

Revised May 24, 2018



**HDCP 2.01 ADDENDUM
TO
HDCP LICENSE AGREEMENT**

This HDCP 2.01 ADDENDUM to Adopter's HDCP LICENSE AGREEMENT ("Addendum") is entered into as of the latest date set out on the signature page hereof ("Effective Date") by Digital Content Protection, LLC, a Delaware limited liability company ("Licensor"), and Adopter named on the signature page of the Addendum and Addendum supersedes any prior addendum.

Whereas, Adopter and Licensor have entered into an HDCP LICENSE AGREEMENT ("Agreement") and Adopter is an Adopter in good standing under such Agreement;

Whereas, Adopter wishes to implement the HDCP Specification Rev. 2.0 (as defined below) and Licensor is willing to grant license rights to HDCP Specification Rev. 2.0 subject to Adopter's Agreement and the additional rights and obligations contained in this Addendum to such Agreement;

Whereas, in furtherance of such desire, the parties agree to amend the Adopter's Agreement as set forth below in this Addendum;

NOW, THEREFORE, Licensor and Adopter hereby agree and acknowledge the following terms and conditions:

Part 1.

1. All capitalized terms not defined or modified in this Addendum shall have the same meaning as set forth in the Agreement, including its Exhibits, the HDCP Specification or the HDCP Specification Rev 2.0.

2. The following definitions shall be added to Section 1 of the Agreement:

(i) "Activation" means, with respect to a Deactivated Keyed Licensed Component distributed by an Adopter, the distribution of a Licensed Component, ("Adopter Activation"), issued by such Adopter, solely for distribution to Fellow Adopter(s), to update such Deactivated Keyed Licensed Component to become a Licensed Component. As an example, Activation of Deactivated Keyed Licensed Components may include decryption of firmware and/or keys necessary to utilize the HDCP functions, with the keys required for decryption provided by the Adopter only to Fellow HDCP Adopters.

(ii) "Circumvention Device" means a device or technology whether hardware or software that is designed and made available for the specific purpose of bypassing or circumventing the protection technologies required by HDCP, provided that (x) no Licensed Product is excused from full compliance with any Robustness Rule and/or Compliance Rule due to the existence of one or more relevant Circumvention Devices, and (y) the broad distribution and widespread use by consumers of a particular Circumvention Device should be examined by the Adopter and will be examined by the Licensor to determine whether the particular situation related to a particular Circumvention Device constitutes a New Circumstance as that term is defined and used in the Advance of Technology provision of the Robustness Rules.

(iii) "Core Functions" of HDCP include encryption of video portions of Audiovisual Content, decryption of video portions of HDCP Content that is Audiovisual Content, storing and handling of Device Secret Keys, Session Keys used to encrypt or decrypt video portions of Audiovisual Content and Master Keys ("HDCP Core Keys") in plaintext form during the HDCP authentication protocol, handling of information or materials, including but not limited to cryptographic keys used to encrypt or decrypt HDCP Core Keys, from which HDCP Core Keys could reasonably be derived, protecting the video portions of Decrypted HDCP Content against unauthorized exposure, maintaining the confidentiality and integrity of HDCP Core Keys and other information or materials, including but not limited to cryptographic keys used to encrypt or decrypt HDCP Core Keys, from which HDCP Core Keys could reasonably be derived.

(iv) “Deactivated Keyed Licensed Component” means a Licensed Component having a Device Key incorporated therein that is designed to be updated via an Activation and is designed such that unless updated via an Activation it shall not (i) perform any HDCP functions; or, (ii) display any HDCP Content via any output.

(v) “Device Secret Key(s)” shall mean a cryptographic value that consists of (a) the secret Global Constant applicable to the HDCP 2.0 Source Device or HDCP 2.0 Repeater Device; or, (b) the secret Global Constant and the RSA private key uniquely applicable to the HDCP 2.0 Presentation Device or function used to receive and decrypt HDCP Content in HDCP 2.0 Repeater Device.

(vi) “Global Constant” shall mean a random, secret constant provided only to Adopter and used during HDCP Content encryption or decryption

(vii) “Hardware” means, for the purposes of the Robustness Rules specified in Exhibit D, a physical device or component, that implements any of the content protection requirements of the HDCP Specification Rev 2.0, and the Compliance Rules 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 (e.g., firmware instructions or data) that are not permanently embedded in such device or component where such instructions or data are specific to such device or component and where the device or component prevents unauthorized modifications that defeat the content protection requirements of the HDCP Specification Rev 2.0, and the Compliance Rules to such instructions or data, to the level of protection specified in, as applicable, Section 4.3 through 4.4.

(viii) “Hardware Root of Trust” means, for the purposes of the Robustness Rules specified in Exhibit D, security primitives composed of Hardware that provide a set of trusted, security-critical functions and that are designed to always behave in the expected manner.

(ix) “HDCP Protected Interface” shall mean an interface to which HDCP has been applied.

(x) “HDCP Protected Output” shall mean an output for which HDCP applies.

(xi) “HDCP 2.0 Presentation Device” shall mean a Presentation Device that implements the HDCP Specification Rev 2.0. For the avoidance of doubt, a Presentation Device is a Licensed Product.

(xii) “HDCP 2.0 Repeater Device” shall mean a Repeater Device that implements the HDCP Specification Rev 2.0.

(xiii) “HDCP 2.0 Source Device” shall mean a Source Device that implements the HDCP Specification Rev 2.0.

(xiv) “HDCP Specification Rev. 2.0” shall mean the specification entitled “High Bandwidth Digital Content Protection System, Revision 2.0 and any revisions thereto (including the “Errata” thereto).

(xv) “Keyed Licensed Component” means a Licensed Component having a Device Key incorporated therein.

(xvi) “Master Key” shall mean a 128-bit random, secret cryptographic key negotiated between the HDCP Transmitter and the HDCP Receiver during Authentication and Key Exchange and used to pair the HDCP Transmitter with the HDCP Receiver

(xvii) “Public Key Certificate” shall mean a certificate, signed and issued by Licensor, that contains the Receiver ID and RSA public key corresponding to the Device Secret Key of a Presentation Device or Repeater Device.

(xviii) “Receiver ID” shall mean a value that uniquely identifies the Presentation Device or Repeater Device and shall be used for the sole purpose of implementing the HDCP Specification Rev. 2.0 or higher.

(xix) “Session Key” shall mean a 128-bit random, secret cryptographic key negotiated between the HDCP Transmitter and the HDCP Receiver during Session Key exchange and used during HDCP Content encryption or decryption.

(xii) “Source Key(s)” shall have the same meaning as “Device Secret Key(s)” as applicable to Source Devices and Source Function of Repeater Devices when used for the sole purpose of implementing the HDCP Specification Rev. 2.0 (including

the “Errata” thereto)

(xx) “Secure Load” means, with respect to any instructions or data included in Hardware or Software, the process by which the initial trusted state for such instructions or data are established before they are executed.

(xxi) “Software” means, for the purposes of the Robustness Rules specified in Exhibit D, the implementation of content protection requirements of the HDCP Specification Rev 2.0 and Compliance Rules through any computer program code consisting of instructions and/or data, other than such instructions and/or data that are included in Hardware.

(xxii) “User-Accessible Bus” means a data bus that is designed and incorporated for the purpose of permitting 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 form usable by end users.

Part 2.

1. The following subsections of Section 1 of the Agreement shall be amended as follows:

(i) Section 1.2 (definition of “Adopter Agreement”) shall be modified by adding the following words at the end of the Section: “... or Robust Inactive Products.”

(ii) Section 1.3 “Affected Adopter” shall be deleted in its entirety and replaced with the following:

“**Affected Adopter**” shall mean, (i) with respect to a KSV for which Revocation is requested or contemplated; or, (ii) with respect to a Receiver ID for which Revocation is requested or contemplated, any Fellow Adopter to whom Licensor or Key Generator has issued a Device Key Set associated with such KSV or Receiver ID, as applicable, under such

Fellow Adopter's Adopter Agreement and applicable HDCP 2.0 Addendum.”

(iii) Section 1.32 “HDCP Specification” shall be deleted in its entirety and replaced with the following:

“**HDCP Specification**” shall mean (i) the specification entitled “HDCP Content Protection Specification, Release 1.1” and any revisions thereto (including the “Errata” thereto); and (ii) the specification entitled “High Bandwidth Digital Content Protection System, Revision 2.0 and any revisions thereto (including the “Errata” thereto), as such specifications may be amended from time to time pursuant to Section 5 of the Agreement.

(iv) Section 1.18 Clarification shall be added to the end of this section as follows:

“Device Key includes secret key for Source Device, Presentation Device and Repeater implementing HDCP 1.1 and its revisions, Global Constant for HDCP 2.0 Source Device, and Global Constant and RSA Private Keys for HDCP 2.0 Presentation Device and HDCP 2.0 Repeater.”

(v) Section 1.19 “Device Key Set” shall be deleted in its entirety and replaced with the following:

“**Device Key Sets**” means (i) a set of Device Keys provided to Adopter or Fellow Adopter by Licensor or its designee for use in a Licensed Product or a Licensed Component; or, (ii) a set of Device Keys provided to Adopter or fellow Adopter by Licensor or its designee for use in a HDCP 2.0 Presentation Device or HDCP 2.0 Repeater Device’s functionality to receive and decrypt HDCP Content. Such Device Key Set shall consist of the Device Secret Key and corresponding Public Key Certificate. Device Key Sets are required for a Licensed Product, HDCP 2.0 Presentation Device or HDCP 2.0 Repeater Device to operate.

(vi) Section 1.33 “Highly Confidential Information” shall be deleted in its entirety and replaced with the following:

“Highly Confidential Information” means (i) Device Keys, Device Key Sets, Device Secret Keys, Global Constants, and any other intermediate cryptographic values or other values identified as requiring confidentiality in Appendix A to the HDCP Specification and HDCP Specification Rev 2.0; (ii) any other proprietary information disclosed to any Person by Licensor, its designee, or Founder or any Affiliate thereof that is marked “Highly Confidential” when disclosed in written or electronic form; and, (iii) any other proprietary information from which any of the foregoing can be derived.

(vii) Section 1.36 “Key Generator shall be deleted in its entirety and replaced with the following:

“Key Generator” means the generator of Device Keys, Device Key Sets, Device Secret Keys, Global Constants, KSVs, Public Key Certificate, Receiver IDs, RSA Private Key, Source Keys and System Renewability Messages designated by Licensor.”

(viii) Section 1.52 “Rescind” shall be deleted in its entirety and replaced with the following:

“Rescind” means with respect to a Revocation of (i) a KSV, to distribute to Content Participants a new System Renewability Message that does not contain such KSV; or (ii) a Receiver ID, to distribute to Content Participants a new System Renewability Message that does not contain such Receiver ID. Rescind shall include generally “Rescission”

(ix) Section 1.55 “Revoke” shall be deleted in its entirety and replaced with the following:

“Revoke” means with respect to (i) a KSV, to distribute information, as authorized or provided by Licensor, to Content Participants for purposes of their further distribution such information with Audiovisual Content in

order to cause such KSV in Presentation or Repeater Devices to be invalidated with respect to such content; or, (ii) a Receiver ID, to distribute information, as authorized or provided by Licensor, to Content Participants for purposes of their further distribution of such information with Audiovisual Content in order to cause such Receiver ID in HDCP 2.0 Presentation or HDCP 2.0 Repeater Devices to be invalidated with respect to such content (generally, “Revocation” or “Revoked”). *Adopter is advised that, although neither the Agreement, this Addendum nor the HDCP Specification Rev 2.0 imposes any obligation on a Licensed Product with respect to how such Licensed Product should respond to such invalidation of a KSV or a Receiver ID, the license agreements relating to other technologies implemented in the product containing an HDCP-protected connection may impose such requirements.*

Part 3

Section 2 of the Agreement shall be amended as follows:

- (i) Section 2 shall be renamed to “LICENSE AND ADOPTER REQUIREMENTS”
- (ii) Section 2.1 shall be deleted in its entirety and replaced with the following (for the avoidance of doubt, Sections 2.1.1, 2.1.2 and 2.1.3 of the Agreement remain unchanged.):

License. Subject to the limitations set forth in Section 2.4 and the other terms and conditions of the Agreement and this Addendum, including but not limited to Adopter’s compliance with Sections 2.2, 2.3 and 2.7 and payment of all fees required hereunder, Licensor grants to Adopter a nonexclusive, nontransferable (except pursuant to Section 12.3), non-sublicenseable, worldwide license (a) on behalf of, and as an authorized agent solely with respect to the licensing of Necessary Claims for, Founder, under the Necessary Claims of Founder in HDCP Specification Rev 2.0, as well as (b) under any trade secrets or copyrights of Founder or Licensor embodied in the HDCP Specification Rev 2.0:

For the avoidance of doubt, Section 2.1.1, 2.1.2, and 2.1.3 shall be deemed to incorporate a license to implement the HDCP Specification Rev 2.0 in, Licensed Products, Licensed Components, Robust Inactive Products Licensed Source Components, and/or Robust Licensed Components.

(iii) Section 2.2 (“Fellow Adopter Non-Assertion”) of the Agreement shall be deleted in its entirety and replaced with the following:

“Subject to the limitations set forth in Section 2.4, and subject to a reciprocal promise by Fellow Adopter and its Affiliates, Adopter, on behalf of itself and its Affiliates, promises not to assert or maintain against any Fellow Adopter, any claim of infringement under its or their Necessary Claims, as well as under any trade secrets or copyrights embodied in the HDCP Specification Rev 2.0, to use, make, have made, sell, offer for sale and distribute such Licensed Products, Licensed Components, Robust Inactive Products for which any Fellow Adopter has been granted a license by Licensor under its Adopter Agreement. Adopter, on behalf of itself and its Affiliates, further promises not to assert or maintain against Licensor, Founder or any Affiliate thereof or Key Generator, any claim of infringement or misappropriation under its or their intellectual property rights for using, making, having made, offering for sale, selling and importing any Receiver ID, Global Constant, Source Key, KSV, Device Secret Key, Device Key or Device Key Set, or for using, copying, displaying, performing, making derivative works from (to the extent that such claim for making derivative works relates to intellectual property rights in or to the HDCP Specification Rev 2.0 or any portion thereof), or distributing the HDCP Specification Rev 2.0. For the avoidance of doubt, the foregoing Fellow Adopter Non-Assertion shall extend to activities or products for which any Fellow Adopter has been granted a license by Licensor under an Adopter Agreement entered into with Licensor prior to the HDCP Specification.”

(iv) Section 2.3 (“Content Participant and System Operator Non-Assertion”) of the Agreement shall be deleted in its entirety and replaced with the following:

“Subject to the limitations set forth in Section 2.4, and subject to a reciprocal promise by such Eligible Content Participant or such Eligible System Operator, Adopter, on behalf of itself and its Affiliates, promises not to assert or maintain against any Eligible Content Participant, Eligible System Operator or any of their respective Affiliates any claim of infringement or misappropriation under any Necessary Claims, as well as under any trade secrets or copyrights embodied in the HDCP Specification, for such Content Participant’s or System Operator’s or Affiliate’s causing or permitting the use of HDCP to protect Audiovisual Content, or in the case of an Eligible System Operator, for using, making, having made, offering to sell, selling or importing Licensed Source Components. For the avoidance of doubt, the foregoing Content Participant and System Operator Non-Assertion shall extend to activities or products for which any Eligible Content Participant or Eligible System Operator has been granted a license by Licensor under a Content Participant Agreement or System Operator Agreement to implement HDCP or to cause HDCP to be used entered into with Licensor prior to the HDCP Specification.”

(v) Section 2.4 (“Limitations on Sections 2.1, 2.2 and 2.3”) of the Agreement shall be deleted in its entirety and replaced with the following:

“The license and promises set out in Sections 2.1, 2.2, and 2.3 shall not extend to (a) claims related to features of a License Product, Licensed Component, Presentation Device, Repeater Device, Robust Inactive Product, Robust Licensed Component, Licensed Source Component that are not required to comply with, or aspects of any technology, codec, standard or product not disclosed with particularity in, the HDCP Specification, even if such technology, codec, standard, or product may be mentioned in or required by the HDCP Specification Rev 2.0 (including, by way of example, specifications such as DVI, HDMI, CSS, MPEG, IEEE 1394, DTCP, Upstream Protocol and tamper resistance technology), even though such technology, codec, standard or product may otherwise be mentioned in or required by the HDCP Specification, the Compliance Rules or the Robustness Rules; (b) claims related to features of a product for which there exists a commercially reasonable non-infringing

alternative ; (c) claims related to features of a product which, if licensed, would require payment of royalties by the Licensor to unaffiliated third parties; (d) claims that read solely on any implementation or use of any portion of the HDCP Specification Rev 2.0 where such implementation or use is not within the scope of the license to use HDCP granted to any Adopter, Content Participant or System Operator by Licensor; (e) claims relating to watermarking technology, semiconductors and semiconductor manufacturing technology, compiler technology, programming language, object-oriented technology, operating systems, middleware and database technology, or networking, internet, extranet or Internet technology; and, (f) to the promises pursuant to Sections 2.2 and 2.3, to any Person that is asserting or maintaining any claim of infringement or misappropriation under a Necessary Claim, or under any trade secrets or copyrights related to the HDCP Specification, against the promisor, where the promisor is not in breach of its Adopter Agreement, Content Participant Agreement or System Operator Agreement, as the case may be, or (g) the promises pursuant to Sections 2.2 and 2.3, to any Person following termination of this Agreement by Licensor pursuant to Section 9.1.2(a) or 9.1.2(b), provided, however, that the licenses pursuant to Sections 2.2 and 2.3 shall not be withdrawn with respect to any licensed activities or products made prior to the effective date of such termination.

(vi) Section 2.5 (“Have Made Obligations”) of the Agreement shall be deleted in its entirety and replaced with the following:

“Have Made Obligations. Adopter shall have the right under the licenses granted under Section 2.1 to have third parties (“Have Made Parties”) make Licensed Products, Licensed Components, Robust Inactive Products, Robust Licensed Components, Licensed Source Components, , or subparts thereof, consistent with the limitations of Section 2.1, 2.4 and 2.7, for the sole account of Adopter, provided that such Licensed Products, Licensed Components, Robust Licensed Products, Robust Licensed Components, Licensed Source Components, or subparts thereof (a) are to be sold, used, leased or otherwise disposed of, by or for Adopter under the trademark, tradename, or other commercial indicia of Adopter or a Person to which

Adopter is authorized hereunder to sell such Licensed Products, Licensed Components, Robust Inactive Products, Robust Licensed Components or Licensed Source Components, and (b) are made by such Have Made Parties using designs whose underlying copyrights and trade secrets are not infringed or misappropriated by Adopter. Adopter shall be fully responsible for such other Have Made Parties' compliance with all terms of this Agreement and Addendum. Have Made Parties must be Fellow Adopters, a Founder or Affiliates thereof, or be subject to an applicable non-disclosure agreement with Adopter on conditions that are no less stringent than the confidentiality provisions set out in Exhibit B-1, and must include the "Third Party Beneficiary" provisions set out therein for Licensor and Content Participant, if such manufacture requires disclosure to such Have Made Parties of (i) Confidential Information or (ii) other information or materials from which Confidential Information could reasonably be derived, (iii) Highly Confidential Information, or (iv) other information or materials from which Highly Confidential Information could reasonably be derived. Adopter agrees and acknowledges that the fact that it has contracted with a Have Made Party shall not relieve Adopter of any of its obligations under this Agreement. Have Made Parties shall receive no license, sublicense, or implied license with respect to any Necessary Claims related HDCP or the HDCP Specification Rev 2.0 or any copyrights or trade secrets contained in HDCP or the HDCP Specification Rev 2.0 pursuant to this Agreement, the Addendum or any such non-disclosure agreement.

(vii) Section 2.6 of the Agreement shall be amended to include reference to this Addendum.

(viii) Section 2.7 of the Agreement shall be deleted in its entirety and replaced with the following:

Compliance with Latest Version of the HDCP Specification Rev 2.0 and the Compliance Rules and Robustness Rules. Adopter shall, when manufacturing for sale or distribution a Licensed Product, Licensed Component, Presentation Device, Repeater Device, Licensed Source

Component, Robust Inactive Product , implement and comply with all requirements not expressly identified as optional or informative in the then current version of the HDCP Specification Rev 2.0 available for licensing from Licensor as of the Effective Date, or such later version as required under Sections 5.2 and 5.3 of the Agreement and the then current version of the Compliance Rules and Robustness Rules, including, any changes thereto as provided under Section 5.2.

(ix) Section 2.8 shall be added as follows:

Liability for Affiliates. The entity named on Exhibit E shall procure and be responsible for its Affiliates' compliance with the terms and conditions of this Agreement and Addendum, and such entity and each of its Affiliates that exercises any of the rights or licenses granted hereunder shall be jointly and severally liable for any noncompliance by any such Affiliate with the terms and conditions of this Agreement and Addendum.

Part 4.

Section 6 of the Agreement shall be amended as follows:

(i) Section 6.1 of the Agreement shall be deleted in its entirety and replaced with the following:

“Individual Privacy Respected.” Adopter shall not use any portion of the HDCP Specification, or any implementation thereof or the Device Keys, KSVs, Public Key Certificates or Receiver IDs for the purpose of identifying any individual or creating, or facilitating the creation of, any means of collecting or aggregating information about an individual or any device or product in which the HDCP Specification, or any portion thereof, is implemented. Adopter may not use the Device Keys, KSVs or Receiver IDs for any purpose other than to support (a) the authentication of a Licensed Product with another Licensed Product and to manage Revocation; (b) the authentication of a Presentation Device and/or Repeater Device with a Source Device and to manage Revocation; and, (c) to perform Revocation processing, both in the manner described in the

HDCP Specification Rev 2.0 and this Agreement and, as applicable, the Addendum. For the avoidance of doubt, nothing in the foregoing section shall prohibit the verification of information needed to ensure that an Update can be made in a manner consistent with the requirements of this Agreement.”

Part 5. Section 7 of the Agreement shall be amended as follows:

- (i) Section 7 shall be entitled “REVOCATION”
- (ii) Section 7.1 shall be deleted in its entirety and replaced with the following:

“Generally” Adopter acknowledges that the HDCP Specification and the HDCP Specification Rev. 2.0 describes means by which KSVs and Receiver IDs may be Revoked.”
- (iii) Section 7.2 shall be deleted in its entirety and replaced as follows:

“**Cause For Revocation**”. Subject to the Revocation procedures set out in this Agreement, Licensor, a Fellow Adopter (solely with respect to KSVs or Receiver IDs issued to such Fellow Adopter) or one or more Eligible Content Participant(s), may cause the Revocation of KSVs or Receiver IDs, as applicable, in accordance with the procedures set out in Section 3 of the Procedural Appendix, when (a) it or they determine(s) that the Revocation Criteria (defined below) have been satisfied or (b) in the case that an Affected Adopter does not consent to the Revocation in accordance with the terms of Section 3 of the Procedural Appendix, (i) an arbitrator determines that the Revocation Criteria have been satisfied, or (ii) as described in Section 4.2 of the Procedural Appendix, a court of competent jurisdiction issues, as an interim measure, preliminary injunctive relief pending the resolution of the arbitration. For purposes of this Agreement, “Revocation Criteria” means:
- (iv) Section 7.2.1 shall be deleted in its entirety and replaced as follows:

“a Device Key Set, Device Secret Key(s), associated with a KSV or a Receiver ID, as applicable, has been cloned such that the same

Device Key Set, Device Secret Key(s) is found in more than one device or product”

- (v) Section 7.2.2 shall be deleted in its entirety and replaced as follows:

“a Device Key Set, Device Secret Key(s) [Global Constant or Source Key] associated with a KSV or Receiver ID, as applicable, has been disclosed in violation of this Agreement or another agreement with Licensor, made public, lost, stolen, intercepted or otherwise misdirected; or”

- (vi) Section 7.2.3 shall be deleted in its entirety and replaced as follows:

“Licensor is required to Revoke a KSV or Receiver ID by the United States National Security Agency, a court order or by other competent government authority”

- (vii) Section 7.3 shall be deleted in its entirety and replaced as follows:

“Notwithstanding Section 7.2, in the event that Adopter is an Affected Adopter with respect to a Revocation and does not consent to such Revocation in accordance with Section 3.3 of the Procedural Appendix, Licensor shall not commence such Revocation unless and until (a) an arbitrator, or, in the circumstances set forth in Section 4.2 of the Procedural Appendix, a court of competent jurisdiction, determines that the claimant has demonstrated likelihood of success of showing that the Revocation Criteria have been satisfied or (b) Adopter otherwise consents to such Revocation. For the purpose of this Agreement, the parties intend the standard for such likelihood of success to be the same as the standard for issuance of a preliminary injunction in a given jurisdiction. Without limiting the foregoing, Licensor shall not Revoke KSVs or Receiver IDs where Revocation is (i) based on Adopter’s general implementation of the HDCP Specification Rev 2.0 in a model or product line that is not Compliant or otherwise based on Adopter’s breach of the Agreement and Addendum (except that if Adopter has caused any of the circumstances described in Sections 7.2.1 or 7.2.2 with respect to any KSV or

Receiver ID, such KSV or Receiver ID, as applicable, may be Revoked) or (ii) in products or devices where the general security of HDCP has been compromised by third parties (other than where the Revocation Criteria have been satisfied).”

- (viii) Sections 7, 7.1, 7.2, 7.2.1, 7.2.2, 7.2.3 and 7.3 shall be modified to add reference to “Receiver ID” where applicable.

Part 6. Section 9 shall be amended as follows:

- (i) Section 9.1.4 (“Breach not capable of cure”) shall be modified as follows:

“In the event of a material breach that is not capable of cure under the provisions of Section 9.1.3, or in the event that a party has committed a third material breach whether or not it has cured prior breaches for which it has received notice pursuant to 9.1.3, the party not in breach may, by giving written notice of termination to the breaching party, terminate this Agreement and Addendum. Such termination shall be effective upon receipt of such notice of termination.”

- (ii) Section 9.3 shall be modified as follows:

The following sections shall survive termination of this Agreement: 2.2, 2.3, 2.4, 2.6, 2.7, 2.8, 3.2, 6, 8, 9.2, 10, 11, 12 and this Section 9.3.

Part 7. Section 10 shall be amended as follows:

- (i) Section 10.2 shall be modified to add Receiver IDs, Device Secret Keys, Source Keys, Public Key Certificate.

Part 8. Exhibit A, Section 1 shall be amended as follows:

- (i) Section 1 shall be renamed as the following:
“Annual Fee, Device Key Fees, Source Key Fees, Receiver ID Key Fees”

- (ii) Section 1.2 shall be amended to add the following:

Device Key Fees are for secret keys for products implementing HDCP Specification Rev 2.0 only.

Source Key Fees. In addition to the Annual Fee, Adopter shall pay the following Source Key Fees annually depending on quantity of HDCP 2.0 Source Devices and HDCP 2.0 Repeaters produced:

US \$20,000	For quantities over 1M per year
US \$10,000	Up to 1M per year
US \$5,000	Up to 100K per year
US \$2000	Up to 10K per year
US \$1000	Up to 1K per year
US \$500	Up to 100 per year

Receiver ID Key Sets. In addition to Annual Fees, Adopter shall pay the following Receiver ID Key Fees for each order of Receiver ID Key Sets:

<u>Number of Receiver ID Key Sets</u>	<u>Fee per Order</u>
1,000,000	US \$10000
100,000	US \$5000
10,000	US \$2000

A new Section 5 shall be added to Exhibit A:

Section 5 – Records

5.1 The requirements of this Section 5 are to be construed as amending Section 3.2 of the HDCP Adopter Agreement.

5.2 Records must be maintained for all Keyed Licensed Components and Deactivated Keyed Licensed Components distributed to Fellow Adopters.

5.3 Records must include: name of entity receiving Keyed Licensed Components or Deactivated Keyed Licensed Components and specific Receiver ID or similar means to effectively trace specific Receiver ID for each Keyed Licensed Component.

5.4 The records must be maintained for a period of three (3) years and Adopter shall provide such records within a commercially reasonable period of time upon DCP's request.

5.5 Failure to maintain such records will constitute a material breach of the Agreement.

A new Section 6 shall be added to Exhibit A as follows:

Section 6: Distribution of Keyed Licensed Components and Deactivated Keyed Licensed Components.

6.1 The requirements of this Section 6 are to be construed as amending Section 3.2 of the HDCP Adopter Agreement.

6.2: Distribution.

6.2.1. Keyed Licensed Components may only be sold or otherwise furnished to Fellow Adopters subject to this Addendum. Under no circumstances may Keyed Licensed Components be sold or otherwise furnished to HDCP Associates or others.

6.2.2. Deactivated Keyed Licensed Components may be distributed to in accordance with Section 3.2 of the Adopter Agreement.

6.2.3 No Keyed Licensed Components may be distributed to an HDCP Associate or other non-adopter. No Licensed Components may be distributed to Resellers who are licensed under the HDCP Reseller Associate Agreement under any circumstance. In either case such distribution would constitute a material breach of the Agreement.

A new Section 7 will be added to Exhibit A:

7. Definitions. All of the definitions from the Agreement and this Addendum are incorporated herein by reference.

Part 9. Exhibit C shall be amended as follows:

- (i) Section 3.3.1 of Exhibit C shall be deleted in its entirety and replaced with the following:

3.3.1 Audiovisual Content

3.3.1.1 A Presentation Device shall not permit the output of Audiovisual Content to digital outputs, except, if the Presentation Device is also a Repeater, as expressly provided in Section 5.3 of these Compliance Rules. Notwithstanding the foregoing, Presentation Devices may output the audio

portions of Decrypted HDCP Content that is Audiovisual Content in (a) analog form 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; or (b) digital form in either compressed audio format or in Linear PCM format and Licensed Products that are not an internal peripheral or software component of a Computer Product shall ensure that the SCMS information corresponding to “Copy-never” is used for outputs that utilize SCMS

- (ii) Section 3.5 of Exhibit C shall be deleted in its entirety and replaced with the following:

“Device Key Sets” Each Presentation Function shall use a unique KSV and a unique Device Key Set. Notwithstanding the above, each HDCP 2.0 Presentation Device shall use a Device Secret Key corresponding to a unique Receiver ID as required by the HDCP Specification Rev 2.0.

- (iii) Section 4.2 of Exhibit C shall be deleted in its entirety and replaced with the following:

Additional Requirements. Adopter is advised that the license agreements relating to other content protection technologies or conditional access systems that act as an immediate upstream content control function to a Source Function and require HDCP Protected Outputs may require the delivery of SRMs to Source Functions or the delivery of Receiver IDs from Source Functions to such immediate upstream content control function, and the protected communication of information from Source Functions in order to ensure the effective protection of Audiovisual Content. If requested by the immediate upstream content control function, the Source Function shall pass the Receiver IDs of all downstream Presentation Devices and Repeaters to such upstream content control function. In any event, the HDCP Source Function is required by these

Compliance Rules of Adopter’s HDCP Adopter Agreement to make available to the immediate upstream content control function information that indicates whether the Source Function is fully engaged and able to deliver protected Audiovisual Content, which means (a) HDCP encryption is operational on all applicable HDCP protected outputs, (b) there are no Presentation Devices or Repeaters on an HDCP protected output whose KSV or Receiver ID is in the current revocation list, and (c) processing of valid received SRMs, if any, has occurred, as defined in the Specification.

- (iv) Section 4.4 shall be added as follows:

“Global Constants” Notwithstanding section 4.3, HDCP 2.0 Source Devices shall require the use of Global Constants.

- (v) Section 5.3 (“ Digital Outputs”) shall be deleted in its entirety and replaced by the following:

“A Repeater shall not permit the output of Decrypted HDCP Content to digital outputs, except when output through HDCP Protected Interface in accordance with this Agreement, the Addendum, if applicable, and the HDCP Specification. “

- (vi) Section 5.6 shall be added as follows:

“Notwithstanding section 5.5, each Repeater Device, for a receiver function or Source Function that implements HDCP Specification Rev. 2.0, shall use a unique Receiver ID and unique Device Key Set as appropriate.”

Part 10. Exhibit D shall be deleted in its entirety and replaced with the following.

ROBUSTNESS RULES

1 Construction. Licensed Products as shipped shall comply with the Compliance Rules and shall be manufactured in a manner clearly designed to effectively frustrate attempts to (a) modify such Licensed Products or the performance of such Licensed Products to defeat the content protection requirements of the HDCP Specification Rev 2.0 and the Compliance Rules (b) discover or reveal Device Secret Keys and other values identified as Confidentiality Required in Appendix A to the HDCP Specification Rev 2.0, and (c) cause such products to use values identified in Appendix A to the HDCP Specification Rev 2.0 as Integrity Required after unauthorized modification of such values occurs. Licensed Products shall not use Confidentiality Required or Integrity Required values for purposes other than those defined in the HDCP Specification.

2 Defeating Functions. Licensed Products shall not include: (a) switches, buttons, jumpers or software equivalents thereof, (b) specific traces (electrical connections) that can be cut, (c) special functions or modes of operation (including service menus and remote-control functions), or (d) active JTAG ports, active emulator interfaces or active test points to probe security functions, in each case by which the content protection requirements of the HDCP Specification Rev 2.0 and the Compliance Rules can be defeated, or by which Decrypted HDCP Content in such Licensed Products can be exposed to unauthorized interception, redistribution or copying.

3 Data Paths. Decrypted HDCP Content shall not be available on outputs other than those specified in the Compliance Rules.

4 Method of Making Functions Robust. Licensed Products shall use at least the following techniques in a manner that is clearly designed to effectively frustrate attempts to defeat the content protection requirements of the HDCP Specification Rev 2.0 and Compliance Rules.

4.1 Content Protection Requirements other than Core Functions. Any portion of the Licensed Product that implements any of the content protection requirements of the HDCP Specification Rev 2.0 and the Compliance Rules, other than Core Functions, shall include all of the characteristics set forth in Sections 1 through 3 of these Robustness Rules. Such implementations shall:

4.1.1 Comply with Section 1 above by a reasonable method including but not limited to: encryption and/or execution of a portion of the implementation in ring zero or supervisor mode (i.e., in kernel mode) 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; and

4.1.2 Be designed so as to perform integrity checking or otherwise ensure integrity of its component parts such that unauthorized modifications will be expected to result in a failure of the implementation to provide the authorized 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 Section 1 of these Robustness Rules. This provision requires at a minimum the use of “signed code” and may also include a robust means of runtime integrity checking operating throughout the code. For the purpose of this provision, “signed code” means a method of achieving trusted distribution of Software by using public key cryptography, keyed hash, or other means at least as effective, to form a digital signature over Software such that its authenticity and integrity can be verified.

4.2 Core Functions. Any portion of the Licensed Product that implements any of the Core Functions shall include all of the characteristics set forth in Sections 1 through 3 of these Robustness Rules. Such portions shall be implemented in a “Hardened Execution Environment” meaning they shall:

4.2.1 Comply with Section 1 above by employing Hardware-enforced mechanisms, where such enforcement is rooted in a Hardware Root of Trust, that (a) protect Decrypted HDCP Content, Device Secret Keys and values identified as Confidentiality Required in Appendix A to the HDCP Specification, where such values are also identified under Core Functions, against unauthorized exposure (such as encrypting Decrypted HDCP Content on any User-Accessible Bus, encrypting Decrypted HDCP Content, Device Secret Keys and such Confidentiality Required values in system memory, isolating memory in which Decrypted HDCP Content, Device Secret Keys or such Confidentiality Required values reside through access controls, using Device Secret Keys and such Confidentiality Required values only inside a secure processor, and embedding Device Secret Keys in silicon circuitry or firmware that is protected from being read, to the level specified in Section 4.3), and (b) effectively and uniquely associate the RSA private key, that is applicable to the HDCP 2.0 Presentation Device or function used to receive and decrypt HDCP Content in HDCP 2.0

Repeater Device, with that device (such as by encrypting the values using a key that is unique to a single device).

4.2.2 Comply with Sections 1 through 3 of these Robustness Rules by protecting against unauthorized modifications of portions of the Licensed Product implementing Core Functions by checking integrity or otherwise ensuring integrity of such portions through the implementation of Hardware-enforced mechanisms, where such enforcement is rooted in a Hardware Root of Trust. Such mechanisms shall include a Secure Load of such portions and shall be designed such that unauthorized modifications made at any time will be expected to result in a failure of the implementation to perform the Core Functions and attempts to remove, replace, or reprogram Hardware elements of a Presentation Device or Repeater in a way that would compromise the content protection requirements of the HDCP Specification Rev 2.0 and the Compliance Rules in Licensed Products would pose a serious risk of rendering the Licensed Product unable to receive, decrypt or decode HDCP Content. By way of example, checking a signature on updateable firmware within a secure boot loader may be appropriate for this means.

4.3 Level of Protection – Core Functions. The Core Functions of HDCP shall be implemented in a reasonable method so that they:

4.3.1 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, file editors, 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, decompilers, integrated development environments and similar software development products ("Specialized Tools"), or software tools such as disassemblers, loaders, patchers or any other software tools, techniques or methods not described in Widely Available Tools and Specialized Tools (e.g., the software equivalent of in-circuit emulators, software tools used for reverse engineering and penetration testing), as would be used primarily by persons of

professional skill and training (“Professional Software Tools”), other than Circumvention Devices, and

4.3.2 Can only with difficulty be defeated or circumvented using professional tools or equipment, such as logic analyzers, PCB rework stations, oscilloscopes, electromagnetic probes, chip disassembly systems, or in-circuit emulators or any other tools, equipment, methods, or techniques not described in Section 4.3.1 (“Professional Hardware Tools) such as would be used primarily by persons of professional skill and training, but not including Professional Hardware Tools that are made available only on the basis of a non-disclosure agreement or Circumvention Devices.

4.4 Level of Protection – Content Protection Requirements other than Core Functions.

The content protection requirements, other than Core Functions, of the HDCP Specification Rev 2.0 and the Compliance Rules shall be implemented in a reasonable method so that such implementations:

4.4.1 cannot be defeated or circumvented merely by Widely Available Tools or Specialized Tools, as those capitalized terms are defined in Section 4.3.1 but not including Circumvention Devices; and

4.4.2 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 4.4.1 of these Robustness Rules such as would be used primarily by persons of professional skill and training, but not including either Professional Tools Or Equipment that are made available on the basis of a non-disclosure agreement or Circumvention Devices.

4.5 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. Notwithstanding the foregoing, in the event that Adopter manufactures, distributes or sells Robust Inactive Products, Adopter shall have the right to continue to manufacture, distribute and sell the same version of such Robust Inactive Products for a period of up to two (2) years following such Notice, or such longer period as Licensor may, in extraordinary circumstances, approve in writing, provided that Adopter shall stop any further activation of the HDCP Functions in any such Robust Inactive Products no later than eighteen (18) months after the Notice. Where an Adopter can demonstrate that the cost of removing HDCP from a Robust Inactive Product would be substantial, Licensor shall not unreasonably decline written approval of an “extraordinary circumstance,” provided that such continued shipment without further activation would not affect the security of HDCP and there have not been repeated breaches of the Agreement by the Adopter.

4.6 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 Licensor, one or more Eligible Content Participant(s) may request that Adopter submit promptly to an independent expert (acceptable to Adopter, which acceptance shall not be unreasonably withheld) detailed information necessary to an understanding of such product’s implementation of the HDCP Specification, Compliance Rules, and Robustness Rules such as would be sufficient to determine whether such product so complies with these Robustness Rules. Adopter’s participation in such inspection and provision of such information is voluntary; no adverse inference may be drawn from Adopter’s refusal to participate in such inspection or provide such information. 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 such Eligible Content Participant(s), Adopter and such expert, such agreement not to be unreasonably withheld, that also provides protections for Confidential Information and Highly Confidential Information that are no less stringent than those provided for in this Agreement. Such examination and report shall be conducted at the sole expense of the Eligible Content Participant(s) that requested such inspection. Nothing in this Section 4.6 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. Once this provision has been invoked by any Eligible Content Participant(s) with respect to any hardware model or software version, it may not be invoked again by the same or other Eligible Content Participants with respect to the same hardware model or software version of a Licensed Product, provided that the right to request inspection shall include the right to request re-inspection of the implementation of such model or version if it has been revised in an effort to cure any alleged failure of compliance. Nothing in this Section 4.6 shall grant a license or permission for any party to decompile or disassemble software code in Adopter's products.

4.7 Licensed Source Components. All terms and conditions of these Robustness Rules applicable to Licensed Products shall also apply with respect to Licensed Source Components. In addition, each Licensed Source Component shall be designed to ensure that when the HDCP functions that implement any of the content protection requirements of the HDCP Specification Rev 2.0 and the Compliance Rules are distributed in a Licensed Product among such Licensed Source Component and one or more other Licensed Source Components, including, without limitation, among integrated circuits, software modules, or a combination thereof, such functions shall be designed and associated and otherwise integrated with each other such that the confidentiality of Device Keys and other Highly Confidential Information, and the integrity of values identified as "requiring integrity" in Appendix A to the HDCP Specification, are maintained in accordance with the standard of protection set out in, as applicable, Section 4.3 through 4.4 of these Robustness Rules.

This Addendum may be executed in any number of counterparts, each of which shall be deemed an original and together shall constitute one instrument. The parties hereto acknowledge and agree that such counterparts may be executed by signatures sent by facsimile transmissions.