

# CONTENT PROTECTION OF ONLINE MUSIC SERVICES

David Konetski, Technology Strategist



Dell recently announced the Dell™ Digital Jukebox (Dell DJ™) music player and a partnership with Musicmatch to provide Dell customers with an easy-to-use and legal way to download and manage digital music from the Internet. The Dell music service reflects a

pivotal industry transition from MP3-based services with no content protection to services that include content protection coupled with lenient usage rights.

In this white paper we focus on content protection systems. While largely transparent to end users, a robust content protection system and the underlying usage rights it confers play a key role in the current upsurge of music services. The choice of content protection systems also has implications for compatibility and interoperability.

## Background

Recent years have seen a steady increase in the popularity of compressed digital music that is delivered over the Internet. A growing amount of music is available, as well as increased capabilities in computer platforms to generate and play the music. Paralleling this trend is the growth of content protection systems designed to protect the owners, creators, and distributors of digital content. At their best, such systems should provide robust protection, reasonable use of the music, and be virtually transparent to the user.

These content protection systems are enabling a new generation of secure online music services, including the new Dell Music Store, Apple iTunes, BuyMusic.com, Rhapsody, and the relaunched Napster. These music download services offer the ability to buy single tracks or entire albums. They also offer more lenient usage rights. For example, the Dell Music Store offers unlimited transfer rights to portable music players, unlimited burning to CDs and DVDs, and the ability to copy to several PCs. This is a key development that is expected to fuel strong growth in music services.

## Why do we need content protection for digital content?

New content protection systems have been developed because digital music, audio, and video content is so much easier to copy and distribute than traditional analog recordings. There are inherent barriers to mass reproduction and distribution of analog recordings:

- Long reproduction time
- Degraded quality on later generations of copies
- One-to-one distribution on physical media

Analog reproduction requires more time than digital reproduction because it is usually performed in real time. For example, it requires approximately one hour to reproduce a typical analog album and even longer to create a custom mix. In addition, the quality of subsequent generations of analog copies degrades. In contrast, digital content can be reproduced almost instantaneously, regardless of play sequence, and the quality of copies are identical to the quality of the source.

Analog content must be recorded on a physical medium (such as cassette or reel-to-reel tape) before it can be distributed. This distribution is typically one-to-one (that is, one copy is distributed to one recipient). Digital distribution does not require this type of physical medium. A digital file can be distributed quickly over a computer network to thousands of recipients. Distribution of entertainment content is made even easier by digital compression algorithms such as MP3 that reduce the size of the copy, but maintain similar quality.

## What is content protection?

The terms “content protection,” “encryption,” and “digital rights management” (DRM) are often used interchangeably, but refer to different solutions. Content protection is a general term that refers to software or hardware systems that safeguard content. These systems can employ encryption, format manipulation, or other types of “obfuscation” mechanisms for tamper resistance to protect the content. Content encryption uses a cipher to encode the content so that it is ren-

dered useless unless unencrypted using the same or a related cipher. Encryption protects digital content from being useful if it is intercepted, stolen, or illegally copied. DRM defines and enforces the rules by which the content may be used. These rules reflect the business model that governs the content. For example, a piece of digital music may carry the following rights:

- For a purchase price of \$.50, the music may be played only on a PC.
- For a purchase price of \$.75, the music may be placed on a PC and burned once to a CD.
- For a purchase price of \$1.00, the music may be used with no restrictions.

Encryption is used in all three of these DRM scenarios to protect the content while being distributed and to prevent its being copied illegally. The DRM scheme can be thought of as a wrapper around the encrypted content that determines how the content may be used.

Many different rights can be associated with content: number of plays, period of time that access is allowed, number of times the content can be burned to optical media such as CD or DVD, whether the content can be transported to a portable player, and expiration date. DRM systems can even request contact information before content is accessed.

Content protection can apply to many different content types, distribution mediums, and protection schemes. In this white paper, we focus on the most popular digital content protection systems used by music services.

## **Content Protection Standards and Solutions**

Content protection solutions for the new digital music services are still in their infancy. Industry standardization has not matured; therefore, all schemes implemented today are proprietary. There has been work on content protection standards, but none of these initiatives have resulted in a definitive direction for the industry. Current efforts that may yield such standards are:

- MPEG-4 content protection proposal by the Internet Streaming Media Alliance (ISMA) and the Digital Home Working Group
- Digital Transport Copy Protection (DTCP) use over IP networks

- Pending FCC rulemaking on Digital Cable Compatibility that is likely to impact the digital content protection landscape

The music recording labels have evaluated and implemented content protection schemes based on two major criteria: the robustness of the solution and its ease of implementation and use. There are two main content protection systems being deployed in the latest generation of music services, one for the PC platform and the other by Apple Computer. The Apple iTunes Music Store uses the Advanced Audio Codec (AAC) file format and the FairPlay content protection system. Music that is distributed in this format requires the Apple iTunes jukebox software and can be transferred only to the Apple iPod portable device.

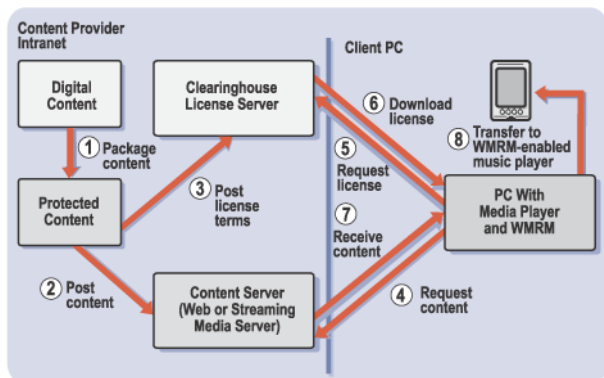
The remaining major services target the PC platform with either the Real Networks Helix solution or, more commonly, the Microsoft® Windows® Media Rights Management (WMM) solution. This white paper focuses on WMM. Most major music services offer tracks in the Windows Media Audio (WMA) file format with WMM content protection. These tracks can be played back using most major PC media jukeboxes, including the Windows Media Player (bundled with current Windows operating systems) and the Dell jukebox by Musicmatch. These tracks can also be transferred to any WMM-secure portable device, including the Dell Digital Jukebox and Dell Axim™. Other secure portable players specifically tested with online music download services can be found at <http://windows-media.com/9series/Personalization/CoolDevices.asp>.

The following section discusses WMM in more depth.

## **Windows Media Rights Management**

Microsoft provides WMM to content owners and developers in a free software development kit (SDK) that contains ready-to-use code for packaging digital content. This capability includes encryption, distribution, and establishing a "license server" that implements and enforces the DRM rules. End users acquire and play the WMM-protected digital music on a PC using a WMM-compliant music jukebox such as Windows Media® Player, or the Dell jukebox by Musicmatch, which have integrated license acquisition and protected content playback capabilities. The content can also be

transferred to and played on a WORM-enabled portable music player. Figure 1 shows the content flow in a WORM system.



**Figure 1. Windows Media Rights Manager Flow**

### Packaging and Posting Digital Music to Internet

As shown in the left half of Figure 1, raw digital content must first be “packaged” in WORM before it is stored for distribution. The WORM packaging process encrypts the content and adds the DRM rules required to use the content. In order to do so, it first divides the content into smaller data units and encrypts each unit using the WORM encryption algorithm, originally published in Eurocrypt '98. Each data unit is encrypted using an encryption key that is unique to the content being packaged. The key is generated from a content ID and “key seed” provided by the content owner. The encrypted content is then stored on a Web or streaming-media server and is ready for distribution.

To use the stored content, it must be unencrypted. Windows Media Rights license services (shown as the “Clearinghouse License Server” in Figure 1) provides unencryption information, known as the content license. To generate the license, these services first allow the content owner to specify the usage rights associated with the content. This information is then combined with the encryption key. The resulting package is also encrypted and packaged as the content license.

### Acquiring and Playing Digital Music

Shown in the right half of Figure 1, an end user must obtain a content license before playing protected music. The license request may be initiated when the user pays for or attempts to download or play the content. License acquisition may be transparent to the user or the user may be presented with a link to acquire the license. Once the business terms for the content have been satisfied (for example, by purchasing the content), a license clearing house approves the transaction and a license server downloads the license to the user's computer. There are various business models for license distribution. Some require payment of the content before granting the license. Others involve free content in which the license transfer process is more transparent to the user. In all cases, the user is authenticated, and the license is transferred and stored separately from the content on the user's computer. WORM content protection then manages unencryption and secure playback.

### Compatibility and Interoperability

As the online music industry continues to grow, interoperability and compatibility are key concerns. Currently, WMA/WORM is the predominant file format and content protection system for the PC platform. In the future, an industry standard for music download interoperability may be adopted. A challenge for the industry during this transition is to ensure that today's hardware is compatible with future content and that the evolution of content protection does not make content distribution and enjoyment difficult. Standardization will provide the key to digital content distribution success.

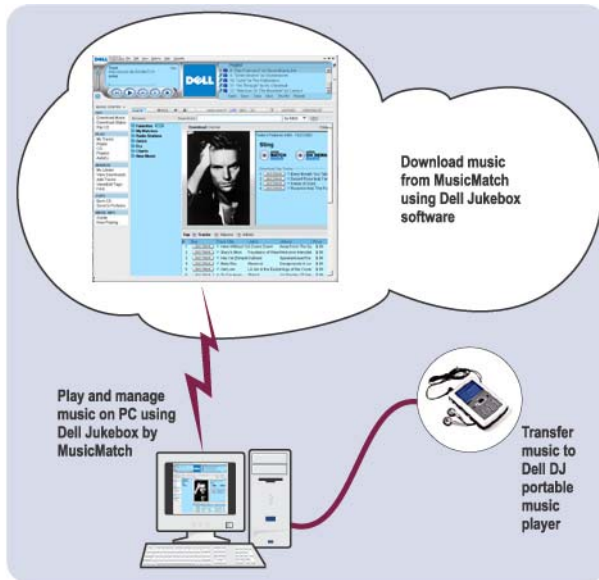
### Dell Music Service

The new Dell music offering is composed of the Dell jukebox software powered by Musicmatch and the Dell DJ music player. As shown in Figure 2, the Dell jukebox by MusicMatch software runs on a PC and provides a simple graphical interface to manage the connection between the PC and the Dell DJ. The jukebox also provides access to the Musicmatch no-subscription track download service. All music tracks have consistent usage rights:

- Unlimited transfer rights to portable music players
- Unlimited burning of single tracks to CDs and DVDs

- Ability to download to up to three PCs

The Dell DJ is a portable digital music player with a 15- or 20-MB hard drive and WORM-protected playback. Together they provide a seamless and compelling digital content solution. For more information on this offering, see [www.dell4me.com/music](http://www.dell4me.com/music).



**Figure 2. Dell Music Service**

Information in this document is subject to change without notice.  
© 2003 Dell Inc. All rights reserved.

Trademarks used in this text: *Dell*, the *DELL* logo, and *Dell DJ* are trademarks of Dell Inc.; *Microsoft*, *Windows*, and *Windows Media* are registered trademarks of Microsoft Corporation. Other trademarks and trade names may be used in this document to refer to either the entities claiming the marks and names or their products. Dell Inc. disclaims any proprietary interest in trademarks and trade names other than its own.