Digital Rights Management Metadata and Standards

Jo Anne Cote
Reginald J. P. Dawson Library, QC, Canada

Eun G. Park
McGill University, Canada

INTRODUCTION

In the digital world, several ways to organize and describe digital rights management (DRM) have been developed to enforce fairness and transparency in business trades. Metadata is beginning to serve this purpose as it attempts to address property rights, licensing, privacy, and confidentiality issues in a manner that ideally renders information or content easily accessible over a variety of platforms (Koenen, 2001). With the rise of security breaches and computer crimes such as identity theft, DRM is increasingly an issue for creators, content owners, purveyors, and consumers of all sorts of digital materials. This article defines what DRM is and explains how it is implemented into description and assessment in practical metadata schemes. DRM components are discussed, in particular those related to identification and rights expression. The two commonly used standards of describing DRM are discussed with Open Mobile Alliance and MPEG-21 (Rosenblatt, 2005). Issues and problems of metadata in DRM are also discussed for future implications.

BACKGROUND: CHARACTERISTICS OF DRM

DRM is a technology used to protect owners of content and services. It was first developed from concerns of security and encryption that protects the content and restricts its distribution and dissemination only to persons who are permitted or who paid (Martin et al., 2002). DRM is a relatively recent development, and only two generations have evolved to date (Rightscom, 2003; Krishna, 2004; Erickson, 2003). The first generation focused on security and encryption that restricted the content and its distribution to only those who paid, and the second generation, in effect, comprises the description, identification, trading, protection, monitoring, and tracking of rights usages over tangible and intangible rights assets including management of rights holder's relationships. Iannella (2001) emphasizes that DRM is the "digital management of rights" and not the "management of digital rights…DRM manages *all* rights, not just those applicable to permissions over digital content" (p. 1).

DRM COMPONENTS

DRM systems need to fulfill a range of functions for a variety of people, which are reflected in the following eight components: (1) secure containers; (2) right expressions; (3) content identification and description systems; (4) identification of people and organizations; (5) authentication of people or organizations; (6) authentication of content; (7) reporting events; and (8) payment systems (Rump, 2003). Secure containers make content inaccessible to users who are not authorized to access the content via cryptographic algorithms such as Data Encryption Standard or Advance Encryption Standard. Some examples include the Multimedia Protection Protocol and Digifile. Rights expressions communicate to whom access to content wrapped in secure containers is permitted. Complex expressions may use the Rights Expression Language (REL) of MPEG-21 (Mulligan & Burstein, 2002). Basic elements of rights expression languages are rights, asset, and party (Guth, 2003, p. 103). Content identification and description systems uniquely identify content (i.e., ISBN, Digital Object Identifier) and associate metadata with content (i.e., Society of Motion Picture and Television Engineers SMPT's Metadata Dictionary, MPEG's Rights Data Dictionary). Identification of people and organizations are expression of association of rights owner claim to content unique identification of consumer in order to

limit access to content as required. Authentication of people or organizations involves cryptographic algorithms that may need an agency to issue "passports or certificates" (Trusted Third Party or TTP). Authentication of content persistently associates identifiers and other information with the content (MPEG-21 PAT). These technologies that may be used are watermarking or fingerprinting. Reporting events applies to the business model that allows event-based payments to proceed (i.e., pay-per-view), and it may be also of interest to organizations that collect royalties. Payment systems are enabled through reporting systems.

Metadata is used to manage these components. Metadata is data about data and can be used to describe discrete information objects. Metadata is used to describe content, context, and structure of an object to enhance access to these objects. It can certify the authenticity or degree of completeness of an information object. It is increasingly useful for digital rights management where identification of people or organizations or rights information is essential.

DIGITAL OBJECT IDENTIFIERS

One way to identify content objects in the digital environment is to use the *digital object identifier* (DOI). DOIs are names assigned to any entity for use on digital networks. They are used to provide current information, including where they (or information about them) can be found on the Internet (International DOI Foundation, 2001). DOIs can be applied to any piece of intellectual property (creation), but not to entities such as people and agreements. Information about a digital object may change over time, including where to find it, but its DOI will not change. The DOI system provides a framework for persistent identification, managing intellectual content and metadata, linking customers with content suppliers, facilitating electronic commerce, and enabling automated management of media. DOIs can be used for any form of management of any data, whether commercial or non-commercial. Using DOIs as identifiers makes managing intellectual property in a networked environment much easier and more convenient, and allows the construction of automated services and transactions (International DOI Foundation, 2005). The aim of the DOI data model is to enhance interoperability and improve the quality of administration of DOIs by Registration Agencies (International DOI Foundation, 2005).

Metadata provides the value of identifiers. Without information that may include names, identifiers, descriptions, types, classifications, locations, times, measurements, relationships, or any other kind of information related to a resource, the identified resource is of little use to either humans or computers (International DOI Foundation, 2005). An important component of the Digital Object Identifier system is the data dictionary. DOI has three metadata components for semantic definition that provide well-formed and interoperable metadata to support the use of DOIs: the Kernel Metadata Declaration; indecs Data Dictionary; and Resource Metadata Declaration (International DOI Foundation, 2005).

Rights Data Dictionary

Every rights expression language has a rights vocabulary that identifies the vocabulary permitted as well as its semantics in relation to each REL instance—that is, valid rights expressions (Mulligan & Burstein, 2002).

For example, in an REL instance the print, play or view vocabulary items may be used as granted permissions; the time, location and individual vocabulary items may be used to express a requirement to obtain a permission. Similar vocabulary definitions exist for requirements, constraints, and the context element. The condition element can be expressed by means of the requirements and constraints vocabulary. (Guth, 2003, pp. 104-105)

Rights data dictionaries define vocabulary applicable to every aspect of a digital object. Ideally they are designed to ensure maximum interoperability with existing metadata element sets; the framework allows the terms to be grouped in meaningful ways (DOI Application Profiles) so that certain types of DOIs all behave predictably in an application through association with specified services (International DOI Foundation, 2005). Metadata must use the terms of the appropriate data dictionary to adequately validate DOIs and RELs.

Rights Expression Language

Rights expression languages offer a way to convey use and access rights to assets (or digital objects/digital