

How does DRM Work?

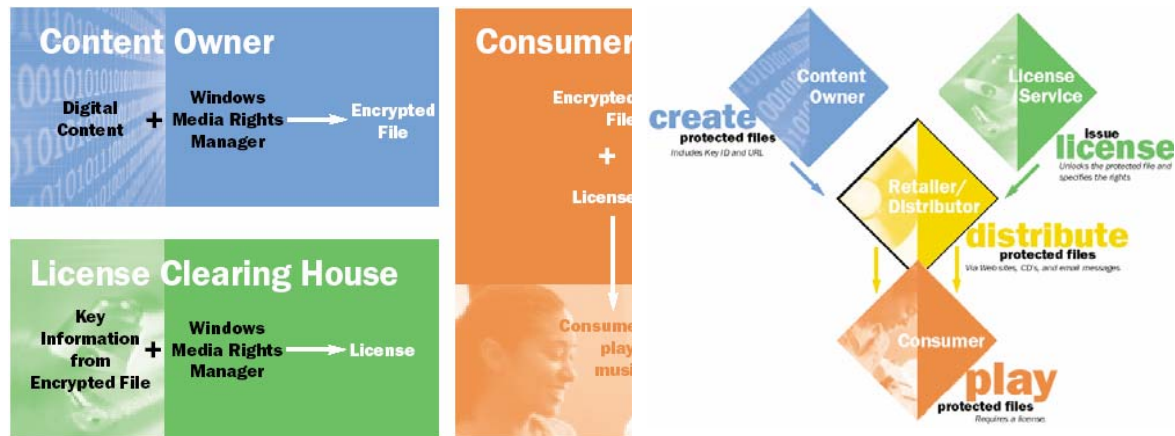


Figure 1: Entities and Processes involved in media Distribution and Licensing

- The content owner first encrypts the files. The content owner uses Digital Rights Manager System to encrypt a digital media file with a key. To create a key, the DRM System creates and uses both a license key seed and a key ID. The license key seed is a secret value known only to the content owner and the license-clearing house. The key ID is created for each media file, and is included in the header of the encrypted file. A URL, from where the license can be acquired, is also included in the file header. The resulting protected media file can be played by any application designed to work with the DRM system to request, acquire and use licenses for real time decryption and media playback.
- The retailer/web site distributes the encrypted files. The content owner can distribute their encrypted media files to retailers, who in turn can distribute or sell them to consumers in a variety of ways. For example, retailers might sell songs through their online store, give them away on promotional CDs, or stream video files from a media server running Windows® 2000 or Unix and many of its variants.
- The consumer acquires the content from the retailer or distributor and then attempts to play the encrypted file. Because the file is protected, the consumer must have a license that contains the key to unlock the content. If a valid license already exists on the consumer's computer, the file plays as expected. If a valid license is not found, a license request is made to the licensing-clearing house using the license acquisition URL.
- When a license-clearing house needs to issue a license for an encrypted file, it can recreate a key by retrieving the key ID from the file. The clearing house will download the key within an encrypted license to the consumer's computer. The license itself contains the rights, or business rules, that govern the use of the media file. Content owners can determine rules for the file such as:
 - The number of times it can be played, from one-time use to unlimited play
 - Whether it can be burned on a CD-RW
 - The security level of the software required to play it
 - License start and expiration dates
 - The portable device or media on which it can be played or transferred

With the flexible nature of today's DRM systems, content owners can deliver the licenses to consumers in different ways and at different times. For example, licenses can be delivered before or after the consumer has tried to play the media file, and licenses can be delivered with or without consumer interaction.

- After the consumer acquires the license, he or she can play the media file according to the rights specified by the content owner. Licenses are bound to the machine that received them and cannot be shared. So if a consumer copies an encrypted media file for a friend, the friend must first acquire his or her own license to play it.