PART D

STANDARDS AND LEGAL ISSUES

17

DRM Standard Activities

Xin Wang
*ContentGuard, Inc., 222 Sepulveda Blvd., Suite 1400,
El Segundo, CA 90245, USA*
Zhongyang Huang and Shengmei Shen
*Panasonic Singapore Laboratories Pte Ltd, Blk 1024,
Tai Seng Ave., #06-3530,
Tai Seng Industry Estate, Singapore 534415*

17.1 INTRODUCTION

With the advent of digital technologies, many new market opportunities have emerged for content owners, content distributors, and consumer electronics/information technology industries. An essential requirement for developing a thriving marketplace is the protection of copyrighted content in digital form. Digital Rights Management (DRM), or Intellectual Property Management and Protection (IPMP), is a collection of hardware, software, services, and technologies for that have been developed for persistently governing authorized distribution and use of content and services according to their associated rights and managing consequences of that distribution and use throughout their entire lifecycle or workflow. As DRM-enabled content, products, and services start to emerge in the consumer market, there are some problems that remain to be solved.

The first problem is the lack of interoperability among the existing DRM system offerings. Fundamentally, these systems work by encrypting content in some manner and binding the content with a set of usage rules that are used to govern the distribution and use of the content. Largely because of business arrangements, different content providers tend to use different formats and different DRM systems to protect and distribute the content. For instance, the bloom of online music distribution services, such as iTunes from Apple, Rhapsody from Real Networks, Napster and Yahoo using Microsoft products, and Vodafone Live! from Vodafone, offers legitimate audio content and provides an attractive value proposition to the consumers. However, songs purchased using one service cannot be played using other players, due to the incompatibility of the DRM-enabled content formats, the licenses for usage rules, and DRM capability requirements on the player applications and devices. This situation is expected to become worse as other major players like Sony, Microsoft, and even Wal-mart and Coca-Cola prepare to enter this online music distribution business.

The second problem of the existing DRM market is the poor renewability of DRM products. Many existing DRM systems are likely to be broken, due to the rapidly growing computer science and technology and the high interests in content of high value or popularity. This is one of the serious problems encountered in the digital content delivery business. It is therefore desirable to design and deploy robust and flexible DRM systems, where one can effectively renew broken DRM systems.

Whereas solving the renewability problem relies on the advance and evolution of DRM technologies and systems themselves, solving the interoperability problem demands open, international standardization efforts so that content can be delivered anytime, and to anywhere in the world and consumed anytime and on any device the consumer wants.

This chapter lists a number of DRM standard activities that thrive at designing robust DRM technologies and DRM systems. It starts with describing in detail the activities in the Moving Picture Experts Group (MPEG) and Open Mobile Alliance (OMA). MPEG provides a general interoperable multimedia framework and component technologies, whereas OMA focuses on a mobile industry-specific DRM system. Next, this chapter introduces briefly a few standards organizations such as the Digital Media Project (DMP), Internet Streaming Media Alliance (ISMA), Advanced Access Content System (AACS), Coral Consortium, and Digital Video Broadcasting (DVB) Project. Finally, this chapter compiles a quick reference list of DRM-related standards and consortiums, many of which are not discussed in this chapter due to space limitation.

17.2 MPEG

MPEG is a working group of ISO/IEC in charge of the development of standards for coded representation of digital audio and video. Established in 1988, the group has produced MPEG-1, the standard on which such products as video CD and MP3 are based; MPEG-2, the standard on which such products as digital television set-top boxes and DVD are based; MPEG-4, the standard for multimedia for the fixed and mobile Web; MPEG-7, the standard for description and search of audio and visual content; and MPEG-21, the Multimedia framework for end-to-end content delivery and consumption.

To ensure secure content delivery and legitimate content consumption, MPEG has been devoting significant efforts, for the last seven years, to achieving the goal of developing DRM standards that enable the functionalities of renewability and interoperability [1]. The MPEG specific term for DRM is "Intellectual Property Management and Protection", (IPMP). The latest IPMP standard for the MPEG-4 system is the MPEG-4 IPMP Extension (IPMPX) [2], the latest IPMP standard for MPEG-2 system is MPEG-2 IPMP [3, 4] (using MPEG-4 IPMP Extension Framework), and the latest IPMP efforts in MPEG-21 multimedia framework [5, 6] are IPMP Components [7], Rights Expression Language (REL) [8], and Rights Data Dictionary (RDD) [9].

The rest of this section first provides some background information for the DRM/IPMP works conducted at MPEG and then provides overviews of the MPEG extension architectures for MPEG-4/2 and the MPEG-21 IPMP Components, and the MPEG-21 REL.

17.2.1 The Need for a Flexible and Interoperable MPEG IPMP Framework

MPEG started its IPMP effort in the development of MPEG-4. The first attempt is often referred to as the "hooks" approach, where normative syntax is defined in the MPEG-4 system to allow the bitstream to carry information that informs the terminal which (of possibly multiple) IPMP system should be used to process the governed content objects in compliance with the rules declared by the content provider. The respective IPMP systems themselves were not specified within MPEG-4 [10]. MPEG-4 integrates the hooks tightly with the MPEG-4 system layer, which makes it possible to build secure MPEG-4 delivery chains in very smart and efficient ways.

This hooks model, however, appears to have many significant problems. For example, IPMP systems can be "hooked" into the MPEG-4 terminal, but it can only be done on a proprietary basis. Since the protection is normally required to be associated with some elements of the MPEG-4 terminal, and its behavior cannot be independent of other parts of the MPEG-4 terminal, if the IPMP system is not interoperable, the MPEG-4 terminal with IPMP protection would also become non-interoperable.

In the year 2000, MPEG began to address this issue of interoperability between different products, often for similar services, as developed within the IPMP framework of the MPEG-4 standard. In addition, with convergence becoming a reality, e.g., through the deployment of broadband Internet access and the start of new services on mobile channels, MPEG further put up a requirement that different types of devices and services should be able to work together to play secure digital

MPEG-4 content from multiple sources in a simple way, e.g., without the need to change the devices. This effort resulted in an extension to the MPEG-4 systems standard published in October 2002 [2].

During the progress of the MPEG-4 IPMPX, most of its architecture and concepts were applied and adopted to the MPEG-2 system. This work led to the MPEG-2 IPMP, published in March 2003 in the forms of an amendment to the MPEG-2 system [3] and a new part 11 of the MPEG-2 standard [4].

The reason for creating the MPEG-2 IPMP part is the following. The old MPEG-2 system provides hooks to proprietary Conditional Access (CA) systems for the protection of content carried in transport streams and program streams. It provides the following functionalities: (i) signaling whether particular packets have been scrambled: elementary stream or transport stream packets; (ii) sending messages to be used in (proprietary) CA systems: the Entitlement Control Message (ECM) and the Entitlement Management Message (EMM); and (iii) identifying the CA system used (under the assumption that registration authorities outside of MPEG take care that no collisions between identifiers occur).While proprietary CA systems can be integrated with the MPEG-2 audio/video technology, there are no provisions for achieving interoperability between different CA systems. The Simulcrypt system, providing a limited form of interoperability in digital television, was integrated in using these hooks with some further semantics defined in the European Digital Video Broadcast (DVB) project. It is also known that MPEG-2's provision for CA systems is not flexible, has no support for CA systems to perform watermarking and rights management, and has no support for multiple CA systems to perform on a same stream simultaneously. Moreover, the provision is not secure enough, as it does not provide good renewability of CA systems. Finally, the lack of syntax for the ECM and EMM also results in less interoperability. The MPEG-2 IPMP is designed to address the above problems, especially, the renewability and interoperability ones.

Recently, a new standardization effort has been put in MPEG to make it possible to deliver content in more interoperable, secure, and global manners. The vision for a new collection of MPEG-21 standards is to define a multimedia framework that will enable transparent and augmented use of multimedia resources across a wide range of networks and devices used by different industries and communities [5, 6]. The intent is that the framework will cover the entire multimedia content delivery chain encompassing content creation, production, delivery, and trade. The MPEG-21 standard specifications describe how these existing components can be used together and provide new models to distribute and trade digital content electronically. Naturally, DRM is a major concern in the MPEG-21 framework. As such, MPEG-21 developed its REL [8] and RDD [9], both published in April 2004, and IPMP Components [7] published in October 2005. These standards, together with others in the MPEG-21 collection such as the Digital Item Declaration, Digital Item Identification, Digital Item Adaptation, and Digital Item Processing and

Event Reporting, provide a suite of DRM components technologies that enable development of robust, flexible, interoperable, and renewable DRM systems and products.

17.2.2 Architectures for MPEG; IPMPX and MPEG-2 IPMP

Key Concepts

It is important to achieve robustness and flexibility in the interoperable framework provided by a standard. To achieve robustness, the IPMPX, provides tool renewability, which protects against security breakdown. It also provides flexibility by allowing use of various cipher tools as well as decoding tools according to system designer's choice. The IPMPX defines the following five key elements:

- **IPMP Tools**. IPMP Tools are modules that perform (one or more) IPMP functions such as authentication, decryption, watermarking, etc. A given IPMP Tool may coordinate with other IPMP Tools. Each IPMP Tool has a unique IPMP Tool ID that identifies the Tool in an unambiguous way, either at a presentation level or at a universal level.

  It is realized that it is not possible to standardize all IPMP Tools, mainly due to two reasons. The first is that different content providers may have different preferences on what IPMP Tools to use. The second reason is that there are some tools that are difficult to standardize. For example, it's not possible to standardize a video watermarking tool, as there is no watermarking algorithm that has been proven to be robust yet. With these considerations, the IPMPX is designed to differ from many prior approaches in that it intelligently provides an open secure framework allowing tools from different vendors to cooperate with each other.
- **IPMP Descriptors**. Originated from MPEG-4 Object Descriptors (OD), IPMP Descriptors describe how an object can be accessed and decoded. These IPMP descriptors are used to denote an IPMP Tool that is used to protect the object. An independent Registration Authority (RA) is used so any party can register its own IPMP tools and identify them without collisions.
- **IPMP Elementary Streams**. IPMP-specific data such as key data and rights data are carried by IPMP elementary streams. All MPEG objects are represented by elementary streams, which can reference each other. These special IPMP elementary streams can be used to convey IPMP-specific data.
- **IPMP Tool Lists**. An IPMP tool list carries the information of IPMP tools required by the terminal to consume the content. It is carried in the Initial Object Descriptor (IOD) of the MPEG-4 system stream or in the IPMP control information table in the Program-Specific Information (PSI) of the MPEG-2 system stream. This mechanism enables the terminal to select, manage the tools, or retrieve them when the tools are missing.

- **Secure Messaging Framework**. The IPMPX framework does not follow the conventional approach to define functional interfaces; instead, it is based on secure message communication. This is one of the most important concepts in the IPMPX. Interaction between the terminal and IPMP Tools is realized through messages via a conceptual entity called “message router”. The syntax and semantics of the messages are clearly defined in order to facilitate full interoperability. Mutual authentication and secure messages are also introduced to define a secure framework.

  The message-based architecture has three advantages over functional interface-based architectures. Note that the normal functional interfaces are unlikely to cover various kinds of interfaces for different algorithms, even for the same encryption function. Furthermore, the normal functional interfaces are highly dependent on the operating system and the implementation. The first advantage is that security can be more easily maintained, as messages are easier to protect in an open framework than the parameters in a function parameter list. The second is that the only entities that need to be concerned with a given message’s definition are those that need to generate or act upon a given message, so additional functionality can be created and supported simply through the addition of the required messages. The third is that full interoperability with IPMP Tools can be easily achieved by registering the messaging application programming interface(API) to an RA and carrying the registered API ID within in the IPMP descriptor or by defining a single messaging API by a third party forum which adopts the IPMPX. Note that MPEG doe not undertake the role of defining a single messaging API, since MPEG standards are mainly developed for a large number of industrial domains. Individual industrial domains should take the IPMPX as a base and fill in the gap in order to make the IPMPX truly interoperable.

MPEG-4 IPMPX Architecture

The terminal architecture within the MPEG-4 IPMPX framework is shown in Figure 17.1. The original MPEG-4 system without IPMP protection is shown at the upper half of the diagram (above the dotted line). The incoming MPEG-4 content stream is de-multiplexed in the Delivery Multimedia Integration Framework(DMIF). Audio, Video, OD, and Binary Format for Scenes(BIFS) bitstream are supplied to the Decoding Buffers (DBS) and then decoded. The decoded audio and video data are fed to the audio composition Buffer (CB) and the Video CB, respectively, and then are composed in the compositor together with the decoded ODs and the decoded BIFS tree or scene graph.

The lower half of the figure (below the dotted line) shows the modules provided by the IPMPX. The Tool List is included in the IOD of the MPEG-4 system stream to identify the IPMP tools required to consume the protected content. IPMP stream

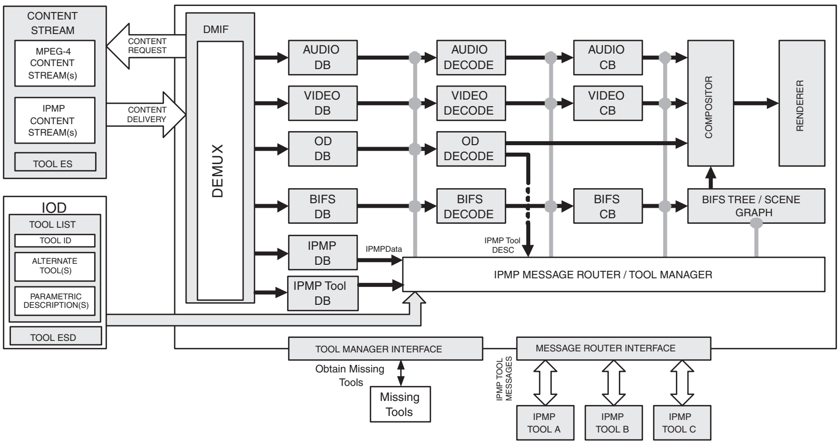

FIGURE 17.1: The MPEG-4 IPMPX terminal architecture.

arrives as an elementary stream multiplexed in the MPEG-4 system stream. Note that the Tool list and the IPMP stream are constructed during the content authoring process. The Tool Manager (a conceptual entity) manages IPMP Tools within the terminal (e.g., downloading a missing tool from a remote location), while the message router routes messages among the terminal and the IPMP tools using a secure messaging framework to ensure that different IPMP Tools from different vendors can work together. IPMP tools can act on several control points, which are positions along the dataflow where the IPMP tool functions by taking over the protected content bitstream, processing it, and returning it back to the control point for subsequent processing of the content by the MPEG-4 terminal. The supported control points are dictated by the gray circles in the architecture diagram. For example, an encrypted MPEG-4 video stream needs to be decrypted by an IPMP tool (decryptor) at the control point right before the video decoder, and a watermark reader may need to be applied to the watermarked audio stream at the control point right after the audio decoder. If necessary, an IPMP tool can be applied to the control points right before the compositor to control the rendering process.

MPEG-2 IPMP Architecture

The new MPEG-2 IPMP framework is depicted in Figure 17.2. The tool list, tool container, and rights container are included in the IPMP control information table which is part of the PSI. An IPMP stream arrives as an elementary stream multiplexed in an MPEG-2 transport or program stream. The tool manager manages IPMP tools within the terminal, while message router routes messages among the terminal and IPMP tools. The incoming content is de-multiplexed by the MPEG-2

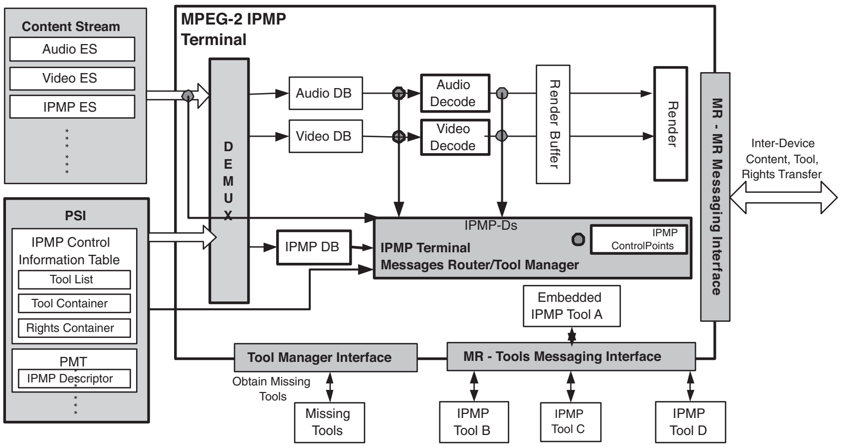

FIGURE 17.2: The MPEG-2 IPMP terminal architecture.

system DeMux. Audio and video bitstreams are supplied to the DB and then decoded and rendered. IPMP tools can act on several control points as dictated by gray circles.

17.2.3 Features of the IPMPX Architecture

The IPMPX architecture has several important features:

- **Interoperability**. The IPMP extension standardizes IPMP messages and the process of message routing. By using a common set of IPMP messages, together with some industry defined messaging API and messages extension, different IPMP Tools can be easily plugged into the terminal and can interact with each other.
- **Renewability**. Through the usage of the tool list and IPMP descriptor, one can easily renew a tool for better IPMP protection by, e.g., indicating to the terminal that a new tool is needed, carrying the new tool in the tool elementary stream in the content stream, or downloading the new tool from somewhere. Note that tool downloading is not mandatory in IPMP; rather, IPMP provides the architecture to facilitate tool downloading.
- **Flexibility**. The IPMPX does not standardize IPMP tools. With the support of independent registration authorities, the ability to carry tools inside the content stream, and the terminal's potential capability to download required IPMP Tools from a remote location, one can choose whatever tools to perform decryption, watermarking, user authentication, or integrity checking.
- **Dynamic Operation**. Various IPMP tools can be signaled in the content with the help of the IPMP descriptor, control point, and sequence code. Different

tools can operate at the same or different control points, acting on the same or different streams.

- **Tool Security**. The terminal and tools can choose to perform mutual authentication using the IPMP authentication messages to achieve a secure communication framework.

17.2.4 MPEG-21 IPMP Components

Without standardalizing a specific system used to deliver the multimedia content like the MPEG-2/4 systems, the MPEG-21 multimedia framework covers the entire multimedia content delivery chain encompassing content creation production, delivery, and trade. The MPEG-21 IPMP Components specification describes the technologies for effectively managing and protecting the digital content. It specifies how protection is applied to content captured as Digital Items in the MPEG-21 Digital Item Declaration Language (DIDL) [11] and facilitates the exchange of governed content between MPEG-21 peers. The basic concepts such as tool list, IPMP tools, and IPMP Descriptor defined in the MPEG-2/4 IPMPX framework are utilized to retain the features of the IPMPX architecture mentioned in Section 17.2.3, but without defining the messaging infrastructure in the MPEG-2/4 IPMPX.

Figure 17.3 illustrates how content is described and protected using the MPEG-21 IPMP within the multimedia content delivery chain.

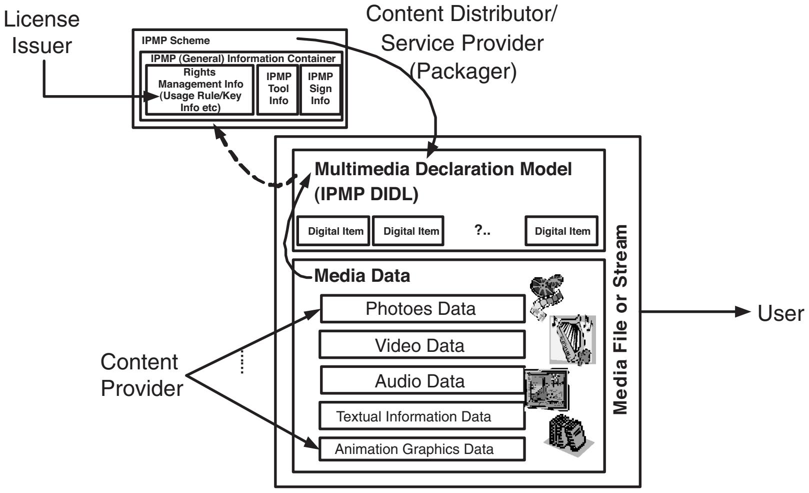

FIGURE 17.3: Block diagram of content creation, distribution, and protection using the MPEG-21 IPMP.

During the digital content creation stage, the content provider supplies the valuable media data which may include all kinds of digital media resources (photos, video, audio, text, animation, graphics, etc.) to the content distributor or service provider. The structure and content of the media data are unambiguously expressed as a Digital Item. As the Digital Item expressed in the DIDL is a clear XML document, the information of the Digital Item represented in the DIDL is all exposed. The MPEG-21 IPMP provides an alternative representation for parts of a Digital Item that require protection and governance. The language for defining this representation is termed as the IPMP DIDL. The language defines governed XML elements in correspondence to entities in the model of digital items. Each of these IPMP DIDL elements is indented to link a corresponding DIDL element (which may be encrypted) with IPMP information about the governance so that the Digital item hierarchy thus represented is used in accordance with the Digital Item author's wishes.

The model provided by the IPMP DIDL can be used to package content together with its associated actual media data to form the digital representation of a work (for example, a digital music album, an e-book, or a piece of software including setup and configuration information). The two most useful and prominent application forms of such a digital work are file and stream that are to be received by the user.

At the same time, the content owner, provider, or distributor can create the scheme description data, IPMP Scheme, that is related to security, protection, and governance of the content. The IPMP Scheme is an IPMP information container and includes not only IPMP tool (capability) information and IPMP signature information, but also the rights management information (e.g., usage rule and key information) that is created by a license issuer and carried inside the IPMP scheme. The description of the IPMP governance and tools is required to satisfy intellectual property management and protection for the Digital Item or its parts to be accessed. The IPMP Scheme can either be placed directly inside the IPMP DID model or be indirectly referred to the declaration model by some means such as Universal Resource Identifier(URI). It is noted the media data input to a file or stream can be in different forms (in encrypted, watermarked, or other formats) as long as the IPMP scheme is associated. Based on the extracted IPMP scheme, the MPEG-21 terminal should convert the protected media data into the clear forms for content consumption or further distribution, if all rights conditions are fulfilled and all required data (e.g., keys) are available.

17.2.5 MPEG-21 REL

In order to develop effective and efficient DRM systems, the capability of specifying and communicating rights information among the participants is certainly required at each step of content delivery and consumption. A content user needs to know what rights are associated with a piece of content. A content distributor needs not only to communicate the rights that are available for consuming the content, but also to understand the rights that pertain for distributing the content. More importantly, a content provider in the upstream of the supply-distribution-consumption value-chain needs to ensure that both usage and distribution rights are granted precisely as intended for every participant in the content delivery chain. With rights properly specified, DRM systems can then correctly interpret them and effectively enforce them.

The MPEG-21 REL [8, 12], published in April 2004 together with the MPEG-21 RDD [9], is an XML-based developed from the ContentGuard's eXtensible rights Markup Language (XrML) version 2.0 [13] that can be used to declare rights and conditions using the action terms as defined in the RDD, as the RDD is developed to ensure that the semantic interpretation of each right be precise and unambiguous in order to promote interoperability at the rights level. Using the REL, anyone owning or distributing content can identify some principals (such as users, groups, devices, and systems) allowed to use the content, the rights available to those principals, and the terms and conditions under which those rights may be exercised.

For example, consider a movie, Ocean Wild, distributed by a studio, Acme Studio, to the owner of a DVD player, called Alice. A typical MPEG-21 REL expression might make the statement, Under the authority of Acme Studio, Alice is granted the right to play "Ocean Wild during the month of November 2003." In the MPEG-21 REL terminology, Alice is considered as a "principal," play is a "right," the movie "Ocean Wild" is a "resource," "during November 2003" is a "condition," and Acme Studio is an "issuer" of the right. While the example is simple, it captures the essence of every MPEG-21 REL expression, as shown in the REL data model in Figure 17.4. The right-granting portion of this statement ("Alice is granted with the right to play 'Ocean Wild' in the month of November 2003") is called a "grant," and the entire statement is called a "license," which in this case consists of the grant and the issuer, Acme Studio.

MPEG has developed its REL to meet the requirements it defined, especially those on unambiguous semantics and comprehensiveness in supporting identified bussiness models. Nevertheless, MPEG recognizes that several industries and communities will need to modify the language to better meet their specific needs. To facilitate easy mapping of the REL to these industry-specific applications, the MPEG REL has been designed in a way that can be profiled as well as extended. Profiling the REL allows selection of only the parts of the language applicable to a target application. This enables optimizing the payload of digital items and computation requirements of MPEG terminals. On the other hand, extending the REL allows the introduction of new types and elements to the language based on particular application needs. This includes the development of new verbs and schematic elements to improve efficiency in a specific domain. It is important to note that profiling and extending can be used concurrently to optimize the applicability of

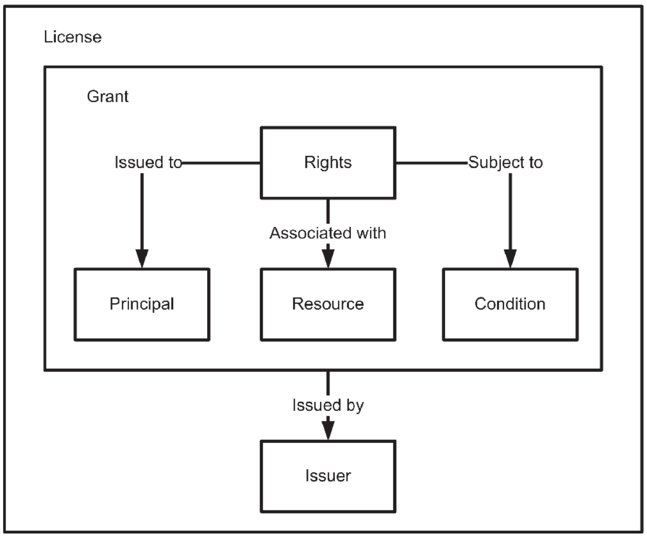

FIGURE 17.4: The MPEG REL data model.

the REL to one specific application. Currently, MPEG is developing a number of REL profiles and extensions for application domains like mobile, optical media, and broadcasting. Some of the resulting profile specification will be published in mid-2006 or early 2006.

17.3 OMA

OMA is an industry standard organization for developing mobile service enabler specification work, in order to stimulate and contribute to the creation of interoperable services. The organization goals of OMA include (1) delivering quality, open technical specifications based upon market requirements that drive modularity, extensibility, and consistency, and (2) enabling interoperability across different devices, geographies, service providers, operators, and networks [14].

Clearly, downloading content to a mobile phone or receiving content by messaging services has become one of the most popular mobile data services. The typical content consumed by a mobile device today includes limited value content types such as ringtones, screensavers, and background images. As new smartphones and other smart devices penetrate the market, and mobile network capacities increase, a demand for a wider range of new and higher value content types (music, game, movies, etc.) is emerging and expanding the digital content market. OMA began working on mobile DRM specifications in late 2001 in response to the clear market demand.

DRM systems must play different roles depending on the time value of information. Some simple digital resources are primarily considered for protection in the OMA release 1.0 DRM solution. Some valued digital resources are also considered to use separate delivery (superdistribution) to protect in some simple cases. The OMA DRM technology release 1.0 finalized in December 2002 is an initial protection system that can be extended into a more comprehensive and secure DRM system. From a security point of view, the OMA DRM release 1.0 is quite lightweight. The rights object or the Content Encryption Key (CEK) carried within is not protected. The device or the DRM agent is not authenticated prior to issuing rights. All this makes it relatively easy to circumvent the DRM protection. OMA continued its effort to work on its 2.0 release, which is trying to include a more sophisticated trust and security model. The latest OMA DRM release 2.0 was issued in March 2006, and recently, the OMA DRM group is also working on the solution for mobile broadcasting content protection.

17.3.1 OMA DRM V1.0

OMA DRM version 1.0 Enabler Release was created as a solution that was timely and inexpensive to deploy, could be implemented in mass market mobile devices, and should not require costly infrastructure to be rolled out. The scope of this standard is to enable the controlled consumption of digital media objects by allowing content providers to express usage rights, e.g., the ability to preview DRM content, to prevent downloaded DRM content from being illegally forwarded to other users, and to enable superdistribution of DRM content.

OMA DRM v1.0 includes three levels of functionality:

- Forward-lock: preventing content from leaving device. The purpose of forward-lock is to prevent peer-to-peer distribution of low-value content. This applies often to subscription-based services such as news, and sports clips. The plaintext content is packaged inside a DRM message that is delivered to the terminal. The device is allowed to play, display, or execute the content, but it is not allowed to forward the content.
- Combined delivery: adding rights definition. Combined delivery equally prevents peer-to-peer distribution, but it also controls the content usage. In combined delivery, the DRM message contains two objects: the content and a rights object. The rights object defines permissions and constraints for the use of the content. These can be, for example, a permission to play a tune only once or to use the content only for x number of days. Neither content nor the rights object is allowed to be forwarded from the target device.
- Separate Delivery: providing content encryption and supports superdistribution. The purpose of Separate Delivery is to protect higher value content.

It enables the so called superdistribution, which allows the device to forward the content, but not the usage rights. This is achieved by delivering the media and usage rights via separate channels. The content is encrypted into DRM Content Format (DCF) using symmetric encryption; the DCF provides plaintext headers describing content type, encryption algorithm, and other useful information. The rights object holds the symmetric CEK, which is used by the DRM user agent in the device for decryption. The rights object is defined using OMA REL.

Superdistribution is an application of separate delivery that also requires a rights refresh mechanism that allows additional rights for the media. Recipients of superdistributed content must contact the content retailer to obtain rights to either preview or purchase the media. Thus, the separate delivery method enables viral distribution of media, maximizing the number of potential customers while retaining control for the content provider through centralized rights acquisition.

17.3.2 OMA DRM V2.0

OMA DRM version 2.0 enabler release [15] was created to meet the new requirements to support more valuable content (e.g., video, music, games, etc.), which requires a more complicated key management infrastructure to provide more security. The scope of this release is to enable the controlled consumption of digital media objects by allowing content providers the ability, for example, to manage previews of protected content, to enable superdistribution of protected content, and to enable transfer of content between DRM agents. The OMA DRM 2.0 specifications provide mechanisms for secure authentication of trusted DRM agents and for secure packaging and transfer of usage rights and DRM-protected content to trusted DRM agents.

OMA DRM v2.0 includes three main technical parts in its specification [15]:

- **OMA DCF**. This part is to define the content format for DRM-protected encrypted media objects and associated meta-data. The DCF can be delivered separately from an associated rights object, which contains the encryption key used to encrypt the media object. There are two DCF profiles. One is used for discrete media (such as still images), and one is used for continuous media (such as music or video). The profiles share some data structures. Both profiles are based on a widely accepted and deployed standard format, the ISO base media file format. But the discrete media profile is meant to be an all-purpose format, not aiming for full compatibility with ISO media files.
- **OMA DRM system**. The OMA DRM system enables content issuers to distribute protected content and rights issuers to issue rights objects for the protected content. The DRM system is independent of media object formats, operating systems, and runtime environments. In order to consume

the content, users acquire permissions to protected content by contacting rights issuers. Rights issuers grant appropriate permissions, in the form of rights objects, for the protected content to user devices. The content is cryptographically protected when distributed; hence, protected content will not be usable without an associated rights object issued for the user's device.

The protected content can be delivered to the device by any means (over the air, LAN/WLAN, local connectivity, removable media, etc.). But the rights objects are tightly controlled and distributed by the rights issuer in a controlled manner. The protected content and rights objects can be delivered to the device together, or separately.

This part defines an end-to-end system for protected content distribution. The Rights Object Acquisition Protocol (ROAP), the key management schemes utilized, and the domain-related functionalities in OMA DRM are described in detail in different sections of this part.

- **OMA REL**. Rights are used to specify the access a consuming device is granted to DRM-governed content. The REL defined in this part specifies the syntax and semantics of rights governing the usage of DRM content. It is based on a subset of the Open Digital Rights Language (ODRL) [16] version 1.1, together with a data dictionary defining additional permissions and constraints beyond those provided by ODRL. DRM-governed content is consumed according to the specified rights. Therefore, the value is in the rights and not in the content itself. Rights objects are specified so that they only become usable on authorized devices.

17.4 CORAL

Founded in late 2004, Coral Consortium is an industry consortium chartered to promote interoperability between DRM technologies for consumer devices and services, so digital music and video can be easily accessed and enjoyed, regardless of the service provider or the device. Coral recognizes the fact that, while recent innovations in digital media distribution provide consumers with new channels to acquire music and video, proprietary differences still exist and will probably continue to exist in underlying DRM or content protection technology that prevent consumers from playing content packaged and distributed using one DRM technology on a device that supports a different DRM technology. Its focus is to define a service provider architecture that allows existing DRM systems to co-exist, and it provides necessary protocols and interfaces to bridge these DRM systems to enable interoperability between different content formats, devices, and content distribution services. Though Coral announced availability of the consortium's 1.0 interoperability specification in March 2005, a full Coral specification is still under development.

Closely related to Coral Consortium is another consortium called the Marlin Joint Development Association (or Marlin JDA), which was formed in early 2005. Unlike Coral, Marlin's objective is to provide a DRM technology toolkit to enable device makers to build DRM functions into their portable digital media devices. The connection between the two consortiums is that the Marlin JDA's specifications are intended to be compatible with the Coral Consortium's services-based specifications in a way that Marlin-based devices will be able to interoperate with Coral-enabled DRM systems even if those systems do not use Marlin DRM components.

17.5 DMP

DMP is a non-profit association, launched in mid-2003, to develop technical specifications for promoting the development, deployment, and use of digital media. The Interoperable DRM Platform, phase I (IDP-1) specification was published in May 2005, enabling the implementation of digital media services based on portable audio and video devices. The phase II specification is currently under development.

The DMP specifications are designed to provide interoperability between value-chain players of governed (i.e., DRM protected) digital media within and between value-chains that exist as well as those expected in the future. To support interoperability in such a dynamic environment, DMP considers that the only practical solution is to provide standardized DRM technologies that value-chain users can configure to suit their needs. The interoperable DRM Platform (IDP) is the assembly of standardized technologies that DMP calls tools. These tools are grouped into the following seven major categories.

- Represent. Tools to represent content, keys, and rights expressions (or licenses).
- Identify. Tools to identify content, licenses, devices, and domains.
- Package. Tools to package content in files or streams.
- Authenticate. Tools to recognize and enable trust between devices and users using certificates, identification data, and certificate proxies.
- Manage. Tools to manage domains for domain establishment, membership management, and content usage control.
- Access. Tools to access and update content and licenses.
- Process. Tools to transform XML documents to their binary format version before transmission or storage and to perform encryption and decryption functions.

The standardized DRM technologies promoted by DMP are mainly from MPEG-21 [5, 6], including the Digital Item Declaration (DID), Digital Item Identification (DII), IPMP components, REL, RDD, and file format.

DMP just released, in February 2006, its IDP phase-II (IDP-II) technical specifications and references designed to support the implementation of value chain centered around stationary audio and video devices, i.e. devices with network access.

17.6 ISMA

Founded in 2000, the ISMA is an industry alliance dedicated to the adoption and deployment of open standards for streaming rich media such as video, audio, and associated data over Internet protocols.

The technical requirements of ISMA DRM can be understood in the context of the archetypal server-client-based DRM architecture shown in Figure 17.5. The MASTERING entity is where a content work is prepared for dissemination. It may be encrypted and associated with a rights specification that is formatted according to an REL (e.g., [8, 15]). The KEY/LICENSE MGT entity associates a rights specification and cryptographic keys with an ISMA content work. It translates the rights specification into a license. The license authorizes particular types of access to the work, possibly according to a set of "business rules." The access may be at a highly granular level of access such as to view/hear the content, write to a DVD, or send to a friend. The SENDER entity manages the requests from receivers (labeled "CONTROL") and disseminates content works ("MEDIA") to receivers; both CONTROL and MEDIA flows may use encryption, authentication, and integrity services. The RECEIVER entity decrypts and authenticates content works contained in the MEDIA flow and may decrypt and

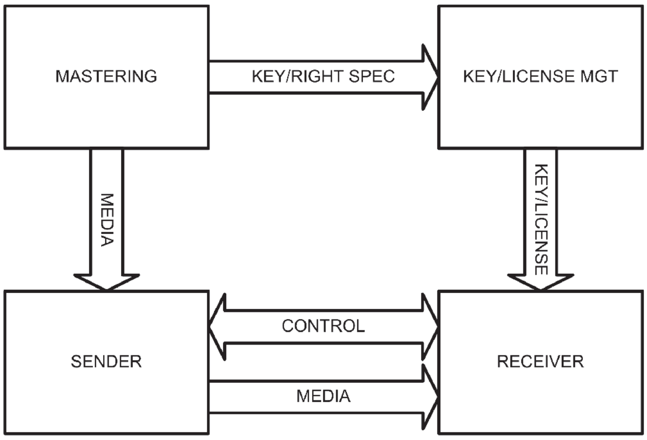

FIGURE 17.5: ISMA DRM architecture.

authenticate CONTROL flows. Depending on the nature of the key/license management protocol in use, the RECEIVER may perform mutual authentication with the KEY/LICENSE MGT entity to prove that the receiver is an authorized platform. This process is controlled by the license, which specifies the terms and conditions under which a key is provided to an ISMACryp device [8, 15]. The license determines what authenticating information is exchanged, such as information about the RECEIVER's hardware, software, or human user.

The latest ISMA DRM specification is officially named Internet Streaming Media Alliance Encryption and Authentication (ISMACryp), Version 1.1. It includes the following features:

- Payload encryption and message authentication for ISMA 1.0 and ISMA 2.0 streams, including AVC/HE-AAC
- Encryption of ISMA 1.0- and 2.0-based files
- Extensible framework allowing combinations of various DRM systems
- Guidelines for combination with OMA DRM version 2 systems

The ISMACryp is being recommended by DVB-H (Digital Video Broadcasting for Handhelds), which is a standard for mobile TV devices embraced by the international European Telecommunication Standards Institute (ETSI) body. Future ISMA specifications will build on ISMACryp and define a complete DRM system that is possibly integratable with multiple key/license management systems.

17.7 AACS

AACS is an industry standard consortium aimed at developing a set of specifications for managing content stored on the next generation of pre-recorded and recorded optical media for consumer use with PCs and CE devices. AACS specifications complement the next generation of high-definition optical discs such as HD-DVD and Blu-Ray.

AACS utilizes advanced cryptography and flexible usage rules to protect and authorize the use of digital media. AACS-protected content is encrypted, via a broadcast encryption scheme [17], under one or more title keys using the Advanced Encryption Standard (AES) [18]. Title keys are derived from a combination of a media key and several elements, including the volume ID of the media (e.g., a physical serial number embedded on a DVD) and a cryptographic hash of the title usage rules. The AACS broadcast encryption-based approach provides a much more effective mechanism for device revocation than earlier content protection systems such as the Content Srambling Systems (CSS) used in the DVD protection [19].

By specification of title usage rules, AACS is flexible to support new distribution and business models for content and service providers, as well as to improving functionality and interactivity for the consumer. For example, AACS supports the ability to grant the users rights, to the extent authorized by title usage rules, to save licensed, protected copies of pre-recorded movie titles onto, for example, a portable player, a desktop PC, or authorized media, while preventing unauthorized reproduction and distribution of next-generation optical media.

17.8 LIST OF DRM STANDARD ORGANIZATIONS AND CONSORTIUMS

Due to the space limitation of this chapter, many DRM-related standard activities have not been discussed. This section, nevertheless, provides a quick reference list of DRM standard organizations and consortiums in addition to those discussed in the previous sections. It should be pointed out that this list is by no means a complete one. This is partially because the limited standards participation and personal views of DRM from the authors and the DRM technologies and applications are still evolving and expanding.

- 4C Entity (4C)
  - URL: http://www.4centity.com
  - Scope: Recordable and Removable Media
  - Work: Content Protection
- Advanced Access Content System (AACS)
  - URL: http://www.aacsla.com
  - Scope: Pre-Recorded and Recordable High-Definition Media
  - Work: Content Protection and Usage Rules-Based Control
- ATIS IPTV Interoperability Forum (ATIS/IIF)
  - URL: http://www.atis.org/iif/index.asp
  - Scope: IPTV Interoperability
  - Work: Requirements and DRM systems
- Audio Video Coding Standard Workgroup of China (AVS)
  - URL: http://www.avs.org.cn/
  - Scope: Audio-Video Technologies and Systems
  - Work: DRM Framework, Rights Expression Language, and Communication Protocols
- ChinaDRM
  - URL: http://www.chinadrm.org.cn
  - Scope: Broadcasting
  - Work: DRM Requirements, Testing Platform, and Technologies

- Copy Protection Technical Working Group (CPTWG)
  - URL: http://www.cptwg.org
  - Scope: Consumer Electronics
  - Work: Copy Protection
- Coral Consortium
  - URL: http://www.coral-interop.org
  - Scope: Consumer Electronics
  - Work: Service-based Architecture and Implementations
- Digital Media Project (DMP)
  - URL: http://www.chiariglione.org
  - Scope: Interoperability Framework
  - Work: Interoperable DRM Platform
- Digital Transmission Content Protection (DTCP, 5C)
  - URL: http://www.dtcp.com
  - Scope: Digital Transmission
  - Work: Content Protection
- Digital Video Broadcasting (DVB) Project
  - URL: http://www.dvb.org
  - Scope: Video Broadcasting
  - Work: Content Protection and Content Management, Usage State Information
- IEEE Learning Technology Standards Committee
  - URL: http://ltsc.ieee.org/wg4/
  - Scope: Electronic Learning
  - Work: Use Cases and Requirements for Rights Expression Languages
- International Digital Publishing Forum (IDPF, formerly OeBF)
  - URL: http://www.idpf.org/
  - Scope: Electronic Publications
  - Work: Rights Expression Language, Publication Specification, Metadata, and Container
- Internet Streaming Media Alliance (ISMA)
  - URL: http://www.isma.tv/

  - Scope: Internet Streaming
  - Work: Authentication and Encryption, Integrated DRM System
- ISO/IEC Moving Picture Experts Group (MPEG)
  - URL: http://www.chiariglione.org/mpeg/
  - Scope: Multimedia Framework and Supporting Component Technologies
  - Work: Intellectual Property Protection and Management, Rights Expression Language, Rights Data Dictionary, Digital Item Declaration, Digital Item Identification, Digital Item Adaptation, Digital Item Processing, Digital Item Streaming, File Format, and Event Reporting
- Open Mobile Alliance (OMA)
  - URL: http://www.openmobilealliance.org
  - Scope: Mobile Communication
  - Work: Mobile DRM System, Protocols, and Rights Expression Language
- Secure Video Processor (SVP) Alliance
  - URL: http://www.svpalliance.org
  - Scope: Digital Home Networks and Portable Devices
  - Work: Content Protection Technology
- Society of Motion Picture and Television Engineers (SMPTE)
  - URL: http://www.smpte.org
  - Scope: Digital Cinema
  - Work: Security and Rights
- TV-Anytime Forum
  - URL: http://www.tv-anytime.org
  - Scope: Audio-Visual Services
  - Work: Rights Management and Protection Information

REFERENCES

[1] L. Chiariglione. Intellectual property in the multimedia framework, in *Management of Digital Rights*, October 2000, Berlin.

[2] ISO/IEC. MPEG-4 system on IPMP extension, *Amendment 3*, Shanghai, China, October 2002.

[3] ISO/IEC. MPEG-2 system: Support of IPMP on MPEG-2 systems, *Amendment 2*, Pattaya, Thailand, March 2003.

[4] ISO/IEC. IPMP on MPEG-2 systems, First Edition, Pattaya, Thailand, March 2003.

[5] J. Gelissen, J. Bormans, and A. Perkis. Mpeg-21: The 21st century multimedia framework, *IEEE Signal Processing Magazine*, 20:53–62, March 2003.

[6] I. Burnett, R. Van de Walle, K. Hill, J. Bormans, and F. Pereira. MPEG-21: Goals and achievements, *IEEE Multimedia*,10:60–70, October – December 2003.

[7] ISO/IEC. Information technology — multimedia framework — Part 4: Intellectual property management and protection components, First Edition, Busan, Korea, April 2005.

[8] ISO/IEC. Information technology — multimedia framework — Part 5: Rights expression language, First Edition, Munich. Germany, April 2004.

[9] ISO/IEC. Information technology — multimedia framework — Part 6: Rights data dictionary, First Edition, Munich, Germany, April 2004.

[10] ISO/IEC. MPEG-4 intellectual property management and protection (IPMP) overview and applications, First Edition, Rome, Italy, December 1998.

[11] ISO/IEC. Information technology — Multimedia framework — Part 2: Digital Item Declaration, Second Edition, Hong Kong, China, January 2005.

[12] X. Wang, T. DeMartini, B. Wragg, M. Paramasivam, and C. Barlas. The MPEG-21 rights expression language and rights data dictionary, *IEEE Trans. Multimedia*, 7:408–417, June 2005.

[13] ContentGuard, Inc. eXtensible rights Markup Language (XrML), Version 2.0, http://www.xrml.org, November 2001.

[14] OMA. OMA DRM Short Paper, http://www.openmobilealliance.org, 2003.

[15] OMA. OMA DRM release 2.0 enabler package, http://www.openmobilealliance.org, March 2006.

[16] ODRL Initiative. Open Digital Rights Language (ODRL), Version 1.1, http://www.odrl.net, August 2002.

[17] A. Fiat and M. Naor. Broadcast encryption, *Lecture Notes in Computer Science*, 773:480–491, 1994.

[18] National Institute of Standard and Technology. Advanced Encryption Standard (AES), *FIPS*, 197:2001.

[19] J. A. Bloom, I. J. Cox, T. Kalker, J.-P. M. G. Linnartz, M. L. Miller, and C. B. S. Traw. Copy portection for DVD video, *Proc. IEEE*, 89:1267–1276, July 1999.