Integrating DAM with DRM: Imperatives and opportunities for digital content lifecycles

Bill Rosenblatt

is President of GiantSteps Media Technology Strategies, a consulting firm whose clients include major content providers and media technology companies. He is the managing editor of the newsletter DRM Watch (www.drmwatch.com), Chair of the Jupiter DRM Strategies conferences (www.drmstrategies.com), and author of *Digital Rights Management: Business and Technology* (John Wiley & Sons, 2001). Before founding GiantSteps in 2000, Bill was chief technology officer of Fathom, an online content and education company backed by Columbia University and other scholarly institutions. He has been a technology and new media executive at McGraw-Hill and Times Mirror Company, and he served as manager of strategic marketing for media and publishing at Sun Microsystems. He was also one of the architects of the Digital Object Identifier (DOI), a standard for online intellectual property identification. Bill has a BSE degree in Electrical Engineering and Computer Science from Princeton, an MS in Computer Science from the University of Massachusetts, and executive education from Harvard and University of Southern California business schools.

Gail Dykstra

is Software Technology Manager at the University of Washington TechTransfer Digital Ventures. Gail's career blends expertise in publishing, licensing and DRM with public access advocacy. Prior to joining UW TechTransfer, her experience includes several years as a consultant on digital rights management and licensing; being Research Manager for Information Services at Microsoft Corporation; being Director of Content Development for Micromedia Limited; and as Senior Director for the Canadian Law Information Council. Gail has been widely published in professional and trade journals on information access, copyright, digital rights, DRM technology, information policy, and content development issues. She is a frequent speaker at conferences and information industry events. Gail has a master's degree in Information Science and Librarianship from the University of Washington.

Keywords: *DRM, REL, rights, DAM, integration, compliance*

Abstract One of the most important elements of complexity in content processes is content rights. The processes of managing access to content based on rights information are increasingly necessary nowadays due to various business imperatives. Adding persistent protection to content is the most effective way to control and track access. In this paper, after a brief introduction to digital rights management terms, we explore many of the business and legal imperatives which have led to content processes that are more complex from a rights perspective. Then we discuss some of the ways in which content-handling systems should integrate rights information in order to provide more complete solutions to digital asset management and distribution problems, at lower costs and with faster, lower-risk deployments. We conclude by explaining how adoption of a standard Rights Expression Language goes a long way towards ensuring that integration of content-processing systems through rights information is seamless, predictable and cost-effective for all types of content producing organizations.

Bill Rosenblatt
President
GiantSteps Media Technology Strategies
1841 Broadway
Suite 200,
New York, NY 10023,
USA
Tel: +1 212 956 1045
Fax: +1 212 258 3286
Email: billr@giantstepsmts.com

Gail Dykstra
Software Technology Manager
University of Washington
UW TechTransfer
Digital Ventures
4311 11th Avenue NE,
Suite 500
Seattle, WA 98105-4608
USA
Tel: +1 206 616 3451
Fax: +1 206 616 3322
Email: gdykstra@u.washington.edu

EXECUTIVE SUMMARY

Many different types of organizations, including media companies, large corporations, government agencies, and

others, have been adopting digital asset management (DAM) systems to help them organize digital content and create content-based products for their customers, employees, and partners. DAM systems are intended to be control centers for entire content lifecycles, including content creation, management, production and distribution, but the increasing complexities and interdependencies of these processes result in DAM systems falling short of their ideal responsibilities.

One of the most important elements of complexity in content processes is content rights. The processes of tracking rights, controlling, and managing access to content based on rights information are increasingly necessary nowadays due to various business imperatives. Adding *persistent protection* to content is the most effective way to control and track access. Vendors of DAM and related content-handling systems should integrate their solutions with persistent content protection by including rights and licensing information in the metadata that their systems track and by ensuring that their products are interoperable using standards-based persistent protection technologies. The result will be integrated content-handling systems that meet their customers' current and future needs.

In this paper, after a brief introduction to digital rights management terms, we explore many of the business and legal imperatives that have led to content processes that are more complex from a rights perspective. Then we discuss some of the ways in which content-handling systems should integrate rights information in order to provide more complete solutions to DAM and distribution problems, at lower costs and with faster, lower-risk deployments.

We conclude by explaining how adoption of a standard Rights Expression Language (REL), such as the ISO standard MPEG REL, goes a long way towards ensuring that integration of content-processing systems through rights information is seamless, predictable and cost-effective for all types of content producing organizations.

OVERVIEW OF DIGITAL RIGHTS MANAGEMENT

Digital rights management (DRM) is a popular term for a field that (like digital asset management) also came into being in the mid-1990s,[1] when content providers, technology firms, and policymakers began to confront the effect of ubiquitous computer networks on the distribution of copyrighted material in digital form. There are two basic definitions of DRM: a narrow one and a broader one.

The narrower definition of DRM focuses on persistent protection of digital content. This refers to technology for protecting files via encryption and allowing access to them only after the entity desiring access (a user or a device) has had its identity authenticated and its rights to that specific type of access verified. Protection in such DRM systems is persistent because it remains in force wherever the content goes; in contrast, a file that sits on a server behind the server's access control mechanism loses its protection once it is moved from the server.

Persistent protection solutions consist of these primary technology components:[2]

- Packagers assemble content and metadata into secure files that are variously called packages, containers, envelopes, etc.[3]
- Controllers reside on client devices (PCs, music players, ebook readers, etc). They authenticate the identities of the devices and/or users that request access to content, verify the nature of the access requested, decrypt the content and provide the access. Controllers may also initiate financial transactions where necessary.
- Some persistent protection solutions, particularly newer ones, also include *license servers*. These create and distribute encrypted *licenses* (sometimes called tickets, permits or vouchers) which describe rights to content, the identities of the users or devices to whom the rights are granted and the conditions (eg payment) under which they are granted. DRM solutions that do not include separate license servers install rights descriptions directly into each content file at packaging time.

A broader definition of DRM encompasses everything that can be done to define, manage and track rights to digital content. In addition to persistent protection, this definition includes these other elements:

- Business rights (aka contract rights): an item of content can have rights associated with it by contract, such as an author's rights to a magazine article or a musician's rights to a song recording. Such rights are often very complex and have financial terms (eg royalties) attached to them that depend on the content's use.
- Access tracking: DRM solutions in the broader sense can be capable of tracking access to and operations on content. Information about access is often inherently valuable to content providers, even if they do not charge for access to content.
- Rights licensing: content providers can define specific rights to content and make them available by contract. It is often not possible to track rights licensing by technological means; for example, a book publisher may offer language translation rights to a novel, and in general there is no technological way to ensure that the licensee's translation is either faithful or distributed according to the same terms as the original book.

BUSINESS IMPERATIVES FOR INTEGRATING RIGHTS MANAGEMENT

In this section, we show how new business imperatives increase the desirability of having agile rights management functionality in enterprise content systems. As organizations turn to more sophisticated production processes and seek out revenue-generation opportunities, they require persistent content protection integrated with DAM to ensure proper business practices and implement new business models.

Intellectual property is increasingly, if not exclusively, in digital form. While the nature of their products and their users differ, media companies, corporations and other entities share similar business needs for ensuring that rights are tracked at ingestion; that access is controlled during production processes; and that protection for the content extends throughout product lifecycles. We concentrate on the shared business concerns rather than focusing

on uniqueness of individual digital media formats, products and processes.

The keystone for building digital products is the recognition, respect and tracking of the relationships between the various layers of rights, licenses, permissions and agreements that accrete to content as it moves through its lifecycle from sources to intermediaries to publishers to consumers. Often the layers of rights are so complex that companies either do not bother to process them correctly or process them through lots of expensive manual overhead.

DAM systems are widely adopted because of their capacity to handle complex, multi-layered relationships and processes, along with their ability to leverage large amounts of metadata. Until recently, the complex nature of rights-related business relationships and layered rights data stymied the inclusion of DRM technologies within DAM systems. Unless the enterprise or the content owner can efficiently and effectively trust the distribution of its valued content, its DAM does not provide the full range of functions. With embedded and multi-faceted rights management technologies, DAM systems will be used to their full potential.

Ideally, DAM systems should govern the entire content processing chain; they should demonstrate the ability to handle any combination of authenticating persons, devices, allowed uses, individual and group roles, and varying levels of permission.

CONTROL ACCESS DURING WORKFLOW

Controlling allowed uses of digital content is a critical function of DRM technology. By pre-determining and controlling the exact use(s) for content, DRM technology extends and enhances the traditional role-based access more commonly found in DAM systems.

Example: Content-rich products, such as music, video and software games, are often pirated during production processes by people working from within the company that owns the content or its production service suppliers. Elaborate password systems are time-consuming to maintain, frequently thwarted and do not provide the level of trusted protection required by businesses with intellectual property that has long-term revenue potential. DRM technologies provide the assurance of secured content both behind as well as beyond the corporate firewall. Not only can the content be protected during the production process, its copyright, licensing, reproduction and conditions adhere to the content throughout its use-cycle.

Example: A draft manufacturing guideline is circulated among an international standards committee and participating qualified companies. Using DRM technology, this becomes a closed circulation. The draft guidelines are in a tamper-proof format, with print-only user-rights, limited to a pre-determined timeframe, after which the draft is withdrawn and replaced by the final set of guidelines. The owner of the content, in this instance the standards committee, can withdraw, alter or grant permissions related to the content at any time.

OUTSOURCING

Outsourcing of content production processes increases the requirement for control of authority and authentication.

Companies are even outsourcing the ''family jewels'' — critical customer-facing and revenue-producing applications.

Offshore processing and data-conversion service bureaus have long been a staple of trade, technical, professional and database publishers. Software and entertainment products are routinely outsourced to contract production and manufacturing services. A less traditional form of outsourcing is the use of vendor-contractor to perform core business functions.

While many firms are familiar with outsourcing data processing, IT or web services, there is a growing trend to rely on outsourced personnel for the roles companies traditionally reserved for employees. Some companies are replacing entire departments with contracted vendor services, while others rely on strategic placement of contract or outsourced personnel to prove a ''need for speed'' or specialized development expertise to accelerate product and service development cycles.

The bottom line is that many of the people working on digital content products and processes do not have long-term relationships with or loyalty to the company. Security and communication become large issues and require a level of embedded knowledge within core business processes. Decisions cannot rely on ''handed-down'' assumptions, knowledge of past practices, or inaccessible files.

Solid business decisions are based on ''knowing about the rights,'' not ''assuming.'' This is especially true when intellectual property rights are at the core of an investment decision or structuring a business model. Rights management technology ensures that information expressed in a standard format to minimize ambiguity, provides an efficient and accurate way to update operational routines and assure appropriate levels of accountability.

DOWNSTREAM USE

Rights-managed content creates new value propositions and value networks. Companies need to deliver controlled access downstream so that content can be licensed, deployed and repurposed by business partners in accordance with the terms of agreements. For this to occur efficiently, rights information about content must be stored as part of ingestion processes.

Example: Music recording companies can license DRM-packaged content to online transactional or subscription services. The DRM-packaged content allows both distributors and consumers to choose from multiple fee/free business models. For example, the content could be included in both the free-play list for one-time use on multiple devices, or it could be licensed on a fee-for-play use by media companies, publishers, corporate, government or institutional users. Further, with DRM-enabled content, owners may chose to permit licensees the ability to re-distribute or enter into re-publication agreements. MusicNet is an example of a company that maintains a large catalog of DRM-packaged music tracks licensed from all of the major recording companies and provides these services.

PROTECTION THROUGHOUT CONTENT LIFECYCLES

Piracy, whether of software, music, film, images or text, costs billions of dollars each year. Besides draining corporate

revenues, piracy squanders valuable company time and resources by requiring costly efforts to detect and deter theft.[4] Further, widespread piracy creates an atmosphere of mistrust that can become counterproductive to developing new business models for digital content; it results in content-based products that are less user-friendly than they might otherwise be.

There are other costs associated with unauthorized uses of content as well. For example, some investment banks employ DRM for mergers and acquisition documents that must be kept secret in order to maximize the values of those deals, preserve various types of business relationships and avoid unwanted publicity. The same is true of certain types of corporate governance documents in large companies.

Fluid business models rely on an assurance that copyright and use-rights are protected and extended beyond content production and distribution systems. DRM-enabled protection continues throughout the distribution of the content, auditing its use and accounting for its fees and licenses.

MODIFICATION OF RIGHTS OVER TIME

Digital content can be transformed, reused, repurposed and renegotiated. Companies look for ways to mold their content as business needs dictate and rights, licenses and relationships allow. Many business cases looking at return on investment (ROI) for DAM deployment are based on the proposition of ''create once, reuse many times.'' Core to this DAM function is the system's ability to accommodate changes by updating the parameters of rights and usage as needed to accommodate new distribution models. The nature of the content and its layer of rights and relationships dictate frequency of updates.

Post-hoc re-do of rights data costs money and has the potential to influence customer confidence in the integrity and accuracy of the rights and metadata; indeed it can be a disincentive for customers who insist on high standards of guaranteed accuracy and flexibility from content owners. Furthermore, the lack of ability to change access rights to content can be a serious business liability.

Example: The US Supreme Court decision in Tasini *v New York Times* (2001) compelled content industry vendors to remove or modify core research records in database archives, because creators of content in those archives were not being properly compensated. Compliance costs for vendors included additional staffing to re-code or remove records, systems development expenses, along with increased demand on customer service and marketing departments.[5]

Example: Sensitive documents are often sent around corporations, and to business partners, via e-mail or web posted content. Even with the popularity of PDF format for web posting and setting ''security'' levels for e-mail documents, recipients find ways to download files (eg ''Save As''), thus gaining the ability to alter or distribute the file. Under normal circumstances, it is impossible to change access rights to a file once it has been ''detached'' from a DAM system or other central repository.[6]

Collaborative business-value chains are built on trust. Rights management technology facilitates collaboration,

creating the ''trusted environment'' needed for collaboration by persistently protecting critical intellectual property beyond the boundaries of business processes and corporate organizations.[7]

Example: A boutique international consulting company leading large government and industry projects uses DRM technology to seal its project documents and control and track its critical intellectual property. With the assurance its intellectual property is protected beyond firewalls, the boutique firm enters into a collaboration agreement with another consulting company that is, in other circumstances, the boutique's competition.

REGULATORY AND BUSINESS STANDARDS

Integrity, *authentication*, *security*, *privacy* and *accountability* are watchwords for legislative and regulatory standards, many of which were put in place in the wake of accounting scandals over the past few years. Privacy legislation demands stringent assurance of security.[8] Conversely, security legislation requires assurances of accuracy and authenticity. Public confidence, investors and stockholders depend on secure and accountable sharing of financial and governance data.

Example: Audited financial statements must preclude tampering while providing more timely, accurate and detailed accounting. Financial reporting and securities research require transparency and personal accountability of corporate offices and boards.[9]

Example: Securities industry regulations mandate that compliance officers monitor communications between investment bankers and securities analysts concerning analysts' research reports to avoid conflicts of interest.

Example: Warranties and liability requirements demand strict assurances that the latest, most comprehensive and appropriate instructions, product information and warning of potential hazards are in the hands of the users.

Integrated DRM-DAM solutions can offer corporations, public sector institutions and regulated industries enterprise-wide assurance that content and document operations comply with current regulatory regimes, accountability, privacy and security legislation. Tracking submissions to government bodies is of particular importance to businesses operating in a regulatory environment. Regulatory requirements are subject to change. Compliance can be mandated within a short timeframe with significant consequences for not being able to meet new, and often more stringent, regulatory or administrative standards for business operations.

Companies doing business on a global basis, or those expanding into new jurisdictions, must meet new regulatory requirements. This may call for an entirely different, and more complex, set of jurisdictional rights to be part of the content property. This is a particular concern for companies doing business in the European Union where privacy and database legislation call for significantly different content rights.

With scalable and integrated DAM-DRM technology, organizations can more rapidly respond to change.

Many of the business requirements for DRM-empowered content management systems can be expressed as gains in productivity. These include:

- Elimination of bottlenecks in manual and paper-file dependent systems.
- Decreasing ''hands-on'' personnel costs in data entry and updating records on rights and permissions.
- Maximizing internal skills through greater specialization and flexibility in staffing choices.

The integration of DRM controls increases the ROI for adoption and deployment of DAM solutions for content industries by accelerating product development cycles, eliminating lengthy delays because of missing rights and licenses, and reducing liability risk. The ability to rely on post-DAM control of users' rights permits a wide array of product specialization to meet customer requirements and affords added flexibility in meeting market demands. Content security, reduction of legal liability and increased customer confidence are additional benefits from integrated DRM and DAM technologies.

TECHNOLOGY INTEGRATION OPPORTUNITIES

Many of the business imperatives described in this paper lead to ways in which vendors of DAM systems and other content-handling systems can improve their value through integration with rights management functions. Interoperation of DAM systems with rights management requires two primary steps:

1. Store standards-based metadata that describe rights with content and other metadata in the DAM system.
2. Provide hooks in the DAM that enable it to interoperate with software components that interpret rights metadata, provide persistent protection, manage contract rights and rights licensing processes, and so on.

In this section, we look at typical content processes that are handled by DAM systems and focus on how integrated rights management adds value to them.

CONTENT INGESTION AND METADATA CREATION

The metadata creation process is the nexus for integration between rights management systems and DAM systems that satisfies business concerns such as those mentioned above. As with all other types of metadata, it is most desirable to avoid having to rely on manual input for creating rights metadata. In addition to adding undesirable overhead to business processes, relying on manual input introduces opportunities for errors and inconsistencies in metadata.

The simplest way to automate the creation of rights metadata at ingestion time is to program the DAM system to use default rights metadata settings according to company policy — for example, to assume, unless otherwise specified, that the company holds copyrights on all assets. A more advanced variation on this idea is to set up the DAM system to infer rights metadata according to rules that take into account the type of content, the type of content creation/editing tool from which the asset is being ingested into the DAM, the user doing the ingesting, or the point in a workflow routing. In cases where no automation is possible, the DAM vendor would integrate a template-based rights editor

into the ingestion process, so that a user can fill in the appropriate rights on a case-by-case basis.

Example: A magazine publisher, which stores copyright information in its DAM system, creates all text content in-house but obtains all images from freelancers or other external sources. In this case, if the user is a text editor who is ingesting text items through a text creation tool such as Adobe InCopy, then the DAM system should infer that copyright on those items belongs to the publisher and set the rights metadata accordingly. For a photo editor who is ingesting images through Adobe Photoshop, the DAM system should prompt the editor for information about the external source of a photo.

A company can achieve even more advanced ways of automating the creation of rights metadata in a DAM system if it uses systems for tracking business rights, such as contracts with content creators and other sources of content. An example of this is shown in Figure 1.

In the scenario of Figure 1, the magazine publisher has a system for keeping track of freelance photographers or stock image agencies; many magazine publishers have such systems in the form of small databases on PCs. Systems for tracking freelancers sometimes also track information from the publisher's contract with each freelancer, covering such elements as the terms under which the publisher can redistribute the images it licenses. Terms can include restrictions by time (eg duration or embargo date), geography (eg USA only) and medium (eg print only, not electronic).

It is beneficial to integrate such rights databases with DAM systems so that, as Figure 1 shows, rights information associated with the content sources can go into the DAM system as rights metadata at ingestion time.

ACCESS CONTROL AND WORKFLOW

The above example concerned a scenario involving DAM and editorial and production workflow at a media

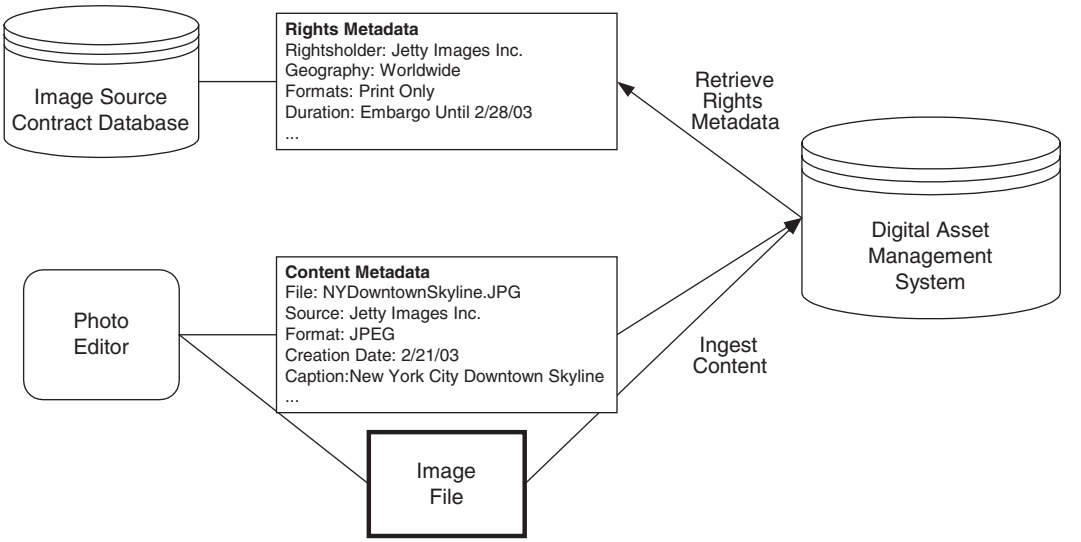

Figure 1: Integrating retrieval of rights metadata with ingestion of a digital image into a DAM system

company. DAM systems used within large corporations depend more on the identities and roles of users, both internal to the company and at the company's external business partners, to determine rights. This is because the ''consumers'' of information stored in corporate DAM systems are employees or business partners of the corporation, whose identities are known and authenticated.

In DAM systems, rights metadata can be supersets of the following types of information typically found in corporate systems:

- File access permissions, such as read, write and delete.
- Resource access control lists of the type found in advanced operating systems and document management systems.
- User and group (role) identifiers, whether local to a single system or network identities, authenticated by passwords, two-factor systems (SmartCards or token cards) or other means.

DAM systems can use rights metadata in integrating with extranet portals that automatically provide selected information to business partners or the general public. Such systems can use identity and other rights metadata to determine what content to make available to which users and under what conditions. When integrated with persistent protection, those access conditions can hold for authenticated users even when they copy content away from the portal (eg on to the hard drives of PCs). Other types of metadata, such as keywords generated by a categorization tool, can help the portal system place each content item in the appropriate place on the website. All this can be done automatically, without user intervention.

Integration of DAM with user and role identity is just as important in certain media industry applications as it is in corporate applications. For example, consider check-in and check-out functions that are common in production workflow and DAM systems in use at media companies. Once a user has checked content out of a workflow or DAM system, there is no telling what could be done with it. In the media industry, one of the ''dirty little secrets'' is that a lot of professional piracy occurs before products are released — that is, piracy is done (or at least facilitated) either by personnel inside a media company or by its business partners, such as post-production houses or mastering labs.

To help combat this problem, content creation/editing tool vendors can provide ''trusted tools'' that interoperate with persistent protection schemes. Tools can incorporate DRM controller (as previously discussed) functions that use rights metadata to determine allowable operations on content, decrypt it and provide that level of access. For example, only a sufficiently privileged user would be able to use a ''Save As'' function within a content editing tool. The tool would read rights metadata which were stored in the DAM system from whence the asset came and packaged with the content (or contained in a separate license). As a backup to such trusted tools, the DAM system could track and report on all content usage, so that any suspicious activity can be identified.

DISTRIBUTION

Various DAM vendors have made claims that their products function equally well for managing content

internally to an organization as for distributing content to customers and business partners, but in reality, DAM and distribution remain largely disparate steps in content lifecycles. As a result, companies must often integrate separate systems for managing and publishing content.

In the classic B-to-C DRM scenario (as previously discussed), a DRM packaging tool takes content files and assorted metadata, and creates packages that are decrypted on the client side by controller hardware or software. DRM packaging applications typically have user interfaces for loading content and specifying rights to that content. A better solution would be to store rights information directly in a DAM system and have the DRM packager simply read it from there through database queries. Simple rights metadata could be stored in a DAM system directly. More complex rights information, especially that concerning business rights or rights licensing terms (see earlier), would more typically be stored in a separate repository, and the DAM system would merely store a unique identifier that links to the appropriate entry in that repository.

A more sophisticated integration between DAM and DRM-based distribution is possible at media companies, which often maintain ''product catalog'' systems containing product metadata. Product metadata overlap with content metadata, but are distinct, because a given item of content can appear in more than one different product. Different products can be intended for different types of customers (eg subscribers vs one-time purchasers vs free trial users, etc.) under different usage terms (unlimited, 30 days only, etc), even though they may all include the same content.

Although few product catalog systems at media companies include this level of detail today, they will need to in the future as media companies put out greater and greater varieties of products based on their content. A further (and admittedly more extreme) need is to define and track products targeted to individual consumers, which implies a requirement to integrate DAM and distribution systems with customer relationship management (CRM) and other types of customer databases, in order to define content rights in terms of individual identities instead of user types.

Example: Some online music retailers have different types of offers for their catalogs of music tracks, including a monthly subscription to the entire catalog, a seven-day free trial of the monthly subscription and paid downloads of individual tracks. A product catalog system should feed a DRM packaging application information about rights to music files that customers request.

As Figure 2 shows, rights metadata in both product catalog and DAM systems can feed directly into DRM packagers to achieve seamless integration with distribution without requiring manual overhead.

Note that rights-controlled distribution is not limited to persistent protection-based DRM systems. Many media companies feed their content to distribution partners under terms that are covered by contract and therefore need not be enforced through persistent protection.

The simplest way to set up multiple content feeds is via file transfer protocol (FTP). A given content provider can

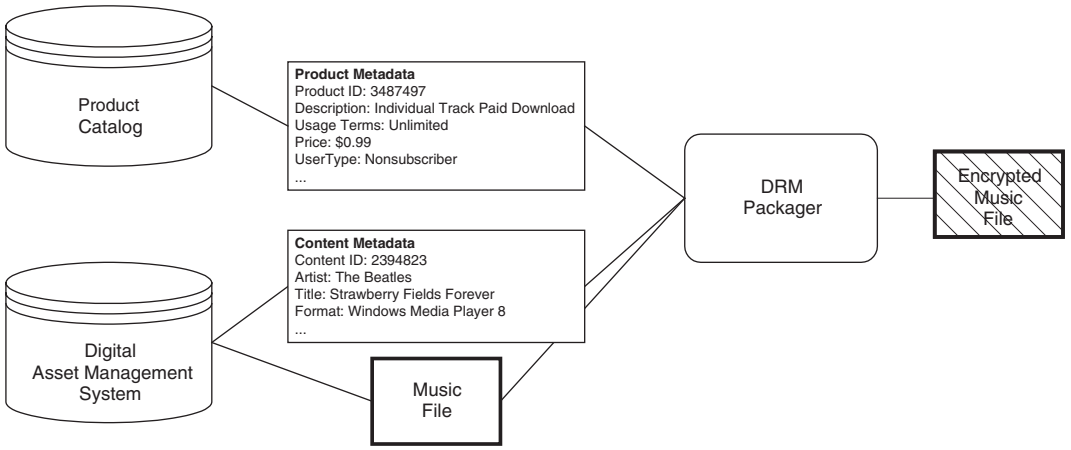

Figure 2: Integrating product and content metadata in a DRM packaging operation

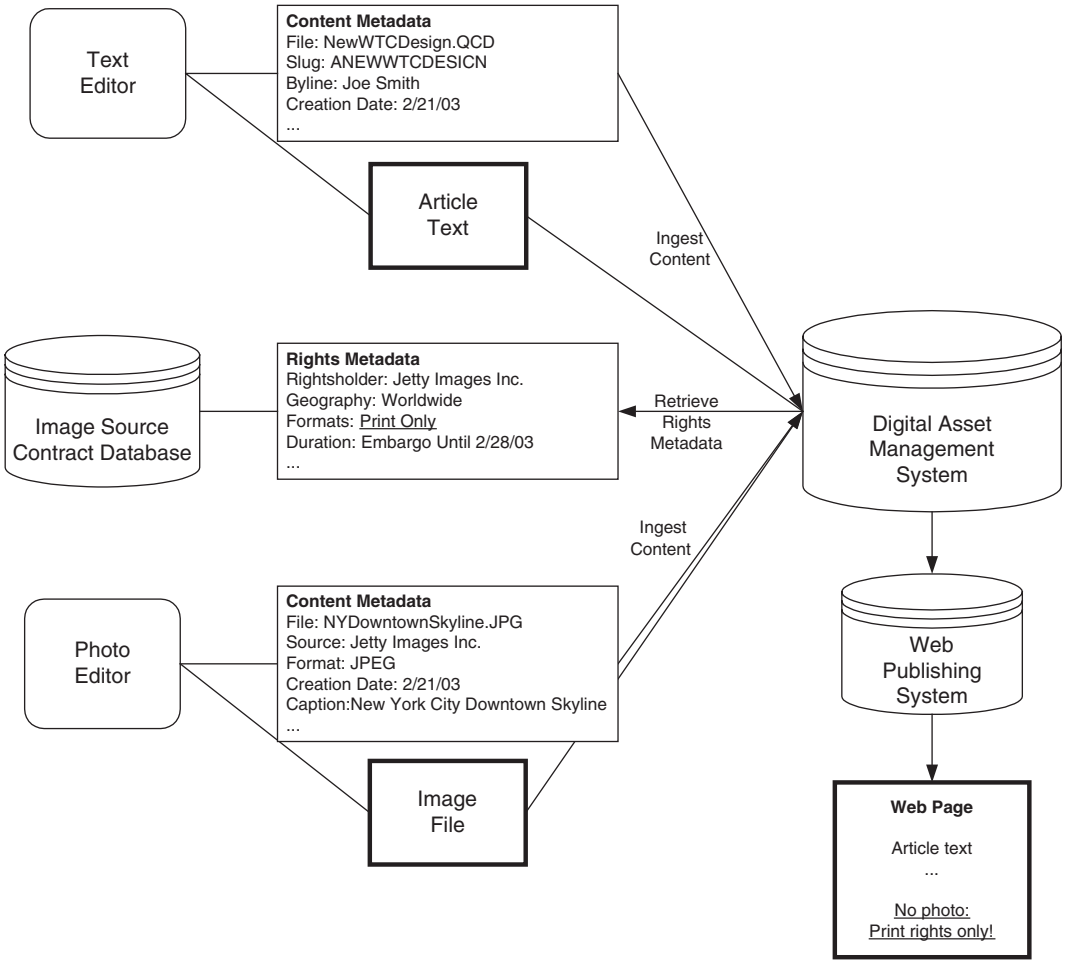

Figure 3: Integrating content and rights metadata through publishing process to ensure that rights are automatically respected

have many different FTP feeds, each of which includes a different subset of the company's content; the ultimate example of this would be a news wire service, which has many different service levels for its subscribers. In this case, information about distribution partners can be linked with rights metadata from product catalog-type systems, which describe different levels of content offerings, to automate the process of putting the appropriate content in various FTP directories for distribution partners to pick up. The Information and Content Exchange (ICE) protocol[11] provides ways of automating this process and describing rights and licensing terms, though without providing a persistent protection mechanism. Really Simple Syndication (RSS)[12] is a less sophisticated but far more popular protocol of the same type.

Example: In the magazine publishing example above, rights restrictions on images derived from contracts with outside content sources result in rights metadata, stored in the DAM system, which in turn governs distribution process so that each customer or distribution partner only sees the content to which they are entitled.

As Figure 3 shows, the magazine publisher from Figure 1 might have a web publishing system that takes content automatically from the DAM system and uses it to maintain the magazine's website. The web publishing system would not use any images with rights metadata set to exclude online distribution.

RIGHTS LANGUAGE: THE KEY TO INTEGRATION

In the above examples, we have seen a number of systems that all depend on the same types of rights metadata to achieve the types of automated process integration mentioned:

- content creation and editing tools;
- digital asset management systems;
- web publishing systems, including corporate portal systems;
- product catalog systems;
- CRM and customer tracking systems;
- content distribution systems.

As we previously noted, integrating all of these types of systems with respect to rights-based processes would be much easier and less costly if every one of these systems had two things:

1. A common understanding of content rights and related information: that is, the same way of specifying, storing and communicating rights information.
2. Standard ways of interoperating with software components that can interpret rights information and act on it in consistent ways — including persistent protection of content; authenticated access to protected content; tracking of content access; and facilitation of financial transactions or other forms of consideration that enable content access according to license terms.

The way to ensure that such integration can take place is to specify content rights and related information in a standard Rights Expression Language (REL). One such REL, the MPEG REL, became an ISO standard in 2004.[13] MPEG REL is part of the MPEG-21 suite of standards for networked multimedia. It was derived from the

XrML (eXtensible Rights Markup Language) from ContentGuard, Inc, which in turn derives from research done in the mid-1990s at Xerox PARC by Dr Mark Stefik into empirical types of content rights information necessary to associate with content rights and ways of expressing all such information with precision and non-ambiguity.[14] MPEG REL has been used as the basis for RELs from other standards bodies including the International Digital Publishing Forum[15] and the Digital Media Project.[16]

Use of a standard REL provides many benefits to content owners. It ensures that the semantics of rights information remain consistent across systems without having to rely on ''lowest common denominator'' mappings among multiple types of rights information, thereby lowering both the cost of systems integration and the risk of legal trouble through misinterpretation of rights information.

For DAM systems and various other types of content processing tools, use of an REL also makes these components more valuable by making them easier to integrate into highly automated end-to-end content lifecycle solutions. Amid all of today's claims of integrated digital media solutions, very few truly end-to-end solutions are available without requiring millions of dollars of risky custom development, much of which is spent on patching together isolated systems. An REL provides a good part of the interoperability ''glue'' that makes integration faster and cheaper, while also helping content owners protect their technology investments by ensuring component-level compatibility as the capabilities of DAM and other systems grow over time.

CONCLUSION

We have described the increasing complexity of content processes in various types of business environments ranging from media companies to large corporations to government institutions. We have shown how persistent content protection and management of rights information are increasingly crucial to ensuring that business processes comply with contractual and regulatory demands, facilitate the implementation of new content-based business models and protect valued corporate digital content both within the enterprise and with business partners.

We have also discussed various ways in which vendors of DAM systems and other content-processing systems should integrate rights information, persistent protection scheme and other rights processing components into their products. We noted that incorporating support for a standard REL goes a long way towards making such integration less costly, time-consuming and risky by giving all components a common understanding of rights semantics as well as a common syntax for expressing them.

Ever since network-based distribution of digital content became a reality, content owners have been searching — mostly in vain — for cost-effective digital asset management and distribution solutions that are truly integrated, to enable them to pursue new business models keep up with the latest technology and ensure that content rights are respected for both legal and economic reasons. Standard Rights Expression Languages will help make this search finally come to a successful end.

References

1 Some observers point to the *Technological Strategies for Protecting Intellectual Property in the Networked Multimedia Environment* conference in late 1993 as the birth of DRM as a discipline. The first commercial DRM solutions became available soon thereafter.

2 The terminology here follows that of Rosenblatt, B., Trippe, B. and Mooney, S. (2001) *Digital Rights Management: Business and Technology*. John Wiley & Sons, New York, NY.

3 Early DRM vendors trademarked names for their secure file formats, such as ''Cryptolope'' from IBM and ''DigiBox'' from InterTrust.

4 See, eg Motion Picture Association of America: http://www.mpaa.org/anti-piracy/ or the International Federation of the Phonographic Industry: http://www.ifpi.org/site-content/antipiracy/piracy-report-current.html, accessed May 23, 2005.

5 The case was settled in March 2005 with payments of up to $18m to the freelance writers who wrote the articles in question.

6 However, some vendors of DRM solutions for corporate applications, such as Authentica, support the ability to revoke rights to a file even after it has been sent to other users by email or other means.

7 CIOs have identified ''lack of trust'' as the #1 factor inhibiting inter-company collaboration. See, eg Paul, L. G. (2003) ''Suspicious Minds,'' *CIO Magazine*, Vol. 16, No. 7, p. 75, January 15, see http://www.cio.com/archive/011503/minds.html.

8 Privacy concerns affect consumer confidence and therefore can have a negative effect on the market for digital content. As an example, news reports about the security breach that exposed eight million credit card account numbers add fuel to consumer concerns about privacy. Governments often respond by legislating new layers of regulation on privacy, e-commerce and credit reporting. See, eg Krim, J. (2003) ''8 million credit accounts exposed,'' *Washington Post*, February 19, p. E01.

9 *Sarbanes-Oxley Act 2002,* SEC and stock exchange reforms.

10 NASD Rule 2711, *Research Analysts and Research Reports*, came into effect on July 9, 2002.

11 The Information and Content Exchange (ICE) protocol from IDEAlliance; see http://www.icestandard.org, accessed May 23, 2005.

12 Really Simple Syndication, an open-source protocol; see http://www.rssprotocol.com, accessed May 23, 2005.

13 ISO/IEC 21000-5:2004; see http://www.iso.ch/iso/en/CombinedQueryResult.CombinedQueryResult?queryString=21000-5, accessed May 23, 2005.

14 See, eg Stefik, M. (1996) ''Letting loose the light: igniting commerce in electronic publication,'' in *Internet Dreams: Archetypes, Myths, and Metaphors*. MIT Press, Cambridge, MA, pp. 219–253.

15 Formerly known as the Open eBook Forum. See http://www.oebf.org/specifications/rrwgcoordinated.htm, accessed May 23, 2005.

16 See http://www.dmpf.org/, accessed May 23, 2005.