MANAGED COPY AMENDMENT

Submitted October 16, 2007
Proposed for CPAC consideration on November 7, 2007

Insert the following definitions (as underlined) into Section I. Definitions:

"Approved Managed Copy Technology" shall have the meaning set forth in Section 6.2.9.3(2).

"Content Provider Default URL" shall mean the information that can be used to redirect a Managed Copy Service in order to obtain authorization from the Content Provider to make a Managed Copy.

"Content Provider Identifier" shall mean a unique identifier associated with each Content Provider. The master list of Content Provider Identifiers shall be published by the Licensor.

"DVD Fingerprint" shall mean the value unique to each DVD Disc Title generated independently by the Content Provider and the Identification Module, set forth in Section 6.2.9.3(1).

"Identification Module" shall mean a product capable of performing Managed Copy DVD Disc Title Identification pursuant to the process described in Section 6.2.9.3(3).

"Identification Request" shall mean the information, set forth in Section 6.2.9.3(3)(a), provided by the Identification Module to an Identification Service.

"Identification Response" shall mean the information, set forth in Section 6.2.9.3(3)(b), provided by an Identification Service to the Identification Module.

"Identification Service" shall mean the system operated by Licensor and/or pursuant to a license from the Licensor that identifies a DVD Disc Title during Managed Copy DVD Disc Title Identification. Licensor is the default entity authorized to direct and operate an Identification Service. Licensor shall license the identification functionality to other entities to operate additional Identification Services. Every Identification Service must contain all of the same information and incorporate at least equivalent identification functionality as the Identification Service directed by Licensor.

"Integrated Product" shall mean a combination of any one or more of a DVD Player, DVD Drive, Descrambler, Authenticator, CSS Decryption Module or Identification Module with any other product, device or component into a single integrated unit that permits, or that is designed for further integration into a product that permits, the transmission of unscrambled content in digital or analog format to any internal or external output or connection, provided that use of the term "Integrated Product" does not affect the obligations or provisions pertaining to any separately defined DVD Product. For purposes of this definition, a “single integrated unit” shall include a group of two or more otherwise disaggregated products that are controlled by a central processor and that are manufactured with the intent that such products be used together as a unit. Integrated Products may include by way of example and not of limitation: (i) integration of DVD Drives or CSS Decryption Modules with or into computer systems; and (ii) integration of DVD Drives or DVD Players with or into television receivers and videocassette recorders.

“Managed Copy” shall mean the process by which a CSS Decryption Module or DVD Player outputs decrypted CSS Data associated with a DVD Disc Title, where the DVD Disc Title has been authorized on terms and conditions for such process by the Content Provider having the right to provide such authorization to a Managed Copy Technology.

“Managed Copy DVD Disc Title Identification” shall mean the process, set forth in Section 6.2.9.3(3), by which an Identification Module sends an Identification Request and, if the DVD Disc Title is authorized for Managed Copy, receives an Identification Response.

“Managed Copy Service” shall mean the system that handles the Managed Copy transaction.

“Managed Copy Technology” shall mean a digital rights management system authorized by the Content Provider specified in the Identification Response to encrypt and store an authorized DVD Disc Title.

“Session ID” shall mean a statistically unique and random number generated by the Identification Module for each Identification Request as described more fully in Section 6.2.9.3(3)(a).

Insert into Section 6.2.9.3 as follows:

> 6.2.9.3. Managed Copy of CSS Data. Notwithstanding any other provision of the CSS Specifications, Licensees may implement the Managed Copy functionality set forth in this Section 6.2.9.3. Whenever a Content Provider has elected to make available for Managed Copy one or more of its DVD Disc Titles, such Managed Copy functionality must implement controls over the number of recordings made from a single DVD Disc to a limit authorized by such Content Provider, when such Content Provider has, with the DVD Disc, its associated packaging, or some other means, provided a means for

uniquely identifying the DVD Disc. The Managed Copy Service must implement a means for tracking the number of copies or recordings from such DVD Disc when so required by the Content Provider. Managed Copy functionality shall be permitted only so long as such action does not affect the integrity or security of CSS protection provided to any other CSS Data. In no event shall any DVD Player or Integrated Product enable Managed Copy of any DVD Disc if such DVD Player or Integrated Product fails to meet all of the requirements and obligations of the CSS Specifications.

(1) DVD Fingerprint. A "DVD Fingerprint" is the value unique to each DVD Disc Title and is generated by applying the SHA-1 algorithm to the data in the largest VTS .IFO file on a DVD Disc (i.e. the file named VTS_01_0.IFO if the first VTS .IFO file is the largest on the DVD Disc) followed by the data in the Video Manager Information .IFO file (VIDEO_TS.IFO). If such .IFO data is longer than 32768 bytes (16 sectors), only the first 32768 bytes of each IFO file are used, for a maximum of 65536 bytes. The resulting hash value is the DVD Fingerprint and is 160 bits long. The DVD Fingerprint ("Fd") is represented in the expression below:

> Fd = SHA-1(VTS_xx_0.IFO || VIDEO_TS.IFO)
>
> where
>
> xx is the index number of the largest VTS IFO file
>
> (Note: SHA-1 refers to the 1994 revision of the Secure Hash Algorithm (SHA) developed by the National Institute for Standards and Technology (NIST), as specified in the ANSI X9.30 (part 2) standard).

(2) Making Available DVD Disc Titles for Managed Copy. No Managed Copy will be permitted for any DVD Disc Titles until and unless two Managed Copy Technologies are approved by CPAC ("Approved Managed Copy Technologies") whereby the license and technical specifications for at least one such Approved Managed Copy Technology allows for its implementation in non-user-programmable, hardware-based consumer electronics devices. No Managed Copy Technology will become an Approved Managed Copy Technology unless a license to such Managed Copy Technology is offered to all CSS Licensees on a reasonable and non-discriminatory basis. Licensor shall inform all CSS Licensees of the Managed Copy obligations set forth in this Section 6.2.9.3, including, without limitation, Content Providers' obligation to provide the necessary information set forth in Section 6.2.9.3(2)(c) if they elect to make available any DVD Disc Title for Managed Copy. Content Providers shall have no obligation to make available for Managed Copy any present or future DVD Disc Title, but if any Content Provider elects to make available for Managed Copy any such DVD Disc Title, then the following provisions shall apply:

(a) The terms and conditions of the transaction shall be determined solely by each Content Provider;

(b) each Content Provider shall either (i) enter into a Managed Copy Service agreement with at least one Managed Copy Service provider, and/or (ii) offer directly a Managed Copy Service, provided, however, that nothing herein shall be construed to compel any Content Provider to enter into any agreement with any Managed Copy Service; and

(c) each Content Provider must convey to the Licensor (i) the associated DVD Fingerprint, (b) the Content Provider Identifier; and the (iii) the Content Provider Default URL. (This information submitted by the Content Provider will be used in the Identification Response pursuant to Section 6.2.9.3(3)(c)).

(3) Managed Copy DVD Disc Title Identification. Decrypted CSS Data of a specific DVD Disc Title available for Managed Copy shall be permitted to be output from a CSS Decryption Module or DVD Player to a Managed Copy Technology only in accordance with and upon successful completion of the following steps:

(a) For each Managed Copy authorization request, the Identification Module shall generate an Identification Request for the DVD Disc Title present in the DVD disc tray that includes the DVD Fingerprint and the Session ID for which a Managed Copy is being requested. The Identification Module shall then provide the Identification Request to an Identification Service.

(b) Upon receipt of an Identification Request, an Identification Service shall use the provided DVD Fingerprint to determine whether a Managed Copy is available for the DVD Disc Title that is in the DVD disc tray. The Identification Service shall then generate an Identification Response containing the Session ID and the DVD Fingerprint, both retrieved from the Identification Request. If the Identification Service determines that the DVD Disc Title is available for Managed Copy, the Identification Service shall send an Identification Response that includes the Content Provider Identifier and the Content Provider Default URL, both associated with the DVD Disc Title. If the Identification Service determines that the DVD Disc Title is not available for Managed Copy (e.g., the DVD Fingerprint does not match to any DVD Fingerprint in the database of DVD Disc Titles available for Managed Copy) then the Identification Service shall not include a Content Provider Identifier in the Identification Response.

(c) The Identification Service shall sign the Identification Response using a 1024-bit RSASSA-PSS digital signature using the MGF1 as the mask generation function on the concatenation of the DVD Fingerprint, and Session ID and the Content Provider Identifier, if available, using the private key of a private key/public key pair which has been obtained from the Licensor.

(Note: RSASSA-PSS refers to the Public Key Cryptography Standard (PKCS) #1 version 2.1 Probabilistic Signature Scheme (PSS) digital signature developed by RSA Laboratories).

(d) Upon the completion of signing the Identification Response pursuant to 6.2.9.3(3)(c), the Identification Service shall provide the signed Identification Response to the Identification Module.

(4) Managed Copy.

(a) Receipt of Identification Response. Upon the Identification Module's receipt of an Identification Response generated and received pursuant to Sections 6.2.9.3(3)(b)-(d), the Identification Module must confirm that the Identification Response is validly signed by verifying that the certificate of the Identification Request was properly signed by the Licensor. If the Identification Module is unable to validate the signature, the Managed Copy process will terminate immediately.

(b) Session ID. Upon positive confirmation of the signature pursuant to Section 6.2.9.3(4)(a), the Identification Module shall validate that the Session ID is the same as that passed to the Identification Service in the Identification Request. If the Session ID does not match the Session ID of the Identification Request, the Managed Copy process will terminate immediately.

(c) Content Provider Identification. The Identification Module will check the Identification Response for a Content Provider Identifier.

(i) Content Provider Identifier Not Present. If a Content Provider Identifier is not present in that Identification Response, that Managed Copy process will terminate immediately.

(ii) Content Provider Identifier Present. If a Content Provider Identifier is present in the Identification Response, the CSS Decryption Module or DVD Player shall output decrypted CSS Data associated with the DVD Disc Title for which a Managed Copy is being requested to the Managed Copy Technology to the extent permitted by the Content Provider specified by the Content Provider Identifier. After receiving decrypted CSS Data associated with the identified DVD Disc Title, the Managed Copy Technology must encrypt the decrypted CSS Data and apply the intended usage rules to such encrypted data. The Managed Copy shall be completed in compliance with the robustness requirements set forth in Section 6.2.9.3(5) below. If the Managed Copy Service provider is not authorized by the Content Provider to make a Managed Copy of such DVD Disc Title, such Managed Copy Service provider may use the Content Provider Default URL to obtain authorization from the Content Provider to facilitate the completion of the Managed Copy.

(iii) If the DVD Disc is removed from the DVD disc tray at any time during a Managed Copy session associated with a Session ID, the Managed Copy process with respect to such DVD Disc will terminate immediately.

(5) Managed Copy DVD Disc Title Identification and Managed Copy Robustness.

(a) The requirements and procedures applicable to Authenticators and Descramblers under Section 6.2.4 shall also apply to Software implementations of Managed Copy DVD Disc Title Identification and Managed Copy, including the output of the decrypted CSS Data from the CSS Decryption Module to the Managed Copy Technology.

(b) The requirements applicable to Authenticators and Descramblers under Section 6.2.5 shall also apply to Hardware implementations of Managed Copy DVD Disc Title Identification and Managed Copy functions of the CSS Decryption Module or DVD Player, including the output of the decrypted CSS Data from the DVD Player to the Managed Copy Technology.

(c) The requirements applicable to CSS Keys under Section 6.2.4.1(2) and DVD Keys in Section 6.2.5.1(2) shall also apply to confidential keys used in the process of Managed Copy DVD Disc Title Identification and Managed Copy functions of the CSS Decryption Module or DVD Player.

(d) The confidentiality requirements under Section 6.2.5.3 applicable to integrated circuit specifications relating to CSS shall also apply to integrated circuit specifications for Managed Copy DVD Disc Title Identification and Managed Copy functions of the CSS Decryption Module or DVD Player.

The foregoing action by DVD Players and Integrated Products set forth in this Section 6.2.9.3 shall be permitted only so long as such action does not affect the integrity or security of CSS provided to any other CSS Data.

(6) No Other Playable Copies.

Other than as set forth in this Section 6.2.9.3, DVD Products shall not be designed to make or direct the making of a playable, persistent copy of CSS Data.