



DEG REPORT

CONTENT PROTECTION & DRM, A glossary

October 2004 – DRM-001-04

Introduction

The key purpose of content protection and DRM is to create secure content distribution methods that permit an increased choice of offerings of content to consumers at varying times and price points. In order to achieve this purpose, technologies are needed to maintain the distinctions between these choices (e.g., prevent the copying of video-on-demand that is purchased by the consumer as a one time “view only” experience). No one technology achieves all of the protection functions required. Rather, a series of technologies is needed to: (i) securely manage the content at its source and during delivery to the consumer, (ii) securely manage the content as it moves within the consumer’s authorized home environment, and (iii) securely manage recordings when the consumer is authorized to copy the content.

The remainder of this document consists of three sections. The **Definitions** section introduces general terminology frequently used in relation to content protection technologies. **Technologies Deployed Today** provides an overview of technologies incorporated in products that are actually on the market today. **Emerging Technologies** provides an overview of technologies in various states of introduction.

Definitions

CONDITIONAL ACCESS

Direct broadcast satellite and cable operators use Conditional Access technologies to protect some or all of their signals. These systems are encryption based and often use a smartcard in the receiver to determine that the user is a legitimate subscriber.

DRM (DIGITAL RIGHTS MANAGEMENT)

The term DRM usually refers to a category of systems aimed at protecting content that can be downloaded to a PC or consumer device from an on-line service. The protection of the content is realized by encryption. The attached

usage rights define what the consumer can actually do with the content. Most DRM systems support a variety of business-based usage models through the use of flexible rights expression languages.

ENCRYPTION

Encryption can be considered as putting a lock on the content. The content is transformed by applying the encryption algorithm in conjunction with the encryption key. The encrypted content cannot be viewed or listened to unless it is decrypted, for which the corresponding encryption key is required. In most cryptographic systems the encryption and decryption key is the same, and the key management protocol defines the scheme that is used to securely transfer the key to the intended receiver of the encrypted content. In public key systems the encryption and decryption key are not the same, and the knowledge of one does not allow the other to be computed.

Manufacturers of consumer products that require decryption keys in order to access the content in the clear obtain those keys under voluntary license from the licensors of the encryption technology. The license agreement conditions include compliance rules that determine how the product must protect the content once it has been decrypted and robustness rules, which determine the level of resistance to alteration that the product implementation must exhibit. These voluntary, licensed-based technologies need no government mandate or regulation for implementation.

FORENSIC TRACKING

Forensic Tracking does not protect the content per se but it provides the means to determine the origin when content appears in unauthorized places. This is done by hiding identification information in the content itself in such a way that it is not perceptible when it is played back. Watermarking technology is often used as the embedding method.

WATERMARK

Watermarking refers to the type of technology used to embed information, including content usage rules, securely into a video or audio signal. Watermarks are designed to be imperceptible by the audience, and they travel with the content even over analog interfaces. Watermarks are directly embedded into the actual content itself and therefore are difficult to remove. Furthermore, watermarks survive and “travel with” content as it is converted from digital to analog form or is re-digitized from analog back into digital. While watermark technology permits content protection rules to “stay with” content, watermarks do not, in and of themselves, protect the content. Watermarking is simply a technology for signaling information and usage rights to devices that may receive the content. Protection is only achieved if devices and products are designed to inspect content for the watermark and respond appropriately to rules carried by the watermark. While an obligation to inspect and respond appropriately to a watermark can be imposed through a voluntary license (e.g., CPRM licensed digital audio recorders must under the terms of the license inspect for and

respond to an audio watermark on incoming analog content), widespread and uniform watermark detection requires a government mandate. This is because as long as plenty of analog content is available in the clear, manufacturers of digital recorders need not take a license for a voluntary content protection technology and may simply rely upon the “analog hole” to permit their customers to make digital recordings. Effectively closing this analog hole will therefore require some sort of government mandate.

Technologies Deployed Today

APS (ANALOG PROTECTION SYSTEM)

This is a system designed to offer protection for content in the analog form, typically used to prevent analog tape recording by VHS consumer recorders. Examples of APS are Macrovision and Dwight Cavendish technologies, both of which interfere with the quality of recordings made to VHS tape.

CGMS-A (CONTENT GENERATION MANAGEMENT SYSTEM-ANALOG)

CGMS-A signals usage rights in analog video content, such as Copy Never, Copy Once, etc. CGMS-A is a data flag consisting of two bits encoded in the vertical blanking interval of the analog video signal. CGMS-A is a widely implemented standard and its use is mandated under a number of content protection technology licenses, including CSS and DTCP. CGMS-A is relatively easily removed and, in some cases video processing equipment will remove the CGMS-A signaling, either by accident or as part of normal operation. Like watermarks or other data flags, CGMS-A does not in and of itself protect content; rather it simply delivers usage rights information that must be detected and properly responded to by downstream devices. CGMS-A will likely serve as a central technology for closing the analog hole, although additional measures, such as Veil marking, may be required to compensate for the low robustness of the CGMS-A signal.

Usage: Required to be applied on analog output signals by various technology licenses including CSS, and DTCP.

CPPM (CONTENT PROTECTION FOR PRERECORDED MEDIA)

Developed by the 4C companies, IBM, Intel, Matsushita and Toshiba, this technology is intended to protect digital audio content on prerecorded optical media against unauthorized further copying or redistribution. It achieves these protections by encrypting the content and cryptographically binding it to the physical media. CPPM is currently used to protect DVD-Audio.

Usage: Required by DVD-Audio technology license

CPRM (CONTENT PROTECTION FOR RECORDABLE MEDIA)

Developed by the 4C companies, IBM, Intel, Matsushita and Toshiba, this technology protects recordings made on digital recordable media (such as recordable DVD discs and flash memory cards) against unauthorized further copying or redistribution. It achieves these protections by encrypting the

recording and cryptographically binding it to the secure, unique identity required to be included on CPRM-compliant physical media. This means that such recordings can then only be played back on devices licensed to decrypt the recordings, and that no 'drag and drop' bit for bit copies are playable. Under the terms of the license such playback devices must follow rules to ensure that the recorded content cannot be subject to further copying (unless authorized) or re-distribution.

Usage: Required by the DTCP technology license

CSS (CONTENT SCRAMBLE SYSTEM)

This is the encryption system used on DVDs to protect video content. It is the industry standard: all DVD players, DVD drives and playback software in PCs, and DVD discs containing commercial pre-recorded video content use CSS. CSS is licensed from the DVD Copy Control Association. Under the terms of the license, DVD players, DVD drives and playback software must protect the video content once it has been decrypted. Although the CSS encryption system was "hacked" a few years ago, DVD players and discs continue to follow the protection rules as set forth in the CSS license. The hack is only relevant in the PC context. In that context, it is only when a user downloads or purchases an illegal software program containing the hack (such as DeCSS), which enables the circumvention of the CSS protection, that the user can gain access to an unprotected digital version of the content on the DVD without any of the content usage obligations of the CSS license. Absent use of such an illicit program, DVD drives and playback software continue to function normally so as to protect DVD-Audiovisual content in accordance with the CSS license.

Usage: Required in order to play back CSS encrypted DVD-Video.

D-VHS (DIGITAL-VHS)

JVC's digital VCR format incorporates an encryption based content protection mechanism.

Usage: Required by the D-VHS technology license.

DTCP (DIGITAL TRANSMISSION CONTENT PROTECTION)

DTCP was developed by the 5C companies, Sony, Matsushita, Intel, Toshiba, and Hitachi. The DTCP technology is a secure transmission technology and protects compressed digital content as it travels among digital devices in a consumer's home network after the consumer has initially received the content. DTCP is based on encryption and authentication technology that can be used to link digital devices such as a set top box, digital television set, digital recorder and personal computer in a protected manner. Digital content that is protected by DTCP will only be accessible by devices that follow the content protection rules specified by the DTCP license. For example, a digital recorder that receives DTCP protected content will not record the content if it is marked as "Copy Never." Furthermore, no device that receives DTCP protected content is permitted to redistribute that content over the Internet. DTCP technology is

available for secure transmission over IEEE 1394 interfaces, IP protocol and MOST.

Usage: Permitted by the DVCCA license as an allowed secure digital output from DVD players.

HDCP (HIGH-BANDWIDTH DIGITAL CONTENT PROTECTION)

Developed by Intel, this technology, like DTCP, is a secure transmission technology that protects digital content in the consumer's home after the content has been initially received. HDCP protects uncompressed digital content being transmitted from an STB or other source device for display on televisions and monitors using the DVI protocol. It is different from DTCP because it is not a technology for transmitting content among various devices in the home, but rather is targeted for use with display devices. HDCP is based on encryption and authentication technology that protects the de-compressed digital content when it flows from a source device, such as a set top box or personal computer, to a display device such as a digital television or monitor. In part the HDCP system relies on the bulky nature of uncompressed video and the sensitivity of the high speed DVI link to prevent copying.

Usage: Permitted by the DVCCA as an allowed secure digital output from DVD players

MACROVISION APS (ANALOG PROTECTION SYSTEM)

APS protects content from unauthorized analog recording on VHS recorders. Unlike watermarks or flags, they do not require an affirmative detection or response on the part of the recorders. Rather, the technologies simply exploit fundamental design features of the VHS recorders to cause distortions in the recorded copy that spoil the viewing experience when the recording is played back. The Digital Millennium Copyright Act of 1998 requires that VHS recorders distributed in the U.S. may not be re-designed to avoid the operation of this protection technology. Although Macrovision dominates this field there is an alternative technology called Dwight Cavendish. This is not yet widely deployed.

Usage: Required by several content protection technology licenses including CSS, DTCP and CPRM to protect analog video outputs.

MICROSOFT'S WINDOWS MEDIA DRM

A DRM system that is built into Microsoft's Windows Media Player software found on almost all Windows based PCs. It is also implemented in several consumer electronics devices.

Usage: Widely used to provide secure internet delivery of audio and audiovisual content over the internet to personal computers.

REAL NETWORKS' HELIX DRM

A DRM system aimed at secure delivery of movies and video over the Internet to personal computers. After Microsoft's DRM, the REAL DRM is the second most widely deployed system.

Usage: Similar to Widows DRM

TIVO GUARD

TivoGuard is an encryption based content protection technology that Tivo applies to its Personal Video Recorders.

Usage: TivoGuard is applied exclusively on Tivo products

VERANCE

Verance is a company fielding an audio watermark technology which has been selected by the 4C companies to protect DVD-Audio.

Usage: Detection of the Verance watermark is required by the CPRM license.

Emerging Technologies

AACS (ADVANCED ACCESS CONTENT SYSTEM)

A next generation content protection technology designed to create a seamless, robust and interoperable environment for the distribution and use of next-generation content. AACS will develop, promote and license technologies designed to enhance digital entertainment experiences for consumers by introducing exciting, flexible new entertainment options for consumers in stand alone, networked home and portable environments. AACS is format-neutral and designed for next-generation optical media formats for use with PCs and other consumer electronics devices. Founders are Warner Bros., Walt Disney, IBM, Intel, Microsoft, Matsushita, Toshiba, and Sony.

BROADCAST FLAG

Digital over-the-air broadcast is delivered in the clear and no protection technology, such as encryption, is applied. Thus, no technical obstacle exists to prevent unauthorized digital redistribution of such broadcasts, particularly over the Internet. To address this problem, a broadcast flag has been developed. The presence of the flag indicates that the broadcast content is prohibited for digital redistribution outside the home/personal environment. If the flag is not present it means that such digital redistribution is not prohibited.

The flag itself does not protect the content; rather the flag must be detected and appropriately responded to by devices that receive digital broadcasts. The FCC (Federal Communications Commission) has initiated a rulemaking proceeding to select which technologies digital broadcast receivers will use to protect content in response to the broadcast flag. The scope of such a response would consist of ensuring that:

(i) digital interfaces between devices are protected by means of encryption, and

(ii) any consumer recordings made of the content are similarly protected by encryption. The flag would not limit the number of digital copies that a consumer could make of the broadcast content and analog copying (i.e. VHS copying) would be unaffected.

Currently the FCC is in its first round of certifications for protection technologies. The submitted technologies include CPRM, DTCP, OMG, Tivo, VCPS, and Windows Media-DRM.

Enforcement: The FCC has issued a Report and Order that requires that any Digital TV receiver sold after July 2005 responds to the broadcast flag when present in over the air TV programming.

CGMS-A+RC

Copy Generation Management System – Analog + Redistribution Control is an extension of CGMS-A that adds a flag to reflect the requirement that the content may not be redistributed over the Internet.

MAGICGATE (MG)

MagicGate or MG-R is a security system that may be used in conjunction with various recording media. It has multiple components as follows;

Secure transfer of content to recording device (using a secure authenticated channel)

Binding of recording so that only the media which made the recording can be used to play it back (prevents copies being made of the recording)

Encrypts recordings with 128 bit AES

Limits the use of digital outputs in MG-R playback devices to approved digital outputs.

Provides a mechanism to revoke software decoders deemed to have been compromised.

Currently there are implementations of MG-R available with MemoryStick and MiniDisc devices that are designed for making secure recordings.

OMA

OMA (Open Mobile Alliance) is an open standard for a DRM system initially aimed at protecting mobile data services on cellular phones. In OMA over 300 companies representing mobile operators, device and network suppliers, information technology companies, and content providers work together.

SMARTRIGHT

SmartRight is designed to prevent content from indiscriminate, unauthorized redistribution, including over the Internet, outside a secure, authorized domain of devices known as a Personal Private Network (“PPN”). SmartRight was originally developed by Thomson whose partners now include Pioneer and ST Micro.

VEIL

Veil (Video Encode Invisible Light) is a technology that places a signal in the active picture area of the video by making imperceptible adjustments to the luminance of the horizontal lines of the picture. Veil technology could serve as a

rights assertion mark for analog originated content and for digital content when converted into analog form. The use of Veil as an effective rights assertion mark requires that analog hole legislation is passed requiring detection of the Veil in analog content immediately prior to digitization.

VCPS

VCPS (Video Content Protection System) is an encryption-based technology developed by Philips and HP that prohibits the indiscriminate redistribution of digital broadcast content that has been recorded onto removable media, specifically DVD in both DVD+RW and DVD+R formats.