7 DRM Standards and Organisations

There are several competing standards in the different areas touched upon by DRM. As stated in the earlier chapters, DRM occupies a rather significant intersection in the content economy and ecosystem. The main objective of this chapter is to examine the various standards that exist in these areas and also to highlight some of the organisations and bodies that help to develop and control them. In order to keep this chapter free from too much noise, every effort is made to ensure that the discussions on standards and organisations are kept as brief and focused as possible and to provide links to other sources of information for those interested in digging deeper.

OVERVIEW

According to the ISO:

> Standards are documented agreements containing technical specifications or other precise criteria to be used consistently as rules, guidelines, or definitions of characteristics, to ensure that materials, products, processes and services are fit for their purpose (CEN/ISSS 2003)

There are several types of standards, which may be described as follows:

- **Formal standards.** These are produced by officially recognised organisations at a national, regional or global level.
- **Industry standards.** A consortium of industry organisations may be formed for the express purpose of creating a standard, based on the consensus by its members within that industry, but which may not have formal standards status.
- **Open standards.** These are publicly available standards that are open to any individual or entity willing to participate in their definition and maintenance.
- ***De facto* standards.** These are widely accepted, non-formal standards that have achieved widespread acceptance in the market over other competing specifications.
- **Proprietary standards.** These are established and maintained through a closed process under the control of an entity or consortium and which may be based on their proprietary intellectual property. These may also be adopted as an industry or *de facto* standard.

One of the main benefits of standards is that they offer an organised, consistent and coherent method for carrying out an activity in a particular area. Without standards there would be utter chaos in the component products and services used and produced by the stakeholders because they would not be able to fit and perform well together even if only affected by a modicum of imprecision. Standards therefore make it easier for stakeholders to get on with the business of providing and consuming content services without worrying too much about the detail in areas outside their control.

The hierarchy of DRM standards

DRM is made up of a suite of technologies, protocols and services that work together to provide some control over the usage rights to a piece of content and, owing to this very fact, it is virtually impossible to have a single standard for DRM systems that will cut across all of the layers through which it provides this service. Table 7.1 describes a hierarchy of standards that map to the different layers and stakeholders in DRM systems as described by Rosenblatt (Rosenblatt et al. 2002; Rosenblatt 2004a).

Table 7.1 *DRM standards hierarchy*

Hierarchy layers	Category	Description and examples
Publisher	Content management	This relates to the many different CMSs and methods in use by the various content service providers. It is not a likely candidate for standardisation in DRM systems and is not discussed in any detail here.
	Rights and holder management	Some standards exist in this category such as the <indecs2> RDD, which is briefly discussed later in this chapter.
	Business models	These are not likely to be standardised as they form the area in which many content businesses try to differentiate themselves. Some established and innovative business models were presented in Chapter 5.
Content and metadata	Content identification	Several unique intellectual property identification standards already exist and include DOI, ISAN, ISWC and UMID. These are described further in this chapter in the 'Identification standards' section.
	Content and product metadata	Many industry-specific standards exist in this category including ONIX, PRISM and NewsML, and these are also explored briefly in the 'Metadata standards' section.

(continued)

Table 7.1 *(continued)*

Hierarchy layers	Category	Description and examples
	Content rights	Rights metadata standards include the XrML-based MPEG REL and ODRL, which we discussed in Chapter 5. They are mentioned briefly in this chapter in the 'Rights standards' section.
	Content formats	This relates to the various formats that are used to distribute and consume the content (e.g. MP3, Windows Media, AAC (Advanced Audio Coding) or RealMedia). These standards are not under the purview of DRM systems and hence are not covered in any detail in this chapter.
Transactional and ecommerce	Payment scheme	This covers the various transactional methods used to purchase content. The standards for payment systems and technologies are not necessarily unique to DRM or influenced by it, so they are not discussed here.
	Authentication	Authentication standards and protocols already exist as part of corporate and ecommerce systems. Examples include the .Net passport authentication technologies used by Microsoft.
	Encryption	Various encryption technologies including some standards were discussed in Chapter 6 and are not presented again here. They include some standard strong encryption algorithms such as AES, Blowfish and RSA.
Connectivity	Internet	The internet standards are the foundation for digital content transmission and distribution in DRM, and they include HTTP (HyperText Transfer Protocol), HTML (HyperText Markup Language) and XML.

The remainder of this chapter is devoted to describing some of the various standards in the different layers above and also the organisations that are responsible for maintaining them. However, before we proceed to that point it is important to take a quick look at the overall benefits and characteristics that standardisation brings to DRM and related areas.

Characteristics and benefits of standards in DRM

There are several factors that influence the push for standards in DRM and its related technologies, processes and business practices and these are also the hallmarks that characterise the benefits of standards to DRM as described in the following sections. The following headings describe some of the main aspects of standards in general and DRM in particular.

Compliance

One major aspect of standards are that they set a certain level of expectation by consumers on any adopting system, therefore those organisations that create and maintain standards must encourage compliance from their adopters. In the same vein any entity, product or service that claims to conform to a particular standard must be able to proclaim and prove compliance with the standard to the prospective buyers or users. This is usually accomplished by some form of accreditation or certification service provided by that standard's organisation or proprietor. After successfully undertaking and passing these compliance checks or tests, the product, service or entity is normally entitled to proclaim itself as compliant to the standard.

Compatibility

A desirable benefit that can be brought by standardisation is the compatibility of products and services from different vendors and service providers. The decision to make a new product or service compatible with existing standards can be relatively easy because of the obvious benefits this can bring for the provider by opening up an existing market of compatible products and services already in use by consumers. Adopting a strategy to ensure that new products are compatible with existing standards (*de facto* or otherwise) can often help in the path to succession of new product standards. This was exemplified by the success of Creative's 1989 SoundBlaster soundcard, which maintained compatibility with the then widely supported AD-LIB soundcard of 1987. Many vendors try, although it is not always possible, to maintain backward compatibility with their own past products for the same reasons. However, product or service compatibility is not the same thing as interoperability, which is a major issue for DRM at the moment and which is also discussed below.

Encourage competition and market growth

One of the loftier ideas of standardisation is to level the playing field for all entrants and operators in a domain and thereby help ignite the market for the resulting standards-based services and products. There is ample historical evidence of this outcome but it is usually found in the more mature fields of enterprise such as in manufacturing, engineering and construction. In the newer (i.e. emerging and converging) fields such as IT, electronics and communications there is a more dynamic flavour to the standards that develop to maturity and this is mostly because the standards themselves often face stiff competition right from the outset unless they are mandated and protected by government agencies, international or commercial bodies. This type of competition by standards may appear at first to be ultimately advantageous for the quality of products and services developed under them; however, the results may be unpredictable unless they are developed with a fair and open system that enables quality to rise to the top. This is particularly true of those standards developed by commercial entities that may become *de facto* standards due to their greater market share and consumer mindshare, at the expense of arguably better-quality rivals (e.g. Betamax versus VHS). These are not negative issues in themselves because ultimately the market determines who wins or loses in these contests; however, the competition for market share by entrenched commercial interests can often stifle some of the major benefits of standardisation (e.g. interoperability).

Interoperability

This is perhaps the most important benefit of standardisation with respect to DRM systems and it has the most to deliver in terms of real benefits to all of the stakeholders in the content value chain. However, and again because of the complexity of the technological, legal, commercial, content and usage intersection occupied by DRM, it is one of the most difficult to achieve across the board. The main issues around DRM standards and interoperability were elegantly portrayed in a presentation by Rajan Samtani in the DRMStrategies 2005 Conference and summarised as follows (Samtani 2005):

- **The Problem**
  - Content – the DRM-protected content of one system cannot be used, distributed and protected by another
  - Rights – the rights, privileges and conditions imposed or granted by one DRM system are not recognised/ enforced across the board by other systems
  - Protection – the protection techniques used by one DRM system may not be recognised and processed by another
  - Trust – the trust models that are used and established by one system may not be usable and/or maintainable by all DRM systems
  - Business models – the models established by or for each DRM system may not be adopted and executed by others
- **The Stakeholder Expectations**
  - Consumers expect that any DRM-protected content should be consumable at any time, any place and on any DRM device or system. Therefore the DRM proposition must offer real choice, flexibility and convenience
  - Rights holders expect that content and rights can be prepared once, distributed by most profitable channels and consumed

(continued)

(continued)

by any DRM system. The DRM proposition must offer choice, flexibility and be cost-effective

  - Vendor – system components can replace similar components from other vendors. The proposition must provide for market share and cost-effectiveness

- **Obstacles to DRM Interoperability**
  - Consumers need to own/access various items like: the devices (e.g. hardware devices, consumer electronics and gadgets); the data (including content, rights, metadata, identification, keys and certificates); and the applications (e.g. software players, decoders and other services)
  - DRM systems need to address numerous items like: metadata (for identification and declaration of content, users and devices); rights (e.g. rights expression, rights data and usage data); protection (e.g. encryption, signatures and watermarks); key management (key hierarchy for encryption and signing); as well as trust management (e.g. trust hierarchy and enterprise policy)
- **Factors that Contribute to Non-Interoperability of DRM Systems**
  - There is a lack (and low adoption) of open common standards for things like: content packaging and protection, rights specification and interpretation, trust establishment and maintenance, business model description and execution
  - There is a hefty cost implication to implementing an interoperable system
  - Some vendors have a high motivation to stay non-interoperable for business reasons. Interoperability requires at least two systems to work together but the owners of these systems may also be competitors for market share (e.g. Apple FairPlay and Microsoft WMDRM or Real Helix systems)
- **Suggested Approaches to Interoperability**
  - Adopting a common open standard (industry-led or *de facto*) for data/content formats, interfaces and protocols
  - Integration with non-interoperable legacy entities by using a shared standard exchangeable data/content format, adaptive interfaces and intermediate protocols
  - Exploiting commercial and other methods to drive some non-interoperable entities out of market, and to reduce alternative, non-compatible standards either by legislation or competition

Figure 7.1 illustrates the important role of interoperability in DRM with a simple electric plug and socket analogy that depicts: the ideal situation of unified, open and interoperable standard; the reality of multiple, fragmented and competing standards; and the compromise solution of adaptation and translation technologies and standards that may be both ugly and inelegant, but which make it all work together anyway.

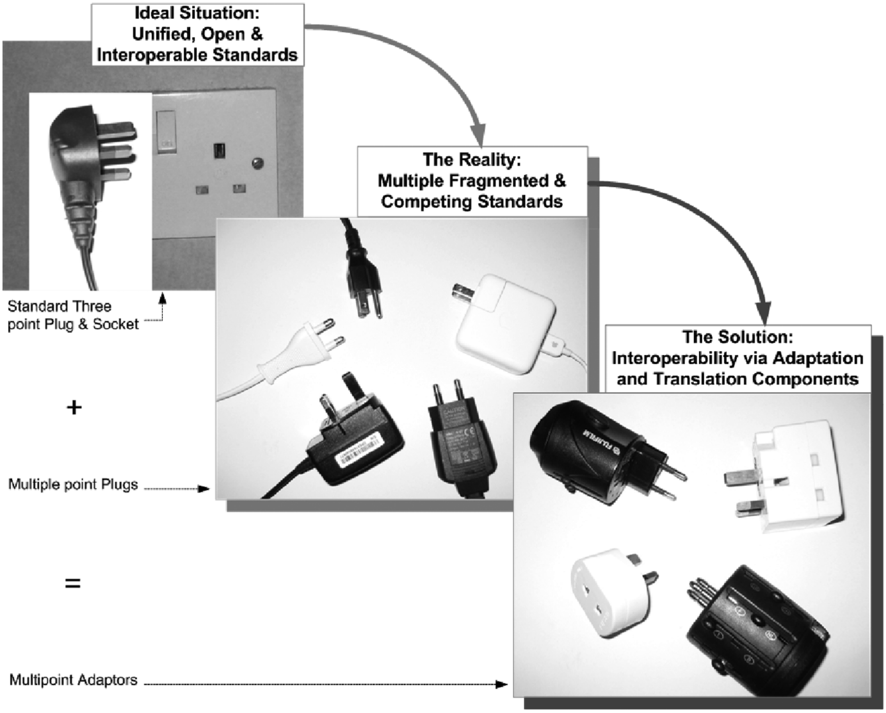

FIGURE 7.1 *Interoperability*

Rights locker

Another approach to DRM interoperability is the use of a rights locker to provide interoperability for content consumers. Basically a rights locker is a central repository for the digital rights of the individual or groups of content users. It works by providing users with a single place to store, maintain and retrieve their usage rights for their content on any connected device (e.g. PCs, mobiles, PDAs, etc.) at anytime and from any place. This is the holy grail of device interoperability and it is very much in line with the trend for service-oriented architectures, which advocate the creation and provision of discrete services by dedicated components that can function independently of the clients or users of that service. The rights locker provides services to the consumer that enables them to download encryption keys and usage rights from a central location irrespective of the device they use to access the content. This may be implemented using established standards for WS standards such as the Simple Object Access Protocol (SOAP):

> The rights locker may also apply internal rules and policies governing how the user accesses the rights and keys from multiple devices; and it could also be used to limit the number of devices allowed etc. (Garnett and Sander 2002)

The above observations adequately sum up the interoperability issue in DRM and point out some of the paths to reaching an interoperable future for DRM systems. In the next section we look at the various standards that exist in the world of DRM and related technologies.

DRM STANDARDS

The following headings are used to group the various standards in the content value chain and DRM landscape into sensible categories of descriptive functionality. This is solely intended to make it easier to present and is neither an exhaustive list nor an authoritative grouping of the standards, but it should provide a fair representation of the types of standards that currently exist in this field.

Identification standards

Content identification schemes started out in the analogue world of books and other physical products to help with the management of stock and other related activities such as cataloguing, shipping and reconciliation. Several content identifications schemes have since evolved or been adapted to cater for online content and they are used to identify different aspects of content including the atomic IP item (e.g. music track), the composite product (e.g. music album or film), the manifest product (CD or DVD versions), as well as the specific product instance (physical media item, e.g. disc ID). Some general guiding principles have been developed and observed in the online content identifier standards and these are outlined below as follows:

- **unique –** online identifiers are designed to be globally unique from the start;
- **dynamic –** independent of physical location;
- **generic –** not dependent on content type;
- **backward compatibility –** can be used with legacy schemes without need to reassign existing identifiers;
- **registry enabled –** global registry functionality to ensure uniqueness, provide lookup service and ownership tracking.

In the following we describe some of the identification standards (including formal international and industry standards) adopted by the different content related verticals. Their home page addresses have been included as a primary source of more information.

International Standard Book Number (ISBN)

This publishing industry standard was originally intended to help with stock handling in the supply chain, but it is now also widely used to aid the identification of books for purchase even in ecommerce systems.

http://www.isbn.org/

International Standard Serial Number (ISSN)

According to the ISSN website, 'the ISSN is an eight-digit number which identifies all periodical publications as such, including electronic serials'. It uses a global database as the register for each serial publication and its assigned ISSN, and the web portal at http://portal.issn.org can be used to access the publication online.

http://www.issn.org/

International Standard Audiovisual Number (ISAN)

This international standard is used in it the film industry for audiovisual content. It uses a 16-digit number to identify a work, that is, the intellectual property item not the physical instance or medium it is manifested in. The ISAN concept includes both an ISO standard international numbering system for audiovisual works and a works database (CEN/ISSS 2003).

http://www.isan.org/

International Standard Work Code (ISWC)

Similar to the ISAN, the ISWC is an international standard used in the music industry to identify intellectual property. It is described on the ISWC website as 'a unique, permanent and internationally recognised reference number for the identification of musical works'. It is composed of a letter 'T' followed by nine digits and an additional check digit at the end (e.g. T-123456789-1), which is allocated by an authorised regional ISWC agency.

http://www.iswc.org/

International Standard Recording Code (ISRC)

According to the International Federation of the Phonographic Industry (IFPI) website, ISRC

> is the international identification system for sound recordings and music video recordings. Each ISRC is a unique and permanent identifier for a specific recording which can be permanently encoded into a product as its digital fingerprint. Encoded ISRC provide the means to automatically identify recordings for royalty payments (IFPI 2006)

http://www.ifpi.org/content/section_resources/isrc.html

Global Release Identifier (GRid)

The GRid system is used to identify sound recording releases for electronic distribution. Like the ISRC above, it is an international standard that is governed by the IFPI on behalf of the international music industry. They have appointed IFPI as the registration authority for the system. The GRid has been designed to allow integration with other identification systems in use by the various music industry entities. The GRid system consists of a release ID, a metadata schema, and data and element definitions for messaging and interfacing with systems (also mentioned in Table 7.2).

http://www.ifpi.org/content/section_resources/grid.html

Unique Material Identifier (UMID)

The UMID is an international industry standard created by the Society for Motion Picture and Television Engineers (SMPTE) for use in creating a unique identifier or reference for any type of audiovisual content. The UMID acts as the link between the content (usually referred to as 'the essence' in this context) and its metadata, and it can be used for identification at a very granular level (e.g. individual still shots or frames in a film). It is a system-generated identifier that uses the automatically generated SMPTE time code in creating the identifiers. The UMID can exist in either a basic or extended form map to 32 or 64 bits respectively:

> The Basic UMID is composed of: A 12-byte label, 1 byte length value, 3 byte Instance number and a 16 byte unique material number. The Extended UMID is comprised of the basic UMID plus another optional 32 bytes of metadata source information which specifies the creation time and date, recording location and name of the organisation and/or content maker (SMPTE 2003)

http://www.smpte.org

cIDf Content Identifier (cID)

The Content ID Forum (cIDf) created this ID system as a robust unique content identifier designed to be used for identifying content instances over a distributed network such as the internet. This level of copy-specific identification is obviously suited to DRM and that is its primary use, along with content instance tracking (each individual copy of a file), copyright clearance, usage monitoring, royalty allocation and anti-piracy surveillance. The cID works by binding the content ID to the content via watermarking, XML signatures and content hash for robustness, and it uses a two-tier issuing authority model to specify the two-part content ID, which is composed of a prefix issued by a central registration authority and a suffix issued by one of many ID management centres:

> The Content ID is applied at the distribution end of the content value chain, hence its ability to track individual instances or copies of files, and it can work in conjunction with other content identification systems either by reference, or by embedding into the content via watermarking (SMPTE 2003)

http://www.cidf.org

Content Reference Identifier (CRID)

The CRID system is designed to facilitate the acquisition of specific audio-visual content instances and it is returned as the location-independent result of a search for content. The CRID may be made up of other CRIDs and used to identify a related group of content (e.g. serial programming):

> The CRID syntax takes the form CRID://<authority>/<data>, and the data portion is similar to, and compliant with, the Universal Resource Identifier (URI) in form and function; it also has to be meaningful to the defining authority (SMPTE 2003)

http://www.tv-anytime.org

Globally Unique Identifier (GUID)

A GUID is a unique 128-bit number that is created and used by applications to identify various item instances (e.g. component, file, application, database record or user). Although typically associated with the Microsoft Windows OSs and applications, which make great use of it, GUIDs are part of the Universally Unique Identifier (UUID) family of identifiers, which are also implemented in other systems and services both online and offline. The sheer number of possible UUIDs means that it is virtually impossible to have a collision (i.e. two components with the same GUID) and they are very useful for identifying even transient content such as online ecommerce transactions or user activity. The IETF has published a proposed standard RFC1422 (http://tools.ietf.org/html/rfc4122) for UUID, which is based on the original specification from the Open Group's Distributed Computing Environment (DCE).

http://msdn2.microsoft.com/en-us/library/aa373931.aspx

Digital Object Identifier (DOI)

The DOI system is an ISO identification standard that is designed for use in the publishing industry to identify any content object in the digital environment. The DOI names, which can be assigned to any object in a digital network, are used to provide information (e.g. location) about that object and although this information may change over time the DOI name remains the same. This persistent identification feature helps to facilitate areas such as content and metadata management, media asset management, ecommerce and interoperable exchange of intellectual property on digital networks. The DOI system is an implementation of the ‘handle system’ (http://www.handle.net), which is a general-purpose distributed information system with a suite of protocols and features that enable the provision of a secure identification and resolution service over a distributed network. The International DOI Foundation, a non-profit organisation, manages the development, policy and licensing of the DOI system to registration agencies around the world.

The DOI is composed of two parts, the prefix and the suffix, which can be represented as *NN.<PREFIX>/<SUFFIX>* (e.g. 10.9999/ISBN.0-7645-4889-1), where NN is the DOI handle, <PREFIX> is the registrant number and <SUFFIX> is the suffix that may incorporate other identifiers such as ISBN in the above example. There is no limitation on the length of a DOI. The two components of the DOI are described briefly as follows:

- **Prefix.** This is assigned to any organisation that needs to register DOIs and there may be multiple prefixes assigned to an organisation. The prefix is separated from the suffix by a forward slash.
- **Suffix.** This identifies the entity and must be unique for each prefix. The suffix may be obtained from an existing identifier (e.g. ISBN) in which case it should be used to refer to the same original entity in both the DOI and ISBN systems.

The DOI system uses the CNRI Handle’s Resolution System to ensure persistence of the current associated value (e.g. URL) to the DOI regardless of any changes to the URL over time. The DOI system also uses a metadata system based on the interoperability of data in ecommerce systems (INDECS) activity, consistent with metadata systems such as Online Information eXchange (ONIX) and MPEG-21 RDD. The DOI metadata enables mappings between application areas to be made consistently. DOI supports added value features such as multiple resolutions to associate a DOI with several data items or related intellectual property items (e.g. versions, derivatives etc.).

http://www.doi.org/

Universal Resource Identifier (URI), Uniform Resource Locator (URL) and Uniform Resource Name (URN)

URIs are short strings that identify resources on the web such as documents, images, downloadable files, services, electronic mailboxes and other resources. According to Sir Tim Berners-Lee a URI can be further classified as a locator or name as follows.

> The term 'Uniform Resource Locator' (URL) refers to the subset of URIs that, in addition to identifying a resource, provides a means of locating the resource by describing its primary access mechanism (e.g., its network 'location') (Berners-Lee 2005)

> The term 'Uniform Resource Name' (URN) has been used historically to refer to both URIs under the 'urn' scheme [RFC2141], which are required to remain globally unique and persistent even when the resource ceases to exist or becomes unavailable, and to any other URI with the properties of a name (Berners-Lee 2005)

A URI syntax generally takes the form of a hierarchical sequence of components, which include the scheme (e.g. protocol such as FTP, HTTP, mailto etc.), the authority (e.g. http://www.bcs.org), the path (starts with the first '/' after the authority), the query (the optional query string starting with '?') and the fragment. Examples of URIs include:

- ftp://ftp.is.co.za/rfc/rfc1808.txt – FTP address;
- http://www.ietf.org/rfc/rfc2396.txt – HTTP address;
- mailto:John.Doe@example.com – Simple Mail Transfer Protocol (SMTP) address;
- news:comp.infosystems.www.servers.unix – Network News Transfer Protocol (NNTP) address.

http://www.w3.org/addressing
http://www.ietf.org/rfc/rfc2396.txt

These standards are used to identify content in a standard and meaningful fashion, but the identity information, while useful in its own right, can be further enhanced with additional information about the content (i.e. the metadata) and there are several standards in this area as we show in the next section.

Metadata standards

As stated above identification systems must be intimately linked to description schemes in order to help deliver DRM functionality. The data/information description schemes are usually referred to as metadata schemes, and they are used in conjunction with the identification schemes to uniquely and unambiguously identify and describe the protected content in the DRM systems. They are also essential for monitoring content usage and the reconciliation of payments to the content owners and other stakeholders in the value chain. This section lists some of the various metadata schemes and standards in use today as follows. Websites have again been included as a source of further information.

Online Information eXchange (ONIX)

This metadata standard has been adopted by book publishers and resellers (including online giants such as Amazon, and Barnes and Noble) where it is used both for physical goods (books) and digital goods (ebooks). It is perhaps the best developed and most adopted metadata scheme in the content industries.

http://www.editeur.org/onix.html

Dublin Core

This standard is mostly used for bibliographic metadata and it is quite general; therefore adopters usually need to customise or extend it to suit their particular needs. The Dublin Core metadata scheme originated at the Online Computer Library Center (OCLC), also formerly known as Ohio College Library Center.

http://dublincore.org

Publishing Requirements for Industry Standard Metadata (PRISM)

This metadata standard is based on the Dublin Core metadata scheme and is mainly used by the magazine industry. PRISM also has an XML-based rights language associated with it and this was discussed earlier in Chapter 5.

http://www.prismstandard.org

CrossRef

This standard is mainly used by the scientific journal community for reference linking via a specified set of bibliographic metadata, which may include DOIs.

http://www.crossref.org

Learning Objects Metadata (LOM)

This scheme covers educational materials (e.g. anything from lecture notes to complete courses work). It is also based on the Dublin Core scheme and is overseen by IEEE's (Institute of Electrical and Electronic Engineers) Learning Technology Standards Committee.

http://ltsc.ieee.org/wg12/index.html

News Markup Language (NewsML)

This metadata standard caters for all types of news content (including text, images, audio and video clips). It was developed by the International Press and Telecommunications Council (IPTC).

http://www.newsml.org/

MPEG-4

MPEG-4 is a standard for multimedia content and is designed to include a large amount of metadata on the multimedia content object. MPEG also has standards for video and audio compression (i.e. MPEG-2 and MP3 respectively). The MPEG-4 standard has some built in support for IPRs via the Intellectual Property Management Protocol (IPMP) interface.

http://www.chiariglione.org/mpeg/standards/mpeg-4/mpeg-4.htm

INDECS

This is an international initiative for rights owners to create standard metadata for use in ecommerce systems; therefore it has been designed from the ground up to cater for all content types. The <indecs> project delivered a framework and approach for interoperable metadata that addressed five distinct areas of interoperability: across media (e.g. books, periodicals, audio, audiovisual, software, abstract and visual works); across functions (e.g. cataloguing, discovery, workflow and rights management); across levels of metadata (from simple to complex); across semantic barriers; and across linguistic barriers. The resulting framework has been adopted by some metadata-focused organisations such as DOI, EDItEUR and Muze Limited.

http://www.indecs.org/
http://www.dlib.org/dlib/january99/bearman/01bearman.html
http://imageweb.zoo.ox.ac.uk/wiki/index.php/DefiningImageAccess/Standard/INDECS

Rights standards

DRM rights standards are used to implement rights models and they are composed of the following items: the rights (e.g. play, view, copy, lend, extract, edit etc.), the measure or extents (e.g. length of time, number of times etc.) and the payment or consideration (e.g. money, user data, membership or promotion or loyalty scheme details etc.). The standards are also used to describe rights relationships between the various entities (e.g. devices, users, institutions) and content items. This section is intended to present some of the main rights description standards and languages used by DRM systems, however, these have been previously covered in Chapter 5 (see the 'Rights modeling and languages' section) so we focus mainly on the two main contenders of competing rights description or language standards in the DRM space as follows.

MPEG REL

The MPEG REL is wholly derived from XrML, which was created by ContentGuard around 2000. XrML was in turn derived from DPRL, which was created by Mark Stefik and others at Xerox PARC circa 1994.

This REL can be used for rights in all types of media and enterprise applications. This standard (as well as XrML) is used by many software and DRM vendors including Microsoft. It is also supported by many standards organisations including ISO, MPEG, Open eBook Forum, CRF and the TV Anytime Forum.

ODRL

Dr Renato Iannella created ODRL while working for IPR Systems Ltd in Australia around 2000. As the name suggests it uses an open specification and uses freeware licence terms.

This rights language is more specific to media applications than XrML and it is extensible via the use of profiles, which are domain specific implementations of its subset. It has been adopted heavily in the mobile telephony space via the OMA DRM profile. It is also positioned for adoption in the open-source community with its CC profile. Standards bodies supporting this language include the OMA.

Other DRM-related standards and initiatives

The following standards are also related to DRM systems and have been included here for completeness. Some of them have been grouped into specific categories, derived from a tutorial by Bill Rosenblatt in 2004, and they range from home network standards to interoperability-focused initiatives, as well as obsolete standards, in order to cover the quagmire of different standards that exist in this field.

MPEG-21

MPEG-21 is a framework for standards in networked multimedia and it encapsulates most of the current existing standards as well as those under development. It is applicable to all content types, formats and networks.

DRM support is focused on the IPMP module, an enhancement to the original MPEG-4 IPMP specification, which had little support for interoperability. MPEG-21 also supports XrML and <indecs2>RDD for its REL and RDD respectively. MPEG-21 became an ISO Standard in 2003.

Home networking standards

DTCP

Already covered in Chapter 6, the DTCP standard is intended to protect digitally transmitted content within the HEN. It was created by the 5C Entity of Hitachi, Intel, Matsushita, Toshiba and Sony, and is discussed later in this chapter.

CPRM and CPPM

Also covered in Chapter 6, the CPRM and CPPM standards provide copy protection for digital content on physical media. They were created by the 4C Entity, which is made up of Intel, IBM, Matsushita and Toshiba.

Secure Video Processor (SVP)

The SVP standard is a hardware DRM specification for use in STBs and other video-enabled content devices. It works by adding security enhancements to a standard video processor in order to make it a secure video processor that can be used to implement the business rules and rights associated to content within the SVP-enabled device and beyond. SVP licensing is handled by its own licensing authority (SVPLA), which issues and manages all of the licences for all of the intellectual property required to implement SVP by any organisation. SVP is supported by some of the major industry players such as NDS, Thomson and STMicroelectronics. The SVP Alliance website at http://www.svpalliance.org/svp.html contains further information.

Meta-DRM standards

Digital Media Project

This meta standard initiative was started in 2003 by Dr Leonardo Chiariglione (who also founded the MPEG organisation) and its aim is to help codify and automate traditional rights usages (TRUs).

Coral Consortium

This was the first major alliance formed specifically to address DRM interoperability issues and it comprised major technology vendors and content providers along with InterTrust. The Coral Consortium proposed to create DRM interoperability through services that would be based on InterTrust's Networked Environment For Media Orchestration (NEMO) technology. The NEMO technology provides an interoperability layer that enables communication between DRM systems via a translation language or service. The proposal relied on the use of a standard specification for interfaces and services that would provide a uniform DRM experience for consumers of any compliant DRM-protected content. The consortium website news pages at http://www.coral-interop.org/main/news/pr20060222.html state that although much has been made about its demise, the consortium is very much alive and increasing its membership, and updated its interoperability specifications in February 2006.

Marlin JDA

The Marlin Joint Development Association (JDA) was created by the members of the Coral Consortium (including Sony, Philips, Samsung, Panasonic–Matsushita and Intertrust) as an alternative approach to interoperability, which is based on the idea of common building blocks for DRM systems in order to enable compliant devices to interact with DRM-protected content using a single toolkit. Marlin is XML-based and built around the technologies of its member community including Intertrust's NEMO and Octopus technologies. The latter technology is a toolkit for creating DRM engines based on selected components from a menu of DRM building blocks that include several rights languages, encryption methods and supported business models. Marlin requires the formation of a licensing authority that will enforce standards compliance and administer patent licensing. Marlin provides user-based authentication (not device dependent) with a 'federated identity' approach from the Liberty Alliance, which is also discussed later in this chapter. Marlin supports a sophisticated domain model that can be enforced locally or by a server and allows temporary sharing such that user of a content service can play their content on other 'guest' devices.

Industry- and application-specific standards

Content Reference Forum (CRF)

This interoperability standards initiative is aimed at providing automated multi-tier distribution for content. CRF uses a content reference concept, which is similar to DOIs and other content identification standards. Its Contract Expression Language (CEL) is complementary to the more common RELs and is based on the MPEG REL. The forum members include industry players such as ContentGuard, Macrovision, Microsoft, Nippon Telegraph and Telephone, Universal Music Group and VeriSign. The CRF's website at http://www.crforum.org/ contains more information.

ISMAcrypt

Internet Streaming Media Alliance (ISMA) created this AES-based encryption standard for streaming media. The Alliance's website at http://www.isma.tv/ has further information.

Obsolete and inactive standards

SDMI

SDMI was originated by RIAA as a DRM mechanism for music players, which was based around encryption and watermarking protection.

OASIS Rights Language

This was originated by ContentGuard as an OASIS-backed standard but was officially discontinued in favour of XrML.

eXtensible Media Commerce Language (XMCL)

XMCL, created by RealNetworks, did not gain much traction and was overshadowed by developments in MPEG-21 around 2001.

The above discussion gives a fair overview of the state of affairs in the world of DRM-related standards and, as can be discerned, it is not an ideal state in which to develop and maintain steady momentum in the quest for a solution that will satisfy all of the stakeholders. There is no doubt that these standards and initiatives are currently rather fragmented and perhaps too numerous to be immediately beneficial to all stakeholders; however, this will likely change in the long run.

DRM STANDARDS ORGANISATIONS AND INITIATIVES

This section looks at some organisations that are involved in creating and maintaining standards for DRM and related technologies. It is purely intended as a quick overview of typical entities that exist in this space.

DRM standards organisations

OMA

The mobile telephony-focused OMA was formed in June 2002 by the consolidation of the WAP Forum and the Open Mobile Architecture Initiative and with the support of many of the leading mobile operators, device and network suppliers, IT companies, as well as content and service providers. Its main purpose is to enable the development of mobile services specifications that support interoperable end-to-end mobile services. A major focus of OMA activities is DRM and their OMA DRM 1.0 standard was designed specifically for simple, low-cost devices with little memory and provided three DRM methods of forward-lock (used for subscription content, no forwarding), combined delivery (caters for rights-enabled content) and separate delivery (supports superdistributed content). OMA DRM 2.0 extended the capability of the OMA system to cater for richer content on more powerful devices and support for more diverse and sophisticated business models, improved security with PKI support and content integrity checking. As stated earlier the OMA DRM standard is based on a profile of the ODRL standard and its specifications are made by the Content Management License Administrator (CMLA) with members that include content providers (e.g. Warner Bros.), mobile operators (e.g. Vodafone, Orange, O2 and T-Mobile etc.), mobile device makers (e.g. Nokia, Matsushita, Samsung), chipmakers (e.g. Intel) and software and DRM vendors (e.g. RealNetworks, CoreMedia and BeepScience). The OMA website at http://www.openmobilealliance.org provides further OMA-related information and documentation.

MPEG

MPEG was established in 1988 and was formally known as ‘Working Group 11 of Sub-committee 29 of the Joint Technical Committee 1 of ISO/IEC’. It is responsible for developing standards for encoded digital audio and video such as MPEG-1 (VCD and MP3), MPEG-2 (DTV and DVD), MPEG-4 (multimedia for web and mobile), MPEG-7 (video and audio description and search) and the latest MPEG-21 framework, which is a standard in 14 parts that includes major DRM components such as MPEG-REL (Part 5) and MPEG-RDD (Part 6). Licensing of the patents in MPEG standards is provided by the MPEG Licensing Authority (MPEG LA). More information can be found on the MPEG homepage at http://www.chiariglione.org/mpeg/, which is maintained by the group's founder Leonardo Chiariglione.

International Digital Publishing Forum (IDPF)

Formerly known as the Open eBook Forum (OeBF), IDPF is the trade and standards association for the digital publishing industry, with membership that includes the academic, trade and professional publishers, various hardware and software companies, as well as digital content retailers, libraries, educational institutions and other related organisations. IDPF has done a lot of work on DRM-related specifications for the publishing industry especially in areas such as rights language (e.g. OeBF REL) and container technologies. According to their website:

> the Open eBook Rights Expression Language is the result of many months effort to create an OeBF Rights Grammar Requirement for digital books based on XML and an industry specific extension of the MPEG REL (OeBF 2003)

Also IDPF is currently working on its Open eBooks Container Format (OCF) specification to be used in creating secure containers for digital content. Generally speaking, the publishing industry has been very active in generating standards for identifiers and metadata (e.g. DOI and ONIX) and the IDPF is geared to pushing this innovation forward through its many working groups. The IDPF website at http://www.idpf.org contains more information.

Coral Consortium and Marlin

As already mentioned, the Coral Consortium and Marlin JDA were formed for the express purpose of promoting interoperability in DRM systems. Their website at http://www.coral-interop.org/ contains further information.

Digital Living Network Alliance (DLNA)

The DLNA is an organisation composed of some major players in computer hardware and software, consumer electronics and content provision. Its main objective is to promote a seamless end-to-end HEN that supports interoperability. To this end the DLNA provides guidelines on interoperability among other things and has adopted the Internet Protocol as the networking standard for connectivity in the home. The DLNA website at http://www.dlna.org/en/industry/about has further information.

4C Entity and 5C Entity copy protection standards

These two entities have technologies that combine to protect content and distribution in the home entertainment environment's systems and devices. As mentioned earlier and in Chapter 6, 4C Entity's CPPM and CPRM technologies, which fall under the CPSA, help to define a framework that enables the integration of major existing content protection technologies including watermarking for disc-based content. Also 5C Entity's DTCP, under the DTLA, is responsible for the technology that protects audio and video entertainment content on the digital network. DTCP is designed to extend protection to content that originates from approved and compliant devices or protection schemes such as CSS for DVDs. 'Essentially the 4C Entity emphasises secure storage, while the 5C Entity emphasises secure transmission' (Larose 2004). The 4C Entity http://www.4centity.com and 5C Entity http://www.dtcp.com/ websites contain more information.

Copy Protection Technical Working Group (CPTWG)

CPTWG is an ad hoc and voluntary group that was formed in 1996 by technology and entertainment companies to evaluate content-protection technologies aimed at the home entertainment environment. This group acts as an arbitration mechanism for resolving major content industry issues, such as copy protection, by inviting submissions from the stakeholders of potential solutions, which are evaluated based on a set of criteria and from which a final recommendation is made for adoption by the industry. Technologies that have passed through the CPTWG process include: DVD-CSS, DTCP, HDCP, CPRM, CPPM and the American 'Broadcast Flag' for digital TV copy protection. The CPTWG website http://www.cptwg.org/ has further information.

TV-Anytime Forum

According to their website this organisation:

> is an association of organizations which seeks to develop specifications to enable audio-visual and other services based on mass-market high volume digital storage in consumer platforms (TV-Anytime 2005)

The TV-Anytime specification is intended to ensure that content can be stored securely in a consumer device and still be interoperable with other compliant devices in the home. Members of the TV-Anytime Forum include major broadcasters (e.g. BBC, BSkyB, RTL and Fuji Television), equipment makers (e.g. Philips and Sony Corporation, JVC, Toshiba, Matsushita and Sanyo), telephone operators (e.g. British Telecom, France Telecom), mobile phone makers (Motorola, Nokia and Sagem) as well as software and content-protection companies such as Microsoft, ContentGuard and NDS. The European Telecommunications Standards Institute (ETSI) adopted and published TV-Anytime's specifications (Phases 1 and 2) as ETSI Technical Specifications. The website http://www.tv-anytime.org/ has further information.

Other related standards organisations

OASIS

According to its website OASIS was founded in 1993 and 'is a not-for-profit international consortium that drives the development, convergence, and adoption of e-business standards' (OASIS 2006). It has been responsible for numerous WS standards as well as various standards for security, ebusiness and other application-specific markets including DRM. OASIS has also adopted an open, transparent governance and operating model, with members driving the agenda and consensus-based decision-making process. The consortium also operates two major information portals on XML and WS (i.e. http://www.xml.org and http://xml.coverpages.org). The OASIS website at http://www.oasis-open.org has further information.

IETF

This is a large open international community of individuals and organisations that are concerned with the evolution of the internet architecture and the smooth operation of the internet. IETF works via several working groups, which are organised by topic into several areas (e.g. routing, transport, security etc.). Within IETF, the Internet Architecture Board (IAB) is a sub-group that has been chartered by the Internet Society (ISOC) to oversee the architecture of the internet. Also under the mandate of ISOC, the Internet Assigned Numbers Authority (IANA) performs the role of central coordinator for the assignment of unique parameter values for internet protocols. The IETF website at http://www.ietf.org/ has further information.

W3C

This is an international consortium with over 400 member organisations around the globe. It is responsible for developing and promoting technology standards for the web, such as HTML, XML and Cascading Style Sheets. XML has developed to become one of the foremost technologies used by DRM systems for managing digital content in the online environment. It is used in the basic structure for XrML and ODRL, which are the foundations of standards such as the MPEG REL, the OMA REL, the MPEG Digital Item Declaration and many other standards and proprietary technologies. W3C membership is open to any organisation that is willing to sign its membership agreement and it adopts a rigorous process through which all proposals must pass before getting its seal of approval. The W3C website at http://www.w3.org has more information.

ISO

This is the ultimate international standards organisation and it is described on its website as:

> a global network that identifies what International Standards are required by business, government and society, develops them in partnership with the sectors that will put them to use, adopts them by transparent procedures based on national input and delivers them to be implemented worldwide (ISO 2006b)

ISO was set up as a federation of the national standards bodies of over 150 countries around the world and it has a total of some 16,077 standards in its portfolio as of August 2006. The ISO website at http://www.iso.org has further information.

European Committee for Standardisation (CEN/ISSS)

CEN is one of three formal European Standards Organisations within which the Information Society Standardisation System (ISSS) operates as the department responsible for standards activity in information and communications technologies (ICTs). In 2003 the CEN/ISSS DRM Group undertook and published an overview report on DRM standardisation, at the behest of the European Commission, in order to identify the status of DRM usage and to ensure effective implementation of DRM in the marketplace. This report is available at http://www.cen.eu/ along with further information about CEN.

SmartRight

Based on the SmartRight technology originally developed by Thomson, the eponymous SmartRight organisation is a consortium of mostly European companies that supports a smartcard-based 'copy protection system for digital home networks'. Licensing is handled by the SmartRight Licensing Authority, which licenses the intellectual property to anyone wishing to implement the SmartRight technology. The SmartRight website http://www.smartright.org/ is a source of further information.

The International Group for Electronic Commerce in the Book and Serials Sectors (EDItEUR)

EDItEUR is the international group responsible for coordinating the development of the standards infrastructure for electronic commerce in the book and serials industries. It is composed of about 90 members from 17 countries and acts as the umbrella body for many national electronic data interchange (EDI) groups in the publishing industry. EDItEUR is managed by the London-based Book Industry Communication (BIC) group and it provides several services to its international membership including research, standards and guidance in areas such as: EDI and other ecommerce standards for book and serial transactions; bibliographic and product information; the standards infrastructure for digital publishing; radio-frequency identification (RFID) tags; and the trading and management of rights. The EDItEUR website http://www.editeur.org/ has further information.

SMPTE

This society was founded in 1916 as an international professional association of motion picture engineers. It is a very active standards developing organisation and has over 400 standards, recommended practices and engineering guidelines for television, motion pictures, digital cinema, audio and medical imaging. Membership is open to any interested individual or organisation in the field. Some significant SMPTE standards include: all film and television transmission formats and media, including digital; physical interfaces for transmission of television signals and related data (such as SMPTE time code and the Serial Digital Interface); the SMPTE Color Bar Test Pattern and other diagnostic tools; and the Material eXchange Format (MXF). See http://www.smpte.org/ for information regarding these and other areas.

Creative Commons

CC is a worldwide organisation that offers copyright alternatives to content developers and owners for use in licensing their works anywhere in the world (see Chapter 3). See http://creativecommons.org.uk for more information.

Liberty Alliance

This alliance led by Sun Microsystems has adopted the mission to establish an open standard for federated network identity through open technical specifications. It facilitates the creation of federated network identity solutions with inbuilt interoperability among multiple identity databases. It is also designed to appeal to the consumer's privacy concerns by not relying on a single central repository of user information, but instead using the federation of linked systems to build a complete profile as required. See http://www.projectliberty.org/ for further information.

Windows Live ID (also Microsoft .NET Passport)

Microsoft's proprietary online identification standard delivers online identity services that are independent of individual websites, services and devices. It ties together Windows XP licence, MSN ID, Hotmail, etc. It was originally designed as a single (logical) database of identities but this was heavily criticised by privacy advocates as a security risk. The .NET Passport and Live ID solutions can also be used within the enterprise where individual privacy is not such a difficult issue. The Live ID homepage at https://accountservices.passport.net/ or http://get.live.com has more information.

CISAC

CISAC is a non-governmental, non-profit organisation that was founded in 1926 with the express goal of working towards increased recognition and protection of creators' rights. It is made up of numerous societies of authors and composers around the world (e.g. members included some 217 societies from 114 countries as of June 2006). Authors may not join CISAC directly; instead they are represented by their societies, which cover creators within all of the artistic repertoires: music, drama, literature, audiovisual works, graphic and visual arts. CISAC developed the Common Information System (CIS) with the aim of implementing a worldwide DRM system based on standardised identification of creative works and linked networks of information between the CISAC societies. The CISAC website http://www.cisac.org/ has more information.

Music Industry Integrated Identifier Project (MI3P)

CISAC and BIEM (an international mechanical rights society body that represents some 45 national mechanical rights societies in over 40 countries, see http://www.biem.org) launched the MI3P initiative to develop a global identification scheme for digital musical content in cooperation with RIAA and IFPI. MI3P was intended to design a system for identifying transactions involving sound recordings in an electronic environment, enabling the delivery of online music to consumers and the management of the associated rights. This system, which would cater for the end-users' desire for content anywhere, anytime and on any device, was to be based on a unique identifier that permanently associates the recording with its rights information. It was also meant to be interoperable with existing identification systems such as CISAC's ISWC and ISRC as well as CIS. The MI3P delivered a global infrastructure for the music industry based on a system of standardised and efficient data exchange between all of the players (music rights societies, record labels and digital service providers (DSPs)). Apart from the unique identifiers the standard also included support for messaging and reporting functionality, which is vital for every stage of music ecommerce. The main identifiers and messages are listed in Table 7.2.

TABLE 7.2 *MI3P identifiers and messages*

Name	Type	Description
MWLI – Musical Work License Identifiers	Identifier	Identifies the licences issued by the music rights societies under which musical works are being exploited
GRid – Global Release Identifiers	Identifier	Identifies the sound recordings that are released and distributed (also described above)
ELM – European Licensing Message	Message	This message is used to complete the full licensing of online rights in Europe

(continued)

Table 7.2 *(continued)*

Name	Type	Description
DSR – DSP Sales Report	Message	This is the message that specifies how sales must be reported by a DSP to a licensor
ERN – Electronic Release Notification	Message	These are the messages exchanged between record labels and DSPs to notify the availability of new releases

Digital Data Exchange (DDEX)

The DDEX was launched in 2005 with the objective of implementing the MI3P standards for music exchange and ecommerce. It is seen as the most effective way to achieve cross-industry adoption and implementation of MI3P and its charter members consist of music rights societies, record labels and DSPs including The American Society of Composers, Authors and Publishers (ASCAP), the Harry Fox Agency Inc. (HFA), The MCPS–PRS Alliance, Sociedad General de Autores y Editores (SGAE), EMI Music, SonyBMG Music Entertainment, Warner Music Group, Universal Music Group, as well as music service providers (i.e. Apple, Microsoft and RealNetworks). The MI3P founding organisations (i.e. CISAC, BIEM, IFPI and RIAA) have licensed their IPRs in MI3P to DDEX in order to better enable it to implement and deliver the business objectives of their standards. However, it is important to note the disclaimer on their website:

> DDEX is not involved in the standardisation of copy or content protections schemes, copyright protections schemes, codecs or other supporting technology. Similarly, DDEX is not involved in the standardisation of any aspect of the licensing of media content and rights (DDEX 2006)

The DDEX websites at http://www.digitaldataexchange.com and http://ddex.net/ have more information.

CONCLUSION

In this chapter we have been able to provide an overview of the various standards and organisations that have evolved in this area and which relate either directly or indirectly to DRM. We have looked at the different types of standards and their position in the standards hierarchy and examined their characteristics as well as the benefits and issues they bring to the table, including the major problem of DRM interoperability or lack thereof. This was followed by an examination of some example standards in the three DRM-related areas of identification, metadata and rights standards, followed by other types of relevant standards. Finally, we have briefly looked at some of the various standards bodies and initiatives in this space, including industry-led efforts such as MI3P and EDItEUR. Perhaps the obvious conclusion to be drawn from all of this is that there are far too many standards and not enough real effort is being focused on the wider picture of the core consumer requirement of content anywhere, anytime and on any device. However, and as observed earlier, this only confirms the difficulty in trying to marshal the dynamic forces that exist in a rapidly evolving sphere of activity such as online digital content creation, distribution and protection. The standards are themselves evolving just as rapidly as the various aspects of DRM that they are tying to influence; therefore we may not see any stabilisation until the inevitable consolidation and rationalisation of DRM technologies and products occur in the not too distant future.