the world as is allowed in the United States by the FCC Waiver Order, or,

(c) any Program on Prerecorded Media, or delivered via an Undefined Business Model that is Comparable to Prerecorded Media unless such model is also a Defined Business Model other than Prerecorded Media or an Undefined Business Model that is Comparable thereto.

2.2 **Image Constraint.** Adopter acknowledges that Content Participants are not permitted to encode, or direct to be encoded, Commercial Audiovisual Content so as to require Decrypted DT Data to be output as a Constrained Image except with respect to Prerecorded Media, Pay Television Transmission, Video-on-Demand, Subscription-on-Demand, Pay-Per-View, a new business model comparable to any of the foregoing or any other Conditional Access Delivery of a Program that (i) had a theatrical release or was released direct-to-video and (ii) is transmitted or delivered uninterrupted by Commercial Advertising Messages. Licensed Products that have a Source Function (a "Source Device") shall set, in accordance with the Specification, the Image Constraint Token associated with a Program so as to permit any Licensed Product with a Sink Function to output such Program in High Definition Analog Form if such Source Device outputs such Program in unprotected High Definition Analog Form other than as permitted in Section 4.3.3 of Part 1 of Exhibit B. In addition, a Source Device shall set, in accordance with the Specification, the Image Constraint Token associated with a Program so as to permit any Licensed Product with a Sink Function to output such Program in High Definition Analog Form if such Program was not specifically encoded to output such Program as a Constrained Image when received by the Source Device.

2.3 **Retention of Copy Never Content**. Except for Prerecorded Media, a Source Device shall set, in accordance with the Specification, the Retention State Field associated with any Commercial Audiovisual Content that is encoded as Copy Never for a period equal to the greatest of (a) ninety (90) minutes from initial receipt of each unit of such data (e.g., frame-by-frame, minute-by-minute, megabyte-by-megabyte, etc.); (b) such other period of time specified in the Specification as a content owner may affirmatively permit; or (c) if the amount of time that such content may be retained in such Source Device is determined pursuant to rules, standards or obligations that were developed under an open-standards process, such period of time specified in the Specification that is closest to, but not exceeding, the period of time that such Source Device is permitted to retain such content. In the case of Prerecorded Media, or if the Commercial Audiovisual Content has previously been retained, the Source Device shall encode the Commercial Audiovisual Content such that no further retention shall be permitted.

2.4. **Analog Sunset.**

2.4.1 With the exception of Existing Models, a Source Device manufactured after December 31, 2010, up until September 30, 2011, shall either:

2..4.1.1 set, in accordance with the Specification, the Analog Sunset Token for Analog Sunset Content; or,

2.4.1.2 set the Image Constraint Token, in accordance with the Specification, for pre-recorded Decrypted AACS Content so as to cause any Licensed Product responding to such Image Constraint Token to output such content as a Constrained Image.

For the avoidance of doubt, Source Devices manufactured on or prior to December 31, 2010, are not prohibited hereunder from (x) setting the Analog Sunset Token in accordance with the Specification for any Decrypted AACS Content, or (y) setting the Image Constraint Token in accordance with the Specification, on pre-recorded Decrypted AACS Content, so as to cause any Licensed Product responding to such Image Constraint Token to output such content as a Constrained Image.

2.4.2 Beginning after September 30, 2011, with the exception of Existing Models, a Source Device shall set, in accordance with the Specification, the Analog Sunset Token on Analog Sunset Content. A Source Device may not set the Analog Sunset Token on any content other than Analog Sunset Content.

2.4.3 Existing Model Source Devices may be manufactured and sold up until December 31, 2011; thereafter they may continue to be sold only if they comply with the Compliance Rules (and other terms of the Agreement) applicable to Licensed Products that are not Existing Models.

2.5. **Digital Only Token.** A Source Device shall not set the Digital Only Token to DOT asserted except where the encoding upstream from the Source Device directs the Source Device to assert the Digital Only Token in the Source Device. For the avoidance of doubt, the Source Device need not set such token to asserted where such DT Data has not been encoded in accordance with the requirements of the Encoding Rules.

2.6 **Remote Access.** A Licensed Product having a Source Function shall not permit the transmission of DT Data to another Licensed Product using Remote Access except as follows:

2.6.1 A Source Function may concurrently transmit DT Data via Remote Access to no more than one (1) Sink Function. Notwithstanding the foregoing, if the Source Function is provided with an affirmative indication (e.g. such as in a flag or descriptor associated with such DT Data) that Remote Access is permitted to more multiple Sink Functions, it shall be allowed according to such indication.

2.6.2 A Source Function may not permit the transmission via Remote Access of DT Data simultaneous with its reception from a DTCP Sink Function.

2.6.3 A Source Function may permit via Remote Access the transmission of stored content to a Sink Function where such content has been encoded as EPN or No More Copies; provided that the recording of such stored content shall have been completed prior to such transmission, except for any DTCP Source Devices made pursuant to government or quasi-government regulation in effect on April 1, 2011 where such regulation does not permit Remote Access for DTCP; or,

2.6.4 A Source Function otherwise may permit via Remote Access the transmission of content it has not stored (except as a Transitory Image) to a Sink Function only where such Source Function is provided with an affirmative indication (e.g., such as in a flag or descriptor associated with such DT Data) that Remote Access transmission is permitted, and in such case the Source Function shall transmit such content encoded as No More Copies.

2.7. **Requirements with Certain Operating Systems.**

2.7.1 **TTL Exception**. The requirement in section 10.2 of Specification Volume 1 Supplement E that "receiving devices shall discard such received IP datagrams which have a TTL value greater than 3" shall not apply where it is not technically feasible and commercially reasonable for a Licensed Product to determine from its operating system the TTL value of a received IP datagram.

2.7.2 **Wireless LAN Security Exception**. The first sentence of section 10.3 of Specification Volume 1 Supplement E shall not apply where it is not technically feasible and commercially reasonable for a Licensed Product to determine from its operating system whether Wireless LAN security is engaged.

2.7.3 Eighteen (18) months after it becomes technically feasible and commercially reasonable for a Licensed Product to conform to 10.2 and/or 10.3 of Specification Volume 1 Supplement E, the exceptions 2.7.1 and/or 2.7.2 respectively will cease to apply to such device.

3. SOURCE FUNCTION OBLIGATIONS REGARDING MOVE.

3.1 If Copy One Generation content recorded on a personal video recorder or other bound recording medium ("PVR") has been encoded as No More Copies, such content may either (a) be encoded as Copy One Generation; or (b) if E-EMI that indicates Move is used in accordance with the Specification, remain encoded as No More Copies; and transmitted to a single Sink Function in a single Licensed Product (regardless of whether such Licensed Product has multiple Sink Functions), provided that such content on the originating PVR is deleted or otherwise rendered unusable.

3.2 Multiple sequential Moves from a Licensed Product having a Source Function to a Licensed Product having a Sink Function, consistent with the requirements set forth in this Section 3 and Section 3 of Part 1, are permitted.

3.3 A Source Function may permit a Move via Remote Access in accordance with the requirements set forth in Section 3 of Part 1 of Exhibit B and this Section 3 of Part 2 of Exhibit B.

3.4 When the Source Function receives Digital Only Token Content and Moves it in accordance with Section 3.1 above, it shall set the Digital Only Token to DOT asserted.

3.5 When the Source Function receives Analog Sunset Token Content and Moves it in accordance with Section 3.1 above, it shall set the Analog Sunset Token to AST asserted.

4. SOURCE FUNCTION OBLIGATIONS REGARDING COPY COUNT. When a Source Function receives CC Content, it may not transmit or Transfer such CC Content except by using one or more of the methods set forth in this Section 4:

4.1 **Transfer with a valid CC Field**. A Source Function may Transfer CC Content with a valid CC Field to a Sink Function as follows:

4.1.1 The Transfer may occur only over a unique connection between that Source Function and a specific Sink Function established using a method set forth in the Specification, provided that:

4.1.1.1 The Source Function may establish a series of such unique connections with multiple individual specific Sink Functions in order to Transfer copies of such CC Content to each such Sink Function.

4.1.1.2 In any Transfer of CC Content (x) where the Transfer is to a single Sink Function, the Source Function shall set the CC Field to a number that is no greater than the Number of Permitted CC Copies associated with the CC Content as received by the Source Function, or (y) where a series of unique connections are established to multiple Sink Functions for Transfer of such CC Content to each such Sink Function, the Source Function shall set the CC Fields for such Transfers so that the sum of all of the CC Fields is a number no greater than the Number of Permitted CC Copies associated with the CC Content as received by the Source Function.

4.1.1.3 If the Transfer is being made from a Bound CC Recording, when the Source Function confirms that the transmission is complete, the Source Function shall ensure that the Licensed Product decrements the Number of Permitted CC Copies associated with the Bound CC Recording by the number of CC Copies that have been Transferred and shall otherwise comply with the requirements of Section 2.9 of Part 1 of this Exhibit B.

4.2 **Transfer without valid CC Field (i.e. CC Field is 0000, or CC Field is not present).** A Source Function may Transfer a single copy of CC Content to a single Sink Function (regardless of whether such Licensed Product has multiple Sink Functions), either without a CC Field or with a CC Field set to invalid as follows:

4.2.1: where the copy is made from a Bound CC Recording, by following the requirements of Section 3.1 (Move), except that the requirement in Section 3.1 to delete or render unusable the bound recording shall not apply and instead (a) the terms of Section 2.9 of Part 1 of this Exhibit B shall apply and (b) for purposes of such Section 2.9, the Number of Permitted CC Copies for CC Content Transferred pursuant to this Section 4.2 shall be deemed one;

4.2.2 where the copy is not made from a Bound CC Recording, by transmitting the content using the Move protocols in the Specification and either (a) encoding the content as Copy One Generation or (b) if E-EMI indicates Move is used in accordance with the Specification, encode the content as No More Copies.

4.3 **Transmit without CC Field.** Notwithstanding Sections 4.1-4.2, above, a Source Function may transmit CC Content other than by Move or Transfer, to one or more Sink Functions, provided that if the transmission is of Bound CC Recording content, it shall be treated by the Source Function as No More Copies.

4.4 **Proper Encoding**. Where CC Content is encoded, or should be encoded pursuant to the Encoding Rules, as EPN, the Source Function may transmit such content via DTCP without regard to the associated Number of Permitted CC Copies (i.e., it may treat such content as if it were not CC Content). Where the Source Function transmits such content using a DTCP output that includes a CC Field, the CC Field shall be set as invalid (i.e., setting the CC Field bits to 0000).

5. AUDIO, SUBSCRIPTION AND ON-DEMAND SERVICES.

5.1 A Licensed Product may send Commercial Entertainment Content comprising “on-demand” or “pay-per-listen” or subscription audio content that is not part of an audio-visual work to a DTCP

input using Full Authentication with Copy Never encoding or with Restricted Authentication. Adopter is advised to consult with the providers of such audio services to determine their requirements for such activities.

EXHIBIT B AUDIO: COMPLIANCE RULES FOR LICENSED PRODUCTS THAT RECEIVE OR TRANSMIT COMMERCIAL AUDIO WORKS

[For Products that receive or transmit Commercial Audiovisual Content, see Exhibit B Audiovisual, Parts 1- 2, which Parts are applicable to Licensed Products that are capable of decrypted or transmitting, using DTCP, Commercial Audiovisual Works.]

INTRODUCTION

1. GENERALLY.

1.1 This Exhibit B Audio ("Compliance Rules Audio") is applicable to Licensed Products that are capable of decrypting or transmitting, using DTCP, Commercial Audio Works and is divided into separate Parts for different audio formats. Sections 2 and 3 of this Introduction to Exhibit B Audio apply to each Part of Exhibit B Audio. Unless otherwise expressly provided, for purposes of this Exhibit B Audio , all section references in any Part of this Exhibit B Audio shall be deemed references to sections in such Part. [Note: DTLA expects to amend these Compliance Rules Audio in the future to include additional rule sets not set forth in this version of Exhibit B Audio.] For purposes of this Exhibit B Audio, all references below to "Exhibit B" shall be deemed references to this Exhibit B Audio.

1.2 Notwithstanding anything to the contrary in the Specifications, Adopter is not required to implement Localization for the transmission of Commercial Audio Works via DTCP in the following cases:

a. for any DTCP Source Devices made in accordance with a license for a content protection technology where such license allowed DTCP outputs for Commercial Audio Works without Localization as of December 31, 2006; or

b. with respect to the transmission of Commercial Audio Works over DTCP for IEEE1394, (a) in any Licensed Product manufactured prior to June 30, 2010, or (b) for any DTCP Source Devices made pursuant to government or quasi-government regulation in effect on October 1, 2005 where such regulation does not require implementation of Localization for Commercial Audio Works for DTCP for IEEE1394.

2. DEFINITIONS. The following terms shall have the meaning ascribed thereto in the Introduction to Exhibit B: Commercial Audiovisual Works, Commercial Entertainment Content, DT Data, Localization, Sink Function and Source Function. Where another capitalized term is used in this Exhibit B but not otherwise defined in this Exhibit B, the meaning ascribed thereto elsewhere in this Agreement shall apply.

2.1 "Audio DT Data" shall mean DT Data comprising Commercial Audio Works.

2.2 "Commercial Audio Works" shall mean Commercial Entertainment Content in the form of audio content, including but not limited to sound recordings, as defined in 17 U.S.C. § 101. For avoidance of doubt, (a) audio content received by a Commercially-Adopted Audio Access Control Method shall necessarily be considered to be "Commercial Audio Works" and (b) "Commercial Audio Works" do not include audio portions of Commercial Audiovisual Content.

2.3 "Commercially-Adopted Audio Access Control Method" shall mean any commercially-adopted access control method for Commercial Audio Works, such as CPPM, CPRM, Super Audio CD Copy Protection Technology and other commercially-adopted access control technologies whether now or hereafter in commercial use.

2.4 "Consensus Audio Watermark" shall mean the watermark technology designated as the "Consensus Audio Watermark" by DTLA.

2.5 "Transitory Audio Data" shall mean data which has been stored temporarily for the sole purpose of enabling the transmission, reception, or immediate rendering of Commercial Audio Content but which (a) does not persist materially after such content has been rendered and (b) is not stored in a way which permits copying or storing of such data for other purposes.

2.6 "Presently Known Audio Watermark Technology" shall mean the Verance Audio Watermark as defined in the specification "4C 12 Bit Watermark Specification" published by 4C Entity, LLC (October 29, 1999).

3. CONSENSUS AUDIO WATERMARK NON-INTERFERENCE.

3.1 **Phase-in Period.** During the period commencing on the later of (a) the Effective Date and (b) the effective date of this Exhibit B, and ending (i) with respect to the Consensus Audio Watermark, eighteen (18) months after the date DTLA declares the Consensus Audio Watermark, and (ii) with respect to the Presently Known Audio Watermark Technology, on the date DTLA declares the Consensus Audio Watermark, Adopter shall not knowingly design or knowingly develop a Licensed Product or a component thereof for the primary purpose of stripping, interfering with or obscuring such Consensus Audio Watermark or Presently Known Audio Watermark Technology in Audio DT Data received by such Licensed Product's Sink Function or knowingly promote or knowingly advertise or knowingly cooperate in the promotion or advertising of Licensed Products or components thereof for the purpose of stripping, interfering or obscuring such watermarks in such Audio DT Data.

3.2 **Protection of the Consensus Audio Watermark**. Without limiting the terms of Section 3.1,

3.2.1 Commencing on the date that DTLA declares the Consensus Audio Watermark, Adopter:

3.2.1.1 Shall not design new Licensed Products or components thereof for which the primary purpose is to strip, interfere with or obscure the Consensus Audio Watermark in Audio DT Data received by their Sink Functions; and

3.2.1.2 Shall not knowingly promote or knowingly advertise or knowingly cooperate in the promotion or advertising of Licensed Products or components thereof for the purpose of stripping, interfering with or obscuring the Consensus Audio Watermark in Audio DT Data received by their Sink Functions.

3.2.2 Commencing eighteen (18) months after DTLA declares the Consensus Audio Watermark, Adopter:

3.2.2.1 Shall not produce Licensed Products or components thereof for which the primary purpose is to strip, interfere with or obscure the Consensus Audio Watermark in Audio DT Data received by their Sink Functions; and

3.2.2.2 Shall not knowingly distribute or knowingly cooperate in distribution of Licensed Products or components thereof for the purpose of stripping, interfering with or obscuring the Consensus Audio Watermark in Audio DT Data received by their Sink Functions.

3.3 **Product Features.** This Section 3 shall not prohibit a Licensed Product or Licensed Component from incorporating legitimate features (including but not limited to fade-in, fade-out, level control, dynamic range compression, pitch control, digital crossover, noise reduction for the purpose of removing hiss or other artifacts, noise shaping, fast-forward, fast-reverse, slow-forward, slow-reverse, reverse-playback, compression, decompression, channel mixing, equalization, and down sampling) that are not prohibited by law, and such features shall not be deemed to strip, interfere with or obscure the Consensus Audio Watermark in Audio DT Data.

3.4 Adopter is alerted that the requirements of this Section 3, and the declaration of the Consensus Audio Watermark, may be rescinded by DTLA if, during the two (2)-year period immediately preceding the fourth anniversary of such declaration, the Consensus Audio Watermark has not been implemented according to criteria to be established by DTLA.

EXHIBIT B AUDIO, PART 1: COMPLIANCE RULES FOR TYPE 1 AUDIO CONTENT

1. APPLICABILITY. This Part 1 of this Exhibit B is applicable to Licensed Products that handle Type 1 Audio DT Data.

2. DEFINITIONS. For purposes of this Part 1 of this Exhibit B, the following terms shall have the meanings set forth below.

2.1 "Decrypted Type 1 Audio DT Data" shall mean, with respect to any Licensed Product, Type 1 Audio DT Data that has been received by such Licensed Product's Sink Function and decrypted by such Licensed Product according to DTCP but has not been (a) protected by a one-generation copy protection technology identified or approved by DTLA pursuant to Sections 3.1.1.1 or 3.1.1.3 or (b) passed to an output permitted by this Part 1 of this Exhibit B.

2.2 "Type 1 Audio DT Data" shall mean Audio DT Data comprising "Type 1: IEC 60958 Conformant Audio" content as described in the Specification.

3. SINK FUNCTIONS

3.1 Permitted Copies. A Licensed Product may not make, or cause to be made, a copy of Decrypted Type 1 Audio DT Data encoded as Copy One Generation ("copy-permitted-per-type" as set out in the Specification) unless each copy (a) is made as Transitory Audio Data or (b) is made using a method set out in Section 3.1.1.

3.1.1 A Licensed Product may make, or cause to be made, first-generation copies of Decrypted Type 1 Audio DT Data by using the methods described in Sections 3.1.1.1 through 3.1.1.3.

3.1.1.1 The copy is scrambled or encrypted using a copy protection technology that is identified by DTLA for use with Type 1 Audio DT Data;

3.1.1.2 The copy is stored using an encryption protocol that uniquely associates such copy with a single Licensed Product so that it cannot be played on another device or that no further usable copies may be made thereof (other than copies made from an output permitted by this Part 1); or

3.1.1.3 Methods which may be approved by DTLA in the future for Type 1 Audio DT Data.

3.2 No More Copies. A Licensed Product may not make, or cause to be made, a copy of Type 1 Audio DT Data that is encoded as No More Copies except as Transitory Audio Data.

3.3 Permitted Outputs.

3.3.1 Digital Outputs. Licensed Products may only pass Decrypted Type 1 Audio DT Data to a digital output as follows:

3.3.1.1 To DTCP-protected outputs as Type 1 Audio DT Data according to the Specification.

3.3.1.2 To IEC60958 or IEC 61937 if Serial Copy Management System information specified in Decrypted Type 1 Audio DT Data is properly transmitted.

3.3.1.3 To outputs protected by other methods, if any, that may be approved by DTLA in the future for Commercial Audio Works.

3.3.2 Analog Outputs. There are no prohibitions relating to analog audio outputs of Decrypted Type 1 Audio DT Data.

3.4 Internet Retransmission. The parties acknowledge that Licensed Products shall not permit retransmission of Decrypted Type 1 Audio DT Data to the Internet.

EXHIBIT B AUDIO, PART 2: COMPLIANCE RULES FOR TYPE 2 AUDIO CONTENT

1. APPLICABILITY. This Part 2 of this Exhibit B is applicable to Licensed Products that handle Type 2 Audio DT Data.

2. DEFINITIONS.

2.1 "CD-Audio Quality or less" shall mean a sound quality of 2-channels or less, no greater than 48KHz sample frequency, and no more than 16 bits per sample.

2.2 "Decrypted Type 2 Audio DT Data" shall mean, with respect to any Licensed Product, Type 2 Audio DT Data that has been received by such Licensed Product's Sink Function and decrypted by such Licensed Product according to DTCP but has not been passed (a) to a recording technology permitted under Section 3.3or (b) to an output permitted by this Part 2 of this Exhibit B.

2.3 "DVD Audio Specifications" shall mean the current version of the document entitled "DVD Specifications for Read-Only Disc Part 4 AUDIO SPECIFICATIONS" published by DVD Forum, as may be amended from time to time by the DVD Forum.

2.4 "ISRC Information" shall mean International Standard Recording Code Information". ISRC Information" is the collective name of "ISRC data" and "ISRC status". "ISRC data" is the ISRC portion out of "UPC EAN ISRC data". Both "UPC EAN ISRC data" and "ISRC status" are defined in Table 7.2.3.1.1-2 RBP 1 and Table 7.2.3.1.2-2 RBP 1 of the DVD Audio Specifications.

2.5 "Legacy Digital Audio Output" shall mean IEC-958, IEC-60958, IEC-61937 or USB Audio Device Class output. [Note that USB Audio Device Class output is defined by those USB specifications necessary for the output of audio to USB speakers, and that all other USB Device Class outputs (e.g. Communication Device Class, Mass Storage Class, etc.) are not included in this definition.]

2.6 "Linear PCM" shall mean audio encoding using Linear Pulse Code Modulation as specified in the DVD Audio Specifications.

2.7 "Packed PCM" shall mean the lossless compression coding system for Linear PCM as specified in the DVD Audio Specifications.

2.8 "Type 2 Audio DT Data" shall mean Audio DT Data that is "Type 2: DVD Audio" content as described in the Specification

3. SINK FUNCTIONS.

3.1 **Copying.** Except for the passing of Type 2 Audio DT Data to permitted recording technologies of Section 3.3, Licensed Products shall be constructed such that Type 2 Audio DT Data received via their Sink Functions may not, once decrypted, be stored except as Transitory Audio Data.

3.2 **Permitted Outputs**. Licensed Products shall not pass Decrypted Type 2 Audio DT Data, whether in digital or analog form, to an output except as permitted in subsections of this section 3.2.

3.2.1 **Digital Outputs.** Licensed Products shall pass Decrypted Type 2 Audio DT Data to digital outputs and accurately transmit Digital CCI and ISRC Information as follows:

3.2.1.1 To DTCP-protected outputs as Type 2 Audio DT Data according to the Specification.

3.2.1.2 **Legacy Digital Audio Outputs.** Legacy Digital Audio Outputs from Licensed Products shall be limited to 1.5 times normal speed, unless the pitch is corrected to the pitch at normal speed. In addition, such outputs shall comply with the following requirements:

3.2.1.2.1 **Limitation on Sound Quality.** Sound quality of Legacy Digital Audio Outputs when playing Linear PCM and Packed PCM streams shall be equivalent to CD-Audio Quality or less.

3.2.1.2.2 **SCMS Status Setting.** Licensed Products that are not operating as an internal, peripheral, or software component of a Computer Product shall ensure that Legacy Digital Audio Outputs IEC-958, IEC-60958, and IEC-61937 shall include SCMS information corresponding to embedded CCI. Licensed Products shall not actively strip out or actively alter any SCMS information contained in the Digital Audio Content.

3.2.1.3 To outputs protected by other methods, if any, that may be approved by DTLA in the future for Commercial Audio Works.

3.2.2 **Analog Outputs.** Decrypted Type 2 Audio DT Data passed to analog outputs from Licensed Products shall be limited to 1.5 times normal speed, unless the pitch is corrected to the pitch at normal speed. Except for the requirement just described, sound quality of analog outputs is not restricted in any way by Digital CCI.

3.3 **Recording Technologies.** Licensed Products shall not pass Decrypted Type 2 Audio DT Data to any recording technology except, where such Decrypted Type 2 Audio DT Data is encoded other than Copy Never or No More Copies, to a technology listed in a subsection of this section 3.3.

3.3.1 The copy is scrambled or encrypted using a copy protection technology that is identified by DTLA for use with Type 2 Audio DT Data.

3.3.2 Methods which may be approved by DTLA in the future for Type 2 Audio DT Data.

3.4 **Internet Retransmission.** The parties acknowledge that Licensed Products shall not permit retransmission of Decrypted Type 2 Audio DT Data to the Internet.

EXHIBIT B AUDIO, PART 3: COMPLIANCE RULES FOR TYPE 3 AUDIO CONTENT

1. APPLICABILITY. This Part 3 of this Exhibit B is applicable to Licensed Products that handle Type 3 Audio DT Data.

2. DEFINITIONS. For purposes of this Part 3, the following terms shall have the meanings set forth below.

2.1 "Decrypted Type 3 Audio DT Data" shall mean, with respect to any Licensed Product, Type 3 Audio DT Data that has been received by such Licensed Product's Sink Function and decrypted by such Licensed Product according to DTCP but has not been passed to an output permitted by this Part 3 of this Exhibit B.

2.2 "Type 3 Audio DT Data" shall mean Audio DT Data that is "Type 3: Super Audio CD" content as described in the Specification.

3. SINK FUNCTIONS.

3.1 **No Copies**. Licensed Products shall be constructed such that Type 3 Audio DT Data received via their Sink Functions may not, once decrypted, be stored except as Transitory Audio Data. Adopter is advised that these Compliance Rules Audio may be amended in the future to permit copying of certain Type 3 Audio DT Data.

3.2 **Permitted Outputs**.

3.2.1 **Digital Outputs.** Licensed Products may only pass Decrypted Type 3 Audio DT Data to a digital output as follows:

3.2.2 To DTCP-protected IEEE 1394 outputs according to the Specification, provided that such Licensed Product passes through, without alteration, the value of the Embedded CCI and EMI (as such terms are used in the Specification) associated with such Decrypted Type 3 Audio DT Data; or

3.2.3 To outputs protected by other methods, if any, that may be approved by DTLA in the future for Type 3 Audio DT Data.

3.3 **Analog Outputs.** Licensed Products may only pass Decrypted Type 3 Audio DT Data to an analog output at a rate equal to or slower than real time.

3.4 **Internet Retransmission**. The parties acknowledge that Licensed Products shall not permit retransmission of Decrypted Type 3 Audio DT Data to the Internet.

EXHIBIT "C"
ROBUSTNESS RULES

1. CONSTRUCTION

1.1 **Generally.** Licensed Products as shipped shall meet the applicable Compliance Rules set forth in Exhibit B, and shall be manufactured in a manner clearly designed to effectively frustrate attempts to modify such Licensed Products to defeat the content protection requirements of DTCP set forth in the Specification and Compliance Rules.

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

(a) switches, buttons, jumpers or software equivalents thereof**,**
(b) specific traces that can be cut, or
(c) functions (including service menus and remote-control functions),

in each case by which the mandatory provisions of the Specification or the Compliance Rules, including the content protection technologies, analog protection systems, output protections, output restrictions, recording protections or recording limitations can be defeated, or by which compressed Decrypted DT Data in such Licensed Products can be exposed to output, interception, retransmission or copying, in each case other than as permitted under this Agreement.

1.3 **Keep Secrets.** Licensed Products shall be manufactured in a manner that is clearly designed to effectively frustrate attempts to discover or reveal Device Keys, the Highly Confidential cryptographic algorithms used in DTCP, and any other Highly Confidential Information.

1.4 **Robustness Checklist.** Before releasing any Licensed Product, Adopter must perform tests and analyses to assure compliance with these Robustness Rules. A Robustness Checklist is attached as Exhibit C-1 for the purpose of assisting Adopter in performing tests covering certain important aspects of these Robustness Rules. Inasmuch as the Robustness Checklist does not address all elements required for the manufacture of a Compliant product, Adopter is strongly advised to review carefully the Specification, Compliance Rules (including, for avoidance of doubt, these Robustness Rules) so as to evaluate thoroughly both its testing procedures and the compliance of its Licensed Products. Adopter shall provide copies of the Specification, the Compliance Rules (including, for avoidance of doubt, these Robustness Rules) and the Robustness Checklist to its supervisors responsible for design and manufacture of Licensed Products.

2. DATA PATHS

Decrypted DT Data shall not be available on outputs other than those specified in the Compliance Rules. Within a Licensed Product that includes Sink Functions, Decrypted Type 2 Audio DT Data, Decrypted Type 3 Audio DT Data, and the video portion of Decrypted DT Data, shall not be present on any user-accessible buses in analog or unencrypted, compressed form.

2.1 A "user accessible bus" means (a) an internal analog connector that: (i) is designed and incorporated for the purpose of permitting end user upgrades or access or (ii) otherwise readily facilitates end user access or (b) a data bus that is designed for end user upgrades or access, such as an implementation of a smartcard, PCMCIA, Cardbus, or PCI that has standard sockets or otherwise readily facilitates end user access. A "user accessible bus" does not include memory buses, CPU buses, or similar portions of a device's internal architecture that do not permit access to content in a form useable by end users.

Clause 2.1(a) should be interpreted and applied so as to allow Adopter to design and manufacture its products to incorporate means, such as test points, used by Adopter or professionals to analyze or repair products; but not to provide a pretext for inducing consumers to obtain ready and unobstructed access to internal analog connectors. Without limiting the foregoing, with respect to clause 2.1(a), an internal analog connector shall be presumed to not "readily facilitate end user access" if (i) such connector and the video signal formats or levels of signals provided to such connector, are of a type not generally compatible with the accessible connections on consumer products, (ii) such access would create a risk of product damage, or (iii) such access would result in physical evidence that such access had occurred and would void any product warranty.

2.2 Licensed Products that use Common Device Keys or are manufactured after December 31, 2006, shall be clearly designed such that when the video portion of uncompressed, Decrypted DT Data with a resolution greater than a Constrained Image is transmitted over a User Accessible Bus, such Decrypted DT Data are reasonably secure from unauthorized interception by using either Widely Available Tools or Specialized Tools, except with difficulty, other than Circumvention Devices. The level of difficulty applicable to Widely Available Tools is such that a typical consumer should not be able to use Widely Available Tools, with or without instructions, to intercept such Decrypted DT Data without risk of serious damage to the product or personal injury. Without limiting the foregoing, if Adopter at any time (the "Applicable Date") distributes a Licensed Product that uses a Common Device Key and that is capable of protecting uncompressed Decrypted DT Data over a User Accessible Bus as set forth in this Section 2.2, Adopter shall at such time and thereafter cause, to the extent technically feasible and commercially reasonable, all first activations of the DTCP functions of units or copies of all versions of such Licensed Product to protect uncompressed Decrypted DT Data over a User Accessible Bus as set forth in this Section 2.2. In the event that Adopter reasonably concludes that a software application contains or consists of a copy of such Licensed Product whose DTCP functions were activated prior to the Applicable Date on a particular device and subsequently re-installed on the same device, the activation or re-activation of the DTCP functions of such re-installed copy shall not be deemed to be a "first activation" for purposes of this Section 2.2 If a software application containing or consisting of a copy of such Licensed Product whose DTCP functions were first activated on a particular device is installed and activated via an Update on a different device, such activation of the DTCP functions of such copy installed on the different device shall be deemed to be a "first activation" for purposes of this Section 2.2, subject to the reasonableness standard of the preceding sentence.

2.3 Adopter is alerted that these Robustness Rules may be revised in the future, upon notification by DTLA, to require that, when DTLA deems that it is technically feasible and commercially reasonable to do so, Licensed Products be clearly designed such that when uncompressed, Decrypted DT Data

other than such data described in Section 2.2 of these Robustness Rules are transmitted over a User Accessible Bus, such Decrypted DT Data are made reasonably secure from unauthorized interception by use of means that can be defeated neither by using Widely Available Tools nor by using Specialized Tools, except with difficulty, other than Circumvention Devices. The level of difficulty applicable to Widely Available Tools is such that a typical consumer should not be able to use Widely Available Tools, with or without instruction, to intercept such Decrypted DT Data without risk of serious damage to the product or personal injury. Adopter is further alerted that, when it is deemed technically feasible and reasonably practicable to do so, DTLA will revise these Robustness Rules to require that uncompressed Decrypted DT Data will be re-encrypted or otherwise protected before it is transmitted over such buses.

3. METHODS OF MAKING FUNCTIONS ROBUST

Licensed Products shall be manufactured using at least the following techniques in a manner that is clearly designed to effectively frustrate attempts to defeat the content protection requirements set forth below.

3.1 **Distributed Functions.** In a Licensed Product having Sink Functions**,** where DT Data is delivered from one part of the Licensed Product to another, whether among integrated circuits, software modules, or otherwise or a combination thereof, the portions of the Licensed Product 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 Decrypted DT Data in any usable form flowing between these portions of the Licensed Product shall be reasonably secure from being intercepted or copied except as authorized by the Compliance Rules.

3.2 **Software.** Any portion of the Licensed Product that implements any of the content protection requirements of the Specification or Section 2.2.1.2 of Part 1 of Exhibit B in Software shall include all of the characteristics set forth in Sections 1 and 2 of this Exhibit C. For the purposes of these Robustness Rules, "Software" shall mean the implementation of the content protection requirements as to which this Agreement requires a Licensed Product to be compliant through any computer program code consisting of instructions or data, other than such instructions or data that are included in Hardware. Such implementations shall:

3.2.1 Comply with Section 1.3 of this Exhibit C by a 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 addition, in every case of implementation in Software, using techniques of obfuscation clearly designed to effectively disguise and hamper attempts to discover the approaches used.

3.2.2 Be designed so as 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 C.

This provision requires at a minimum the use of "signed code" or more robust means of "tagging" operating throughout the code.

3.3 **Hardware.** Any portion of the Licensed Product that implements any of the content protection requirements of the Specification or Section 2.2.1.2 of Part 1 of Exhibit B in Hardware shall include all of the characteristics set forth in Sections 1 and 2 of this Exhibit C. For the purposes of these Robustness Rules, "Hardware" shall mean a physical device, including a component, that implements any of the content protection requirements as to which this Agreement requires that a Licensed Product be compliant and that (i) does not include instructions or data other than such instructions or data that are permanently embedded in such device or component; or (ii) includes instructions or data that are not permanently embedded in such device or component where such instructions or data have been customized for such Licensed Product or Licensed Component and such instructions or data are not accessible to the end user through the Licensed Product or Licensed Component. Such implementations shall:

3.3.1 Comply with Section 1.3 of this Exhibit C by any reasonable method including but not limited to embedding Device Keys and Highly Confidential cryptographic algorithms in silicon circuitry or firmware that cannot reasonably be read, or employing the techniques described above for Software.

3.3.2 Be designed such that attempts to remove, replace, or reprogram Hardware elements in a way that would compromise the content protection requirements of DTCP (including compliance with the Compliance Rules and Specification) in Licensed Products would pose a serious risk of rendering the Licensed Product unable to receive, decrypt, or decode DT Data. By way of example, a component that is soldered rather than socketed may be appropriate for this means.

3.4 **Hybrid.** The interfaces between Hardware and Software portions of a Licensed Product shall be designed so that the Hardware portions comply with the level of protection that would be provided by a pure Hardware implementation, and the Software portions comply with the level of protection which would be provided by a pure Software implementation.

3.5 **Level of Protection.** "Core Functions" of DTCP include encryption, decryption, authentication, the functions described in Sections 2 (excluding Sections 2.2.1.1 and 2.2.1.3), 3 and 4.4.1 of Part 1 of this Exhibit B and Sections 2.3 and 3 of Part 2 of Exhibit B, maintaining the confidentiality of Highly Confidential cryptographic algorithms and Device Keys and preventing exposure of compressed, Decrypted DT Data. The Core Functions of DTCP shall be implemented in a reasonable method so that they:

3.5.1 Cannot be defeated or circumvented merely by using general-purpose tools or equipment that are widely available at a reasonable price, such as screwdrivers, 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 decompilers ("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 by DTCP ("Circumvention Devices"); and

3.5.2 Can only with difficulty be defeated or circumvented using professional tools or equipment, such as logic analyzers, chip disassembly systems, or in-circuit emulators or any other tools, equipment, methods, or techniques not described in Section 3.5.1 such as would be used primarily by persons of professional skill and training, but not including professional tools or equipment that are made available only on the basis of a non-disclosure agreement or Circumvention Devices.

3.6 The following shall be implemented in a reasonable method that is intended to make such functions difficult to defeat or circumvent by the use of Widely Available Tools, not including Circumvention Devices or Specialized Tools as defined in Section 3.5.1:

(i) delivery of Decrypted DT Data to the functions described in Part 1 of Exhibit B, Sections 4.2, 4.3, 4.4.2 and 4.6; and

(ii) the method by which the DTCP functions in individual units or copies of certain Licensed Products or Licensed Products
incorporating Robust Licensed Components are designed to cease to function as
required by Section 2.2(i)(y) of the Procedural Appendix.

3.7 **Advance of Technology.** Although an implementation of a Licensed Product when designed and first shipped may meet the above standards, subsequent circumstances may arise which, had they existed at the time of design of a particular Licensed Product, would have caused such products to fail to comply with these Robustness Rules ("New Circumstances"). If an Adopter 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 (18) months after Notice such Adopter shall cease distribution of such Licensed Product and shall only distribute Licensed Products that are compliant with the Robustness Rules in view of the then-current circumstances.

4. EXAMINATION

4.1 **Generally.** A group of Content Participants is being or has been formed ("CPUG"). If CPUG so requests via DTLA, Adopter shall provide, once per model or version of product, any publicly available technical design documentation and, under a reasonable, mutually-acceptable non-disclosure agreement, the service manual for such product, in order to assist in the evaluation of the compliance of such product with these Robustness Rules.

4.2 **Inspection and Report.** Upon a reasonable and good faith belief that a particular hardware model or software version of a Licensed Product designed or manufactured by Adopter does not comply with the Robustness Rules then in effect for such Licensed Product, and upon reasonable notice to Adopter via DTLA, CPUG may request Adopter to submit promptly to an independent expert (acceptable to Adopter, which acceptance shall not be unreasonably withheld) for inspection

such detailed information as Adopter deems necessary to understand such product's implementation of the Specification and Compliance Rules, such as would be sufficient to determine whether such product complies with these Robustness Rules. Adopter's participation in this inspection procedure is voluntary; no adverse inference may be drawn from Adopter's refusal of the CPUG request or refusal to participate, in whole or in part, in such inspection. The conduct of such inspection and the contents of any report made by the independent expert shall be subject to the provisions of a nondisclosure agreement, mutually-agreeable to CPUG, Adopter, and such expert, such agreement not to be unreasonably withheld, that also provide protections for Confidential Information and Highly Confidential Information relating to DTCP that are no less stringent than those provided for in this Agreement. Such examination and report shall be conducted at the sole expense of CPUG. Nothing in this paragraph shall limit the role or testimony of such expert, if any, in a judicial proceeding under such protective orders as a court may impose. Adopter shall not be precluded or estopped from challenging the opinion of such expert in any forum; nor shall any party be entitled to argue that any greater weight or evidentiary presumption should be accorded to the expert report than to any other relevant evidence. This provision may not be invoked more than once per hardware model or software version, provided that such right of inspection shall include the right to re-inspect the implementation of such model or version if it has been revised in an effort to cure any alleged failure of compliance.

EXHIBIT C-1
ROBUSTNESS CHECKLIST

Notice: This Checklist is intended as an aid to the correct implementation of the Robustness Rules for hardware and software implementations of the DTCP Specification in a Licensed Product. DTLA strongly recommends that you complete this Checklist for each hardware model or software version of a Licensed Product before releasing any product and at a sufficiently early date in design, as well as during production, to avoid product compliance redesign delays. This Checklist does not address all aspects of the Specification and Compliance Rules necessary to create a product that is fully compliant. Failure to perform necessary tests and analysis could result in a failure to comply fully with the Specification, Compliance Rules or Robustness Rules in breach of the DTLA Adopter Agreement and, as a consequence, in appropriate legal action of DTLA and Eligible Content Participants.

Notwithstanding whether any particular design or production work is being outsourced or handled by contractors to the company, compliance with the above Rules remains the responsibility of this company.

DATE: _____

MANUFACTURER: _____

PRODUCT NAME: _____

HARDWARE MODEL OR SOFTWARE VERSION: _____

NAME OF TEST ENGINEER COMPLETING CHECKLIST:

TEST ENGINEER: _____

COMPANY NAME: _____

COMPANY ADDRESS: _____

_____

PHONE NUMBER: _____

FAX NUMBER: _____

GENERAL IMPLEMENTATION QUESTIONS

1. Has the Licensed Product been designed and manufactured so there are no switches, buttons, jumpers, or software equivalents of the foregoing, or specific traces that can be cut, by which the content protection technologies, analog protection systems, output restrictions, recording limitations, or other mandatory provisions of the Specification or Compliance Rules can be defeated or by which Decrypted DT Data can be exposed to unauthorized copying?

2. Has the Licensed Product been designed and manufactured so there are no service menus and no functions (such as remote-control functions, switches, check boxes, or other means) that can intercept the flow of Decrypted DT Data or expose it to unauthorized copying?

3. Has the Licensed Product been designed and manufactured so there are no service menus and no functions (such as remote-control functions, switches, check boxes, or other means) that can turn off any analog protection systems, output restrictions, recording limitations, or other mandatory provisions of the Specification or Compliance Rules?

4. Does the Licensed Product have service menus, service functions, or service utilities that can alter or expose the flow of Decrypted DT Data 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 Decrypted DT Data.

5. Does the Licensed Product have service menus, service functions, or service utilities that can turn off any analog protection systems, output restrictions, recording limitations, or other mandatory provisions of the Specification 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 content protection features of DTCP (including compliance with the Compliance Rules and the Specification).

6. Does the Licensed Product have any user-accessible buses (as defined in Section 2.1 of the Robustness Rules)?

   If so, is Decrypted DT Data carried on this bus?

   If so, then:
identify and describe the bus, and whether the Decrypted DT Data is compressed or uncompressed. If such Data is compressed, then explain in detail how and by what means the data is being protected as required by Section 2.2 of the Compliance Rules.

7. Explain in detail how the Licensed Product protects the confidentiality of all keys.

8. Explain in detail how the Licensed Product protects the confidentiality of the confidential cryptographic algorithms used in DTCP.

9. If the Licensed Product delivers Decrypted DT Data 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 Decrypted DT Data are secure from interception and copying as required in Section 3.1 of the Robustness Rules.

10. Are any DTCP functions implemented in Hardware?

    If Yes, complete hardware implementation questions.

11. Are any DTCP functions implemented in Software?

    If Yes, complete software implementation questions.

SOFTWARE IMPLEMENTATION QUESTIONS

12. In the Licensed Product, describe the method by which all Device Keys are stored in a protected manner.

13. Using the grep utility or equivalent, are you unable to discover any Device Keys in binary images of any persistent memory devices?

14. In the Licensed Product, describe the method used to obfuscate the confidential cryptographic algorithms and Device Keys used in DTCP and implemented in software.

15. Describe the method in the Licensed Product by which the intermediate cryptographic values (e.g., values created during the process of authentication between modules or devices within a Licensed Product) are created and held in a protected manner.

16. Describe the method being used to prevent commonly available debugging or decompiling tools (e.g., Softice) from being used to single-step, decompile, or examine the operation of the DTCP functions implemented in software.

17. Describe the method by which the Licensed Product self-checks the integrity of component parts in such manner that modifications will cause failure of authorization or decryption as described in Section 3.2.2 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 DTCP functions, and describe the method and results of the test.

HARDWARE IMPLEMENTATION QUESTIONS

19. In the Licensed Product, describe the method by which all Device 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 Device Keys in binary images of any persistent memory devices?

21. In the Licensed Product, describe how the confidential cryptographic algorithms and Device Keys used in DTCP have been implemented in silicon circuitry or firmware so that they cannot be read.

22. Describe the method in the Licensed Product by which the intermediate cryptographic values (e.g., values created during the process of authentication between modules or devices within a Licensed Product) are created and held in a protected manner.

23. Describe the means used to prevent attempts to replace, remove, or alter hardware elements or modules used to implement DTCP functions.

24. In the Licensed Product, does the removal or replacement of hardware elements or modules that would compromise the content protection features of DTCP (including the Compliance Rules, the Specification, and the Robustness Rules) damage the Licensed Product so as to render the Licensed Product unable to receive, decrypt, or decode DT Data?

Notice: This checklist does not supersede or supplant the DTCP Specification, Compliance Rules, or Robustness Rules. The Company and its Test Engineer are advised that there are elements of the Specification and 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 D: ACTIVATION NOTICE

The undersigned ("Adopter") having entered into a DIGITAL TRANSMISSION PROTECTION LICENSE AGREEMENT – Development and Evaluation License (the "Adopter Agreement") with the Digital Transmission Licensing Administrator, LLC ("DTLA") hereby activates its rights under the Adopter Agreement in accordance with Section 2.2 of the Adopter Agreement subject to the following:

(1) Adopter chooses to be a:
Component Supplier ☐
Adopter- Small ☐
Adopter- Large ☐
(choose only one category)

(2) The fees to be paid in connection with the: (i) activation of the Adopter Agreement and selection of an Adopter category; and (ii) issuance, shipping and handling of Device Certificates and Device Keys, are set forth on Exhibit A to this Activation Notice, which may be amended by DTLA in accordance with the terms of the Adopter Agreement.

(3) The evaluation fee paid by Adopter shall be credited against the fees associated with the chosen Adopter category.

(4) Adopter acknowledges and agrees that DTLA shall ship all orders for Device Certificates and Device Keys in electronic form using Pretty Good Privacy (PGP) as described in the DTLA DTCP Keying Material Order Guide.
If Adopter does not have or is unable to provide DTLA its PGP public key, Adopter shall, at its own cost and expense, with each order placed with DTLA, designate an agent who shall pick up the generated Device Certificates and Device Keys at a location designated by DTLA.

(5) All capitalized terms not otherwise defined herein shall have the meanings set forth in the Adopter Agreement.

Please make checks payable to "DTLA" and send such check, together with an executed copy of this Activation Notice and, if available, a CD-ROM containing Adopter's public key, to the following address:
Digital Transmission Licensing Administrator
c/o License Management International, LLC
380 Tennant Avenue, Unit #4
Morgan Hill CA 95037

Please call for wire information.

_____
Company Name
By:_____
Name:_____
Title:_____
Date: _____

EXHIBIT A
TO THE
ACTIVATION NOTICE

ADOPTER CATEGORY ADMINISTRATION FEES

Component Supplier: $14,000
Small Adopter Fee: $14,000
Large Adopter Fee: $18,000

DEVICE CERTIFICATE AND DEVICE KEY FEES

CATEGORY	Per Unique Certificate Fee	
	Order Format 1 Order Format 5 Full	**Order Format 3 Restricted/Full**
Small Adopter	.06	.07
Large Adopter	.05	.06

Shipping and Handling - $200.00 / order

Per Common Certificate Fee (Large Adopter Only)
Unit Options Up to a maximum of 4 keys/total 20,000 units or copies -- $1,000 Up to 100,000 units or copies -- $2,000 Up to 200,000 units or copies -- $4,000 Up to 500,000 units or copies -- $6,000 Up to 1,000,000 units or copies -- $10,000 Up to 2,000,000 units or copies -- $12,000 Up to 5,000,000 units or copies -- $15,000 Up to10,000,000 units or copies -- $25,000 Up to 30,000,000 units or copies -- $50,000 Blanket Option Up to a maximum of 5 Common Device Keys and Common Device Certificates -- $100,000 Additional Common Device Keys and Common Device Certificates -- $1,000

Shipping and Handling - $200.00 / order

OTHER FEES:

- The fee for replacing a PGP key is $3000.00
- The fee for additional hardcopies of DTLA confidential or highly confidential specifications is $500.00