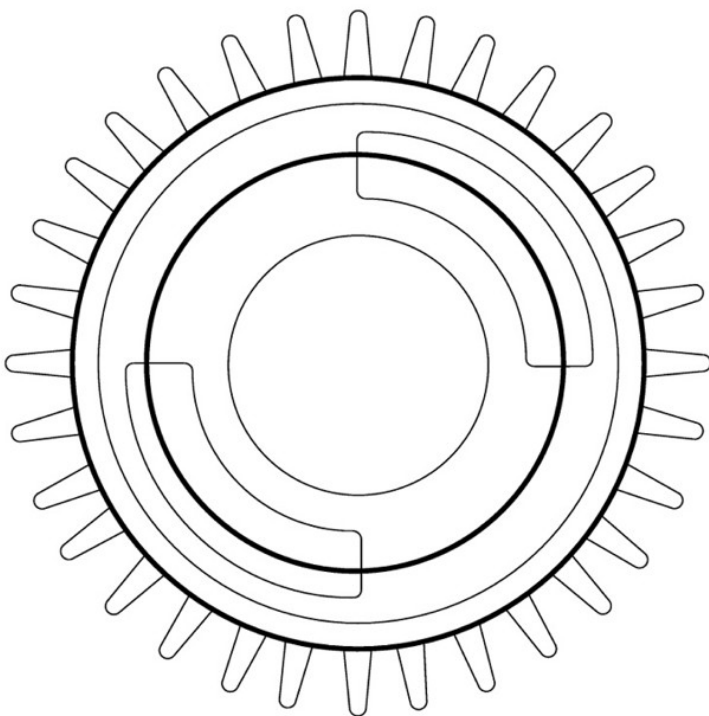


Digital Rights Management



Discussion Document



BCi
Woodbine House
Eastleigh Road
Havant
Hampshire
PO9 2NY
T: +44 (023) 92 477950
F: +44 (023) 92 477951
W: www.bci.eu.com



Introduction

The protection of computer files against unauthorised use in a web environment is normally controlled by a combination of access and Digital Rights Management (DRM) software. This paper discusses an approach to DRM and reviews some technical options.

Concepts

The management of rights, protecting the ownership of anything in a digitised form, has become an increasing area of concern over the years as new means of exploitation via the Internet have emerged and developed. The music industry in particular has taken exception to the exploits of some entrepreneurs using the Internet to freely distribute music tracks and albums. As broadband connectivity has become more prevalent the 'problem' has escalated to DVDs, Television programmes and other areas where the size of files was once a barrier. Digital Rights Management solutions have developed to counteract these activities, although they only work with official sources of the files, if users acquire the content via a different route, ingest and publish, then management solutions do not work.

The protection of copyright has been one of the main drivers in the development of the various DRM solutions. The other key driver has been commercial exploitation of copyrighted material; hence many solutions are geared to e-commerce type applications, for such as pay per use, timed access, etc.

A distinction should be made as to what the digital rights management arena covers, it is the protection of the digital file itself, it is not concerned with the rights associated with the actual content of the file. So the contributor rights and any copyright aspects of the content, whether it is video or audio, need to be managed contractually as before. Digital Rights Management concerns the prevention of unauthorised use of the files once published.

A content file is normally protected using an encryption algorithm that transforms the file into something unusable. The encryption protects the file whilst it is in transit, and should anyone attempt to 'hack' into the web site and download it illicitly. The encryption algorithms that are typically used have 128-bit keys, which is the same 'strength' as those used for secure transactions when purchasing goods over the Internet. A licence is created at the same time that contains the decipher key that will permit the content to be made usable again. The licences are not stored with the content but sent to a separate licence server. On requesting use of the content the user would be directed to the licence server to download a licence at the same time.

This process may be 'silent' and performed without interfering with the user experience or the user may be requested to record their details depending on how this is set-up, and the versions of software employed. The user will be 'verified' as having appropriate credentials to use the content as part of the process. Typically a licence is restricted to a single users' desktop, although the ability to permit transferring or copying the content to other devices is available should it be deemed appropriate. However, this means that if a user downloads some content and subsequently shares it with other users, the other users would be directed to acquire a licence and be subject to the same verification process prior to a licence being issued for them.

The licence contains the rights with respect to how the content may be used. Different usage rights may be expressed for the file based on different user profiles or intended use of the content. The types of usage rights that can be granted include such as:

- One time use
- Save and use multiple times restricted to single desktop
- Save and use multiple times restricted to time period
- Save and distribute – each recipient would need to acquire their own licence to use the content
- Save and Decipher/Edit

There is a grey area in this proposition when files are downloaded and edited. The ability to protect a file needs to be removed so that it can be used in the creative process. Once the supplied files have been edited, with original material added, then this new work may have elements that are technically the copyright of the creator. In addition, the creator may have used other copyrighted material to enhance the work, for example a music track that was not in the original. The new files produced, and submitted for sharing with other users, will therefore potentially have a different set of contributor rights and copyright elements to deal with from a traditional rights management standpoint prior to publication or being made available for other users to download/view.

There are other technologies that can be employed that are not so much concerned with managing rights but detecting the source of any rights violation. These technologies employ digital watermarking and/or fingerprinting techniques to identify the original files used. These mechanisms require that the content files are digitally altered to include a small key, which does not alter the user experience of the content, but does uniquely identify it. To be useful this means that a file would need to be created for each download so that the original source of any licence violation can be identified, and its history traced. This technique may be more useful in a general sense to prove the ownership of a particular piece of content. Obvious implementations of this technique would be to add a Digital on-screen Graphic, which may act as a deterrent – although trans-coding applications can often crop the source or a solid graphic overlaid rendering it useless. These techniques are mentioned as possible areas of further investigation at a later date and are not explored any further in this document.

Note that when a file is downloaded for the purposes of editing it is not protected on the users desktop. Therefore the user can modify and distribute the content without any restriction. Unprotected downloads should really only be available to 'trusted' users, otherwise the content could be easily find itself distributed via various file sharing



networks, and may be edited in an un-moderated fashion, the effort and expense of providing any protection would then be wasted.

Work-flow

The DRM work-flow is similar irrespective of the solution provider. In each case the content is encrypted and packaged/wrapped and is separated from the usage rights associated with it. Each is accessed separately such that the content packages could be distributed widely, but the right to use the content would be controlled by acquiring a key to unlock the package. Figure 1 illustrates the generic work-flow process – each provider has subtle differences to this but do not materially change the flow.

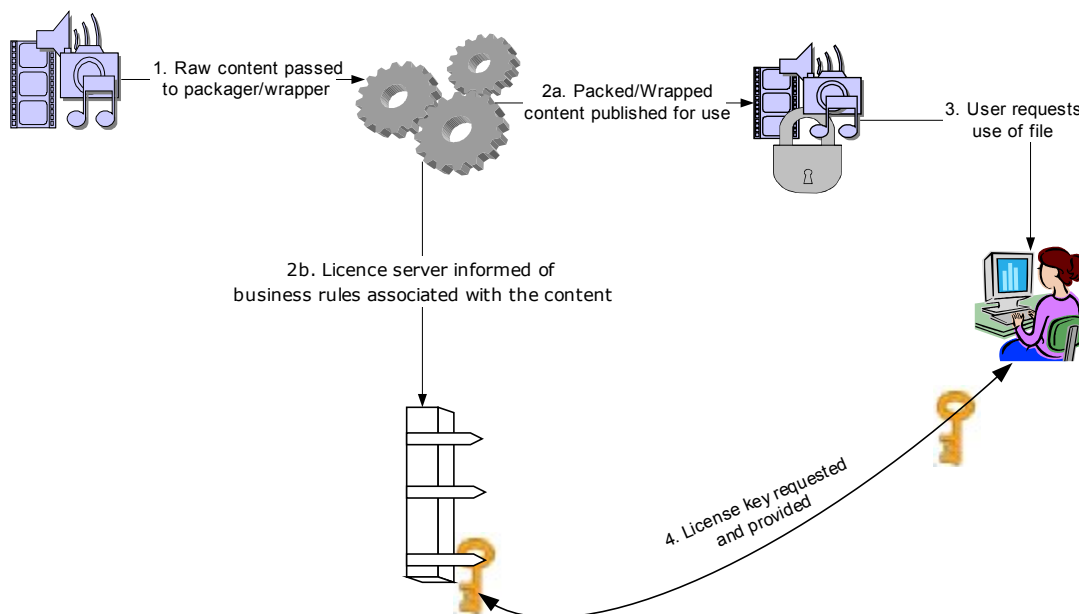


Figure 1: DRM Workflow

Step	Description
1	Raw content passed to packager/wrapper ‘Raw’ content is passed from the ingest process to be wrapped/packaged. This content is already encoded to the appropriate file format.
2.a	Packed/wrapped content published for use The content is protected by packaging in a rights ‘wrapper’. This entails that the content is encrypted, typically with a 128-bit key. Details of where to access the licence key to ‘unlock’ the content are contained within the wrapper so that a client application can acquire the key.
2.b	Licence server informed of business rules associated with the content The details of the nature of the protection, i.e. the business rules – typically by user roles, are passed to a licence key server which associated the access rights with the filename.

Step

3 User requests use of file

Description

The user selects the file to download or play. Depending on the particular solution this may initiate a download of software to interpret the content wrapper, and initiate a request to the licence server for the key to unlock the content. User details may need to be provided at this time.

4 Licence key requested and provided

The nature of the use of the file indicates the type of licence request made to the licence key server. The credentials of the user would be verified and assuming that the request is authorised, the key is passed back and the user can play or download the file.

This request and issue of the licence can be performed 'silently'. However, where desirable/necessary the flow can be interrupted to collect details from the user via form.

Effects of the Distribution Models

The work-flow above does not assume the means by which a user acquires the content to use. The most obvious approach would be for the user to request the use of the content from a web site. If there is a registration process then all the necessary user details could be acquired prior to downloading or viewing any content, in which case their logon details would act as their credentials in step 4. This would be the case when a user acquires content from a centrally hosted and controlled distribution model or from an edge server based model.

If the content is shared between users, either by email, peer-to-peer mechanisms, or by a shared LAN, then each user would need to acquire a licence on use. In this case if the recipient of the file was a registered user then the licence could be issued silently, if they were not already a registered user then their details would need to be recorded and checked prior to a licence being issued. A single user wishing to use the content on different desktops may need to acquire a licence for each desktop.

The registration process would effectively be a check that the user is permitted to use the content, and potentially for what purposes – this may be from such as a territorial rights perspective so that only UK users can access the content. This

Potential Effects of Customer Relation Management Tools

The main driver for DRM solution development has been from protecting the owners copyright and also to exploit it. Therefore the ability to add steps into the process to acquire payment details and to process payments, either for cost recover or commercial purposes are catered for by the solution providers.

The process described above would be interrupted at step 4 so that payment details can be acquired and processed.

Alternate work-flow approach

The work-flow assumes that all content is treated in the same way irrespective of how it is protected. The download and edit option may be approached in a different way. For the user to edit content it has to be unprotected. Therefore as a deterrent for them abusing the privilege of this the acknowledgement of a licence agreement is an important step in the process. Figure 2 illustrates the work-flow for the alternate approach to editable downloads.

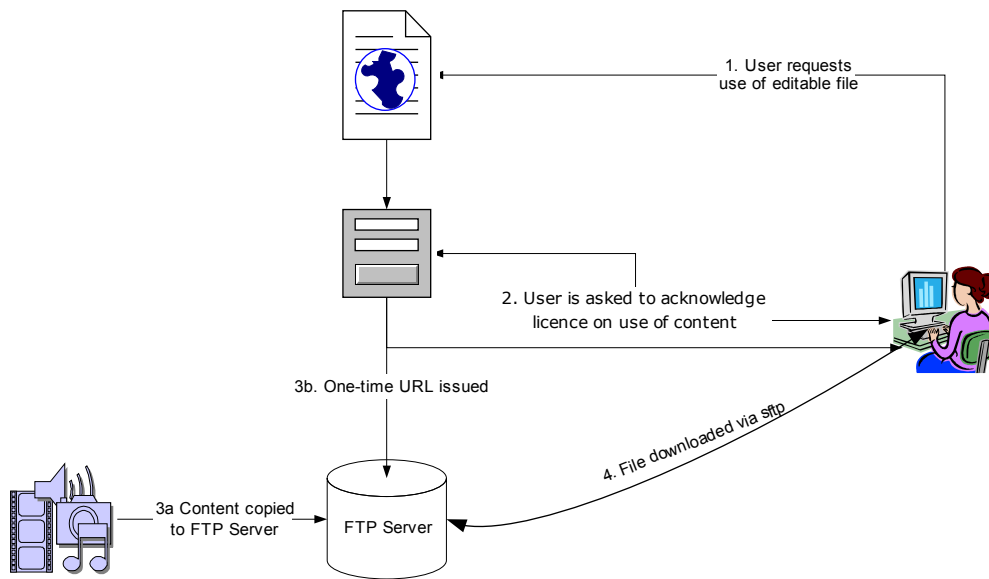


Figure 2: Alternate download Workflow

Step	Description
1	User requests use of editable file This predetermines that the user is requesting the use of files from the web site.
2	User is asked to acknowledge licence on use of content The user will need to register, if they have not so already, acknowledge the reading of a licence which explains the restrictions on its use.
3a	Content Copied to FTP server The requested content file is copied from the content store to the FTP server.
3b	One-time URL issued A one-time URL is created for that content for that particular download and issued to the user
4	File downloaded via sFTP The file is downloaded to the users desktop using secure FTP.

Logical Architecture

The logical architectures of the various providers are very similar, as might be expected from the similarities of the work-flow. Figure 3 illustrates the logical architecture for a centrally hosted model.

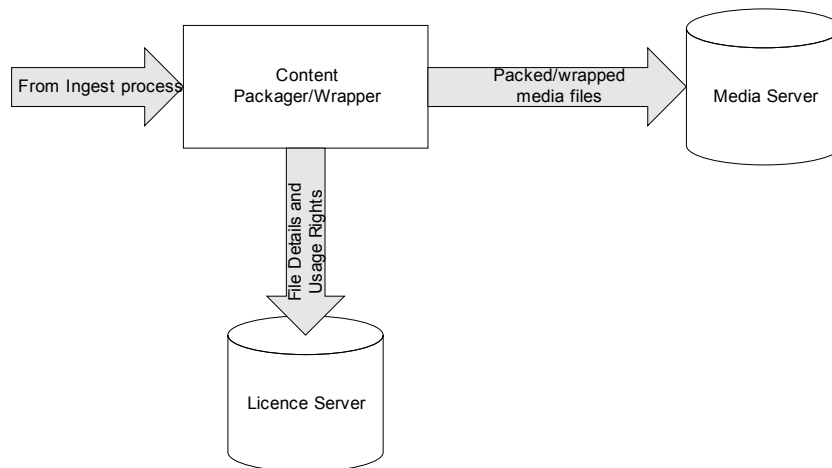


Figure 3: DRM Logical Architecture

There are three main components of the architecture:

A content packaging/wrapper server

This is where the content received from the ingest process is encrypted to protect the contents and a packed file containing the content is created. In parallel a licence is created containing the decipher key and business rules/access rights for using the content.

Media server

This contains the finished wrapped/packed media files ready for streaming or download, (physically they may be separate functionally and load balanced across multiple servers)

Licence Server

The actual components of the logical architecture will depend on the solution to be employed, the logical architectures of the various providers are very similar there are however differences in their physical implementations.

Effects of the Distribution Model

Figure 3 illustrates the logical architecture for a centrally hosted distribution model. The edge server model would have multiple media servers. It is not anticipated that the volume of traffic would require additional Licence servers, although multiples of these – aligned with the media servers – are possible.

Any file sharing distribution methods rely on the central server type model to be employed so that a consistent URL for the Licence server can be identified.

Potential Effects of Customer Relation Management Tools

The additional steps in the process for taking user payment details and authentication may have some impact on the logical architecture, depending on the tools chosen. Secure areas for payment details and secure links for payment authentication would need to be added.

Technical Options

Three options have been considered in detail.

Basic Product Data

Supplier	Product	Server Technology Required	Media Formats Protected	Desktop Access Means
Microsoft	Windows Media DRM	Windows 2000/2003	Windows Media Formats .asx, .wma, .wmv	Windows Media Player
RealNetworks	Helix DRM	Win32, Solaris, HP-UX, AIX, Linux	RealAudio RealVideo MP3 MPEG-4	RealOne
SealedMedia	SealedMedia	Windows 2000	Quicktime MPEG-1 MPEG-4	SealedMedia Add-in (2.5MB download)

Product Pros/Cons

Product	Pros	Cons
Windows Media DRM	<ul style="list-style-type: none"> • The target player is on the majority of end user desktops • Close alignment between DRM technology and player 	<ul style="list-style-type: none"> • File formats limited • Players not widely accepted on other operating systems • Would require use of the SDK to implement the facility to save/decipher/edit option (a more sensible approach may be to use secure ftp download option) • May need to upgrade to newer software revisions for user desktops

Product	Pros	Cons
Helix DRM	<ul style="list-style-type: none"> • Close alignment between DRM technology and player • The target player is a popular and well recognised one for streaming viewing media files • It can be used across all common operating systems • Well integrated toolkit • Client Open Sourced providing possibilities to extend capabilities 	<ul style="list-style-type: none"> • Client application needs to be downloaded • Question over stability, support of certain file formats yet to be verified • Would require use of the SDK to implement the facility to save/decipher/edit option (a more sensible approach may be to use secure ftp download option)
SealedMedia	<ul style="list-style-type: none"> • Works with MPEG-4 files • Has capability of protecting other types of file formats • Have the tools to permit download, edit and 'resealing' type rights deployment. 	<ul style="list-style-type: none"> • A plug-in/add-in is required to which means downloading a 2.5Mb file • It is not associated with a particular player • This company has indicated that it has no commitment to this market area. It is focussing on protection of business information.

Indicative Costs

The implementation costs associated with a DRM solution will be driver primarily by the number of users and the volume of content available for them to consume and their rate of consumption. Actual costs for the software elements have been difficult to obtain. An additional solution option is added to the product costs which is a managed service

Summary Cost Estimates

The following table contains some cost elements indicating the basic set-up costs for a minimum operation.

Product	Software Licences	Hardware (Inc O/S)	Set-up	Total Estimate	Comments
Windows Media DRM	£12,000	£6,000	£50,000	£61,000	No formal costs acquired. SDK costs estimated from information available on Microsoft web site.
Helix DRM	N/A	£4,000		£100,000+	No formal costs acquired. Anecdotal estimates (from peer discussions and options expressed on various web sites) range from £100,000 to ridiculously expensive
SealedMedia Managed Service	N/A	N/A	N/A	£9,000	No costs acquired Estimates based on minimum throughput, this may be subject to an additional storage charge.