Global Information Assurance Certification Paper

Protecting Today's Digital Media with Windows Media Rights Manager

by

Cheryl L. Jones

for

SANS GSEC
Security Essentials

August 1, 2003

Cheryl L. Jones
Security Essentials Certification (GSEC) version 1.4b option 1
Protecting Today's Digital Media with Windows Media Rights Manager
1 August 2003

Abstract-
In recent years, just about everything has become accessible over the Internet. Users can now purchase numerous items without leaving the comforts of their own home or office. The Internet has also become a place where users can find media such as movies, music, books, and software and obtain them without paying for them, which results in loss of revenue to media companies. Many companies that distribute these types of media have been looking for a way to prevent this activity. For example, Sony, the world's second largest consumer electronics maker, has blamed digital piracy for eroding profit at its music business, which posted a loss of $160 million in the three months to June 30, 2002. *(1)*

This paper will attempt to explain how the Windows Media Rights Manager, a component within the Windows Digital Rights Management technology, protects digital media.

Overview-

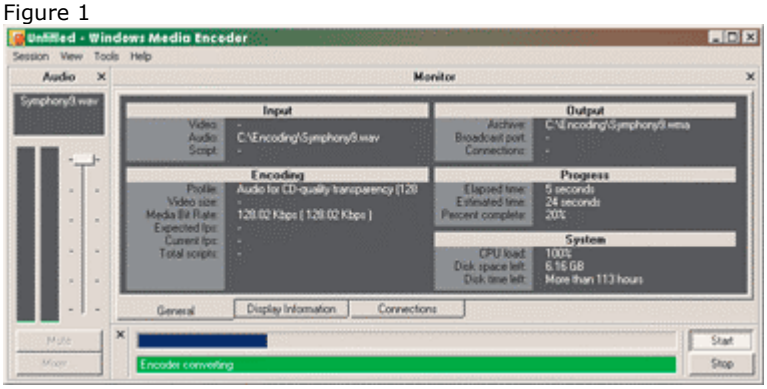
The Digital Rights Management (DRM) system, on an industry level, has been around for some time now. These systems are used to protect high-value digital assets and control distribution of unauthorized content. Instead of the consumer buying the content, they purchase a license that will grant certain rights.

Windows Digital Rights Management utilizes the standard industry DRM framework via the Windows Media Rights Manager to facilitate the packaging, distribution, license generation and issuance, and deployment of digital media content.

Packaging-

The first step to protecting digital content using Windows Media Rights Manager is through the creation and packaging of the digital media files. File creation is done through the Windows Media Encoder application. Figure 1, below shows what the Encoder interface looks like:

Figure 1



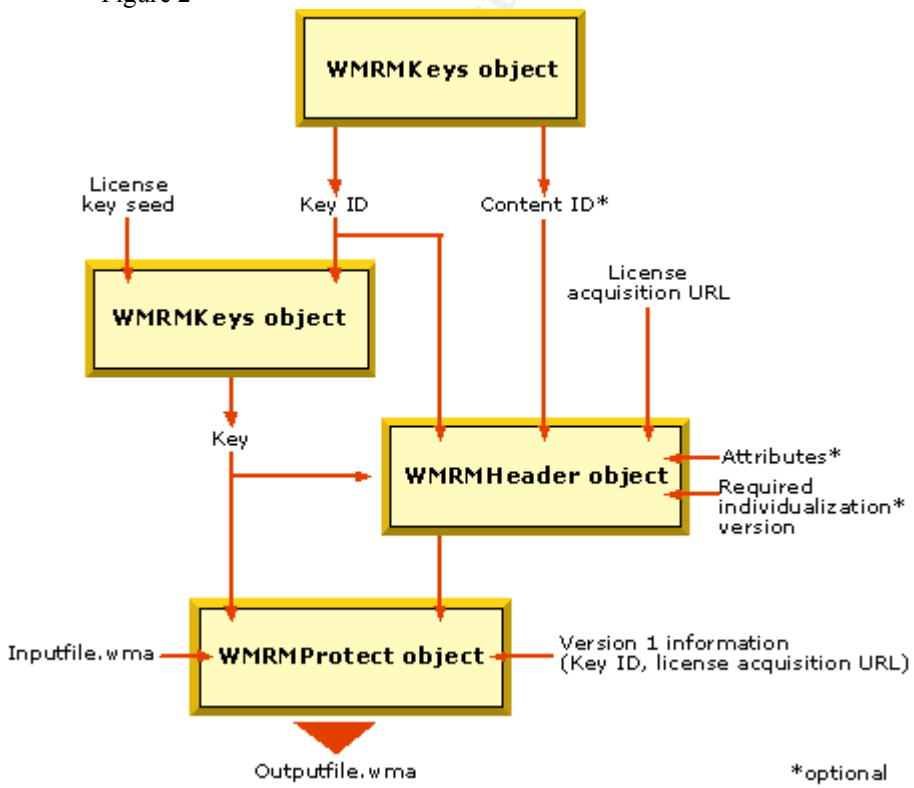
(2)

The encoder adds information about the file such as the name of the artist, title, and copyright that will appear in the player. Once the file is created, it goes through the packaging process.

The file is encrypted using asymmetric encryption mechanisms. The process is very fast, over 540,000 bytes per second. (2) Once this is complete the file is locked with a key.

Below, Figure 2, a diagram from Microsoft, shows the flow of packaging a file. I would like to go into detail and explain the process and how it works.

Figure 2



(5) http://www.ebizis.com/techcenter/media.html

The WMRMKeys object generates the key ID. It is generated separately per piece of content. When a separate key is used per file, it definitely increases

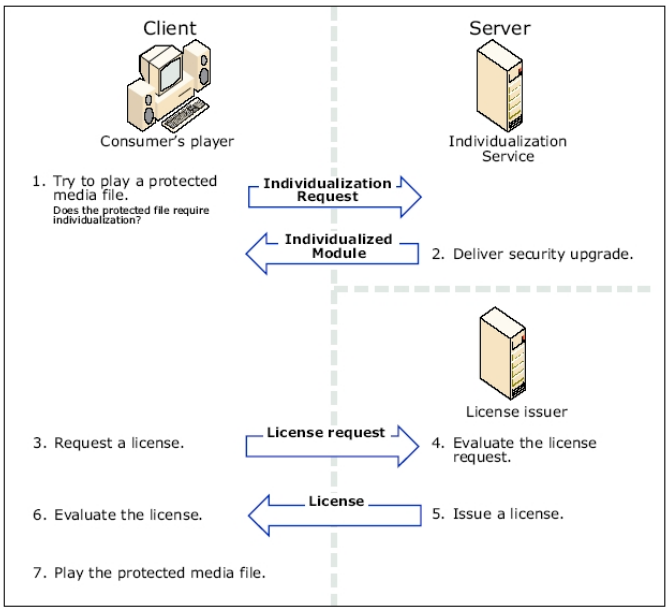
the level of security and is more flexible. However, there are instances when one key can be used for more than one file. Files that share the key also share the license. So a single license, for instance, can be used for each tune on a CD. The WMRMKeys object can issue the content ID as well. The content ID identifies each packaged file. It is optional, but highly recommended.

The use of the key ID and the license key seed, along with the WMRMKeys object generates the key. The license key seed can be used by an organization to package all of their files. So, if you have 500 songs, then 500 key ids will need to be created by the record label, then the license key is used to generate 500 keys. This can be done using the GenerateSeed option within the WMRMKeys object.

Now let's examine the WMRMHeader object. This object along with the key, key ID, content ID, and license acquisition URL comprise the content header. The content header contains information about the packaged file. The license acquisition URL is the web site address at the beginning of the license acquisition process. The Windows Media player will open this URL, when a license isn't found for a file. The page would then let the consumer know that a valid license is needed and how much it would cost to obtain one, etc.

Also included in the WMRMHeader object are attributes and required individualization version. Attributes add special information to the packaged file such as the artist, title, content owner, distributor, and rating. This information is extremely important when more than one person manages the file, for communication and tracking purposes. Using an individualized version number means the consumer would have to use an individualized player application with a minimum version. If the user agrees, the individualization process begins. If not, then the files cannot be played. Below, figure 3 illustrates how this process works:

Figure 3



(3) http://www.microsoft.com/windows/windowsmedia/wm7/WMRM_security.pdf

The individualization feature makes the distinction between a media application on one computer and another application residing on the same computer. The end result of this means that if an individualized application is hacked, then just that version will be affected. This helps in decreasing the possibility of global attacks to the application, thus making attacks more difficult and costly to the attacker.

Content owners use the individualization feature to require consumers to use individualized software to play their packaged files and as a step in the installation process. The player sends a request to the Microsoft Individualization Service on the Internet. This service generates a DLL that is digitally signed and then bound to the requesting client computer by the hardware ID. This whole process is untraceable and doesn't affect or violate the consumer's privacy.

Next in the process of packaging a file, the WMRMHeader object signs the content header. After this is completed, the WMRMHeader object Header property is used and set to the Header property in the WMRMProtect object. The WMRMProtect object includes the inputfile.wma (the Windows Media file that needs to be packaged), key, and content header to produce the packaged media file.

Distribution-

The packaged files are distributed to consumers in a number of ways. They can be streamed from a media or Web server for download, protected file sharing between consumers, or distributed via email or CD. The digital license contains the decrypted content keys and the usage rules that specify how the content is going to be used, such as pay-per-view or rental, etc. There are three types of distribution that I wish to elaborate on: streaming, superdistribution, and subscription.

Streaming digital media is an option for making content available to consumers without copies of it being given away. The consumer must play the content from the vendor's website. The packaged content is completely secure when it is streamed. A license is needed to play the saved stream. Unprotected files can be saved and shared with others. There are four steps to the streaming process:

1) Have the license delivered before the file is streamed.
2) Grant the rights to play the file.
3) Limit the times a file can be played.
4) Specify a license acquisition URL, set whether or not local copies of the media will be played. *(2)*

Superdistribution is when file sharing is done between consumers; this increases the distribution and sales of the packaged file. The receiver of the packaged files has to acquire a license of their own before the files can be

played. The new receivers of the file will have contact with the initial retailer so that they get credit for the sale. This is done through specifying attributes to the content header. Attributes can be created in the packaging process, as discussed earlier, or it can be done after the retailer receives files from the content owner.

The subscription service provides the consumer access to a large amount of digital media content. There is usually a monthly fee, and a license granted for a monthly time period to be able to play or download unlimited music, etc. The consumer must renew their subscription to receive a new license, which is done through the license acquisition page.

License Generation and Issuance-

Licenses are different on every device and cannot be shared, copied, or used on different devices. Windows Media files need to have a license and a key to unlock the content before they can be played. Licenses add more security to the Windows Media Rights Manager system. All of the licenses that are generated are done so through the use of the Windows Media License Service. This service is used by the person or organization that is issuing the license. It can be done through a license clearinghouse, for instance. The clearinghouse handles all of the financial transactions for issuing the digital license to the consumer, providing royalty fees to the content provider and distribution fees to the distributor. The clearinghouse logs how the consumer uses the license.

License Generation-

In order to generate a license, the issuer uses the license key seed with the key ID within the Windows Media file to generate a key, and specify the rights.

Below are some of the rights specified by Microsoft:

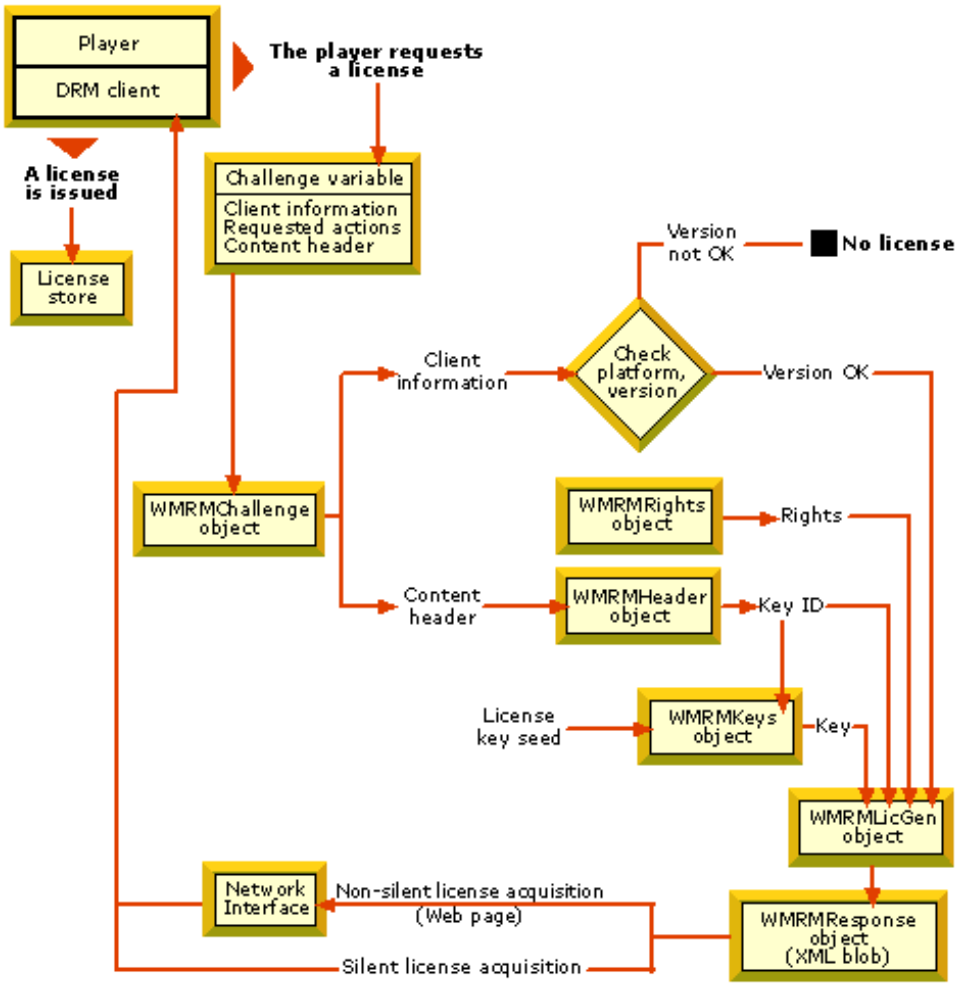
- AllowPlayonPC- allows the consumers to play the WMA file on the computer. This right is set by default.
- PlayCount-specifies the number of times the consumer is allowed to play the WMA file. By default this right is not set; unlimited plays are allowed.
- AllowBurnToCD- specifies if the consumer can copy the WMA file to a CD. By default this right is set.
- BurnToCDCount- specifies the number of times the consumer can burn the WMA file to a CD. By default this right is not set; unlimited copying is allowed.
- AllowBackupRestore- allows the consumer to manage licenses by backing up and restoring them. Consumers can restore licenses on the same computer or to different computers. By default this right is set.

(5) http://www.ebizis.com/techcenter/media.html

Issuing a License-

Figure 5 shows the license issuing process:

Figure 5



(5) http://www.ebizis.com/techcenter/media.html

The player makes a request for a license using the challenge variable, which includes the client information, requested actions, and content header. The request is received and put into a WMRMChallenge object. The WMRM rights object then generates the rights that will need to be included in the license. The content header information is included in the WMRMHeader object to retrieve the key ID. The key ID and the license key seed are put into the WMRMKeys object to generate the key. The client information, rights, key ID, and the key are included in the WMRMLicGen object to generate the license. The individualization version number and platform information are also determined using the WMRMLicGen object. If the version number and platform are okay, the process will continue. If not, then a license isn't issued. The license is put into the WMRMResponse object to generate a response that is sent back to the consumer and put into the license store on the consumer's computer.
There are five ways to issue a license:

1) Issuing the license before the file is played
2) Issuing by player request

3) Issuing silently
4) Issuing non silently
5) Issuing a license based on platform and the consumer's player *(16)*

Issuing a license before the Windows Media file is played, or predelivery, means that after the consumer selects a song from a website and pays, a license is issued and the consumer is able to download the song. It can be played immediately because the license is already on the consumer's computer. There are not additional steps for the consumer to acquire a license.

Predelivered licenses offer the consumer more for their money when purchasing a song; they also get a license that includes another song that the company is trying to promote. The promotional song can be set to play a certain number of times before a screen comes up giving the consumer information on purchasing it.

There are two methods that can be used to predeliver licenses from a content owner prospective. One method is through the use of the RMGetLicense.GetlicenseFromURL, where a license request is made using HTTP. The Windows Media License Service will return a license to the consumer. This works best when silent license delivery is used and enables the content owner to specify a URL from which to issue a license. The other method is through the use of RMGetLicense.GetSystemInfo, is used when a hidden form in a Web page sends client information to the Windows Media License Service. The license service then returns a license and a new Web page to the consumer. *(2)*

Issuing a license by player request is when the consumer doesn't have a license to play the file and the player uses the license acquisition URL stored in the Windows Media file to request a license. The Windows Media License Service from the URL issues a license so that the consumer can play the file.

Issuing a license silently is when a player requests a license without the consumer noticing it. The consumer's PC will check to see if a license exists to play the media. The only thing that the consumer needs to do is provide credit card information. Generally the license service has all of the required information. The consumer may have registered or paid a subscription fee. The purpose is to eliminate any further input of the consumer and to hide the license acquisition process.

Issuing a license non silently means that the license can be issued after the consumer provides personal information or submits payment. There can also be a web page that displays the license information to the consumer.

Licenses that are based on the consumer's player and platform provide greater security depending on either the player or the platform. Different license or none at all can be issued, depending on the player and/or platform.

The method that is used should be very flexible for instances where a consumers player can't do silent license acquisition. The consumer can acquire packaged files from friends. If the license is predelivered, it must be able to handle the license acquisition that is started by the friend's player. When the

friend tries to play the file without a license, the license acquisition URL opens. This page handles any situation in which a license is needed.

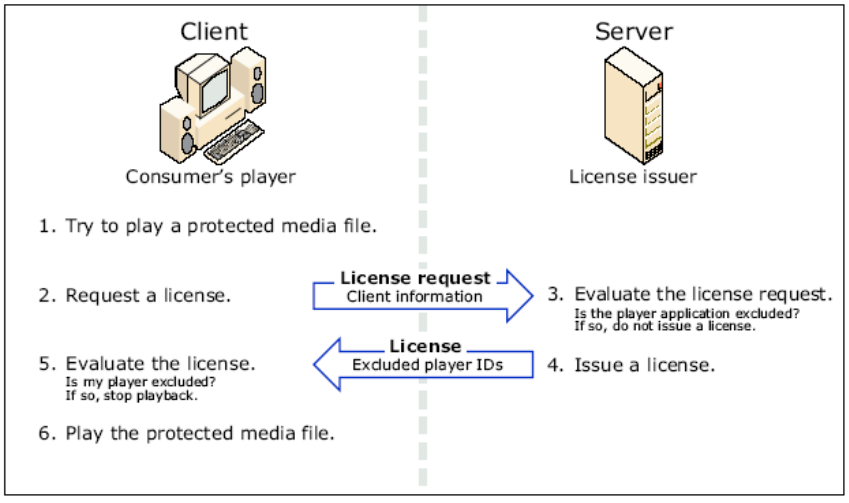
Every license that is issued by a server that is running Windows Media Rights Manager comes with what is called a revocation list that contains all of the application certificates of player applications that are broken or corrupted. When the trusted certificates are compromised they are rendered invalid if more content is licensed. Revocation prevents global attacks on a DRM system. It limits the opportunity for an attacker by forcing the upgrade of compromised software to play new digital media.

Revocation can mean revoking an individual DRM security component or refusing license issuance to numerous applications. It can be granular or very broad. Content Revocation, Player Application Exclusion, and Protected Content Manager Exclusion are three methods that use revocation to make it so that the user cannot playback the content file.

Content Revocation gives the content providers the control to revoke specific content from the user's machine by issuing a license with a content revocation key. This is a public key that is used to sign the header of the content. If the content provider wants to revoke the content, all they have to do is add the public key to the revocation list that is included in the license, which is done through the license server.

Player Application Exclusion allows a license issuer to prevent specific player applications from playing certain packaged files. This is enforced on the client by the license or through the license acquisition process. When the license is generated for a packaged file, the ID that needs to be excluded from the player application is specified by the license issuer. This results in the consumer being unable to play the packaged file on the excluded player application. Figure 6 shows how the player application exclusion process works:

Figure 6



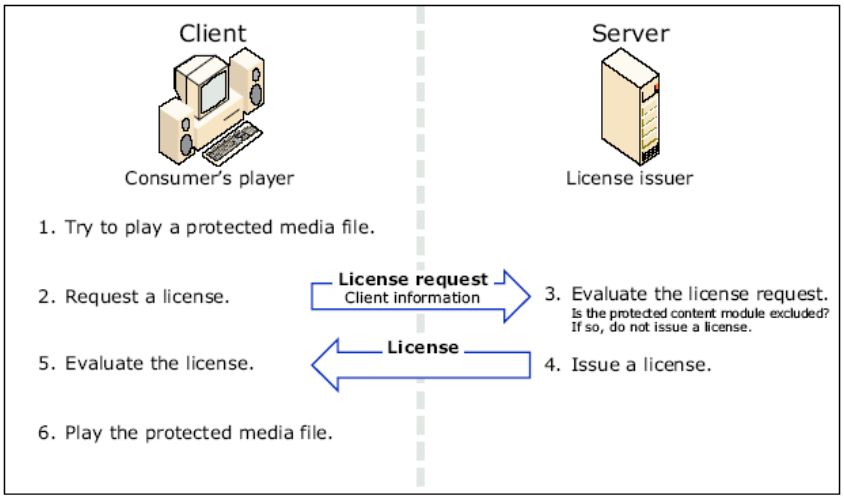
(3) http://www.microsoft.com/windows/windowsmedia/wm7/WMRM_security.pdf

If a license is predelivered, then the request for a license and the evaluation of the license are not done. Only the license is used to prevent an excluded player from accessing the protected file. A consumer could use one

player to make a request and receive a license, then later use a different player to play the protected file. Evaluating the license provides the certainty that an excluded player can't play the protected file, even after the license acquisition process.

A Protected Content Manager is included on players that support packaged files. This manager enforces the rights contained in the licenses. The exclusion feature allows the identification of player applications that are based on a compromised Protected Content Manager. This is enforced by the license server. License issuers must obtain and update the Protected Content Manager exclusion list that is published by Microsoft. The end result is that if a license issuer receives a request from a player that is based on an excluded Protected Content Manager, the issuer can refuse to issue the license. The issuer can instead display a link for downloading a new player or for upgrading. Figure 10 shows how the protected content manager process works:

Figure 10

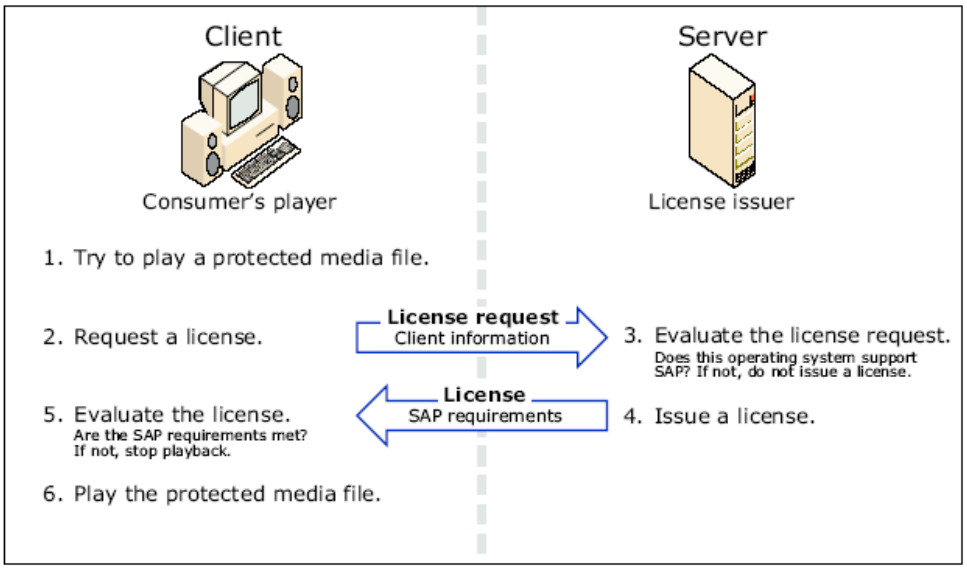


(3) http://www.microsoft.com/windows/windowsmedia/wm7/WMRM_security.pdf

Secure Audio Path, a feature of Windows ME and XP that ensures that protected files remain protected until the audio reaches the output device, provides security between the protected content module of the player software and the protected content module of the operating system kernel. It reduces attacks based on false plug-ins because these components only have access to encrypted data. It prevents digital copying, the ability to set security levels for sound cards, and isn't restricted to the Windows Media Player. The license issuer can usually determine before issuing a license if the consumer is using the operating system that supports Secure Audio Path. It can only be used for protected files. It doesn't affect unprotected digital media files such as MP3s. Secure Audio Path must be set as a requirement in the licenses for the protected files. Some features that can be enabled are requiring components that receive the decrypted audio signal to be certified by Windows Hardware Quality labs, requiring a specific security level of audio drivers, and disabling digital output of the device (the content will not play the protected media if the consumer's computer doesn't meet the requirement).

Figure 11 shows how Secure Audio Path is enforced on the client through a license:

Figure 11



(3) http://www.microsoft.com/windows/windowsmedia/wm7/WMRM_security.pdf

Figure 11 shows the license request, which contains client information. If the operating system doesn't support SAP then no license is issued. If it does, then the process continues. The requirements are evaluated in step 5, if they aren't met then playback stops, before the content can be played.

What happens if a computer is damaged or replaced during the licensing process? Licenses can be reissued to the customer from the specified website. For each license transaction, the userID and keyID, as well as rights, for the license that was issued must be recorded for the same type of license to be reissued.

Playing the Windows Media file-

The consumer's media player must support Windows Media Rights Manager, in order to play the digital media file. Then it can be played according to the rules and rights included in the license. If the consumer sends the file to someone else, they must obtain their own license to play the file. This license scheme ensures that the packaged digital media file can only be played by the computer that has granted the license key for the file.

Consumers can play files in several ways. They can play them on a personal computer, using a Windows Media player, transfer Windows Media files to a portable player, or copy Windows Media files to portable media, and then play them on a computer or portable player.

Summary-

In conclusion, Windows Media Rights Manager provides a secure solution to protecting digital media for companies and consumers. Based on the Digital Rights Management technology, Windows Media Rights Manager provides the packaging, distribution, license generation and issuance, and deployment methods to make sure that content is secure through encryption. The technologies within each step in the process, such as individualization, Secure Audio Path, and revocation further solidify its effectiveness. Windows Media Rights Manager is continuing to advance and grow as the demand for distributing content through the Internet increases. Windows Media Rights Manager is not used solely as a means for selling music directly to the consumer, but for corporate training, company presentations, and distance learning. In Windows 2003, Microsoft has taken the protection of digital content one step further with introduction of Rights Manager Services (RMS), which looks at protecting data from an enterprise prospective, meaning the transmission of electronic confidential documents.

References-

1) "Digital Rights Management for Content Distribution" by Qiong Liu, Reihanch Safavi-Naini and Nicholas Paul Sheppard
http://crpit.com/confpapers/CRPITV21ALiu.pdf

2) "Windows Media Technologies: Using Windows Media Rights Manager to Protect and Distribute Digital Media"
http://msdn.microsoft.com/msdnmag/issues/01/12/DRM/default.aspx

3) "Security Overview of Windows Media Rights Manager"
http://www.microsoft.com/windows/windowsmedia/wm7/WMRM_security.pdf

4) "Architecture of Windows Media Rights Manager"
http://www.microsoft.com/windows/windowsmedia/WM7/drm/architecture.aspx

5) "Windows Media Security Issues- Whitepapers" by Ranjit Roy
http://www.ebizis.com/techcenter/media.html

6) "Security Features of Windows Media Rights Manager"
http://www.microsoft.com/windows /windowsmedia/wm7/drmnewin7.aspx

7) "Architecture of Windows Media Rights Manager"
http://www.microsoft.com/windows/windowsmedia/wm7/drm/architecture.aspx

8) "Protecting Audio and Video with Digital Rights Management"

http://www.microsoft.com/windows/windowsmedia/howto/articles/DRMProtect

9) "Windows Media DRM FAQ"
http://www.microsoft.com/windows/windowsmedia/wm7/drm/faq.aspx

10) "Welcome to .NET-how MS plans to dominate digital music sales"
http://www.you.com.au/news260.htm

11) "Distribute Media Securely with Microsoft Digital Rights Management"
http://www.devx.com/security/Article/7868/0/page/1

12) "Secure Audiobook Distribution Utilizing Microsoft Windows Media Technologies"
http://ssl.overdrive.com/whitepaper/Secure_Audiobook_Distribution.pdf

13) "Understanding Secure Audio Path"
http://www.microsoft.com/windows/windowsmedia/wm7/WMRMsap_bro.pdf

14) "Digital Rights Management for Microsoft Windows Media Technologies"
http://www.microsoft.com/windows/windowsmedia/wm7/WMRMwhitepaper.pdf

15) "Windows Digital Rights Management"
http://www.microsoft.com/israel/products/windowsmedia/files/Windows_Media_DRM.doc

16)"Issuing Licenses"
http://msdn.microsoft.com/library/default.asp?url=/library/en-us/wmrm/htm/issuinglicenses.asp