INTERNATIONAL ORGANISATION FOR STANDARDISATION
ORGANISATION INTERNATIONALE DE NORMALISATION
ISO/IEC JTC 1/SC 29/WG 11
CODING OF MOVING PICTURES AND AUDIO

ISO/IEC JTC 1/SC 29/WG 11 N10684
Maui, HI, US – April 2009

Source: **System**
Title: **MPEG Intellectual Property Management and Protection**

MPEG Intellectual Property Management and Protection

Table of Contents

1 Introduction

As can be seen from the lists in Sections 2 and 3 of this document, since its early days MPEG has developed a range of standards related to Intellectual Management and Protection (IPMP), an enabler of ways of doing business with digital media.

Even though the term Digital Rights Management (DRM) is more commonly used nowadays, MPEG prefers to stick to its name IPMP. One reason is that there is no universally accepted definition of "DRM"[1] and another is that the common use of "DRM" is often associated with "protection" while the MPEG name explicitly separates Management from Protection. Indeed some MPEG IPMP standards are designed for "management" of Intellectual Property and some others for "protection" as well to respond to the needs of a broad variety of applications.

Additional information about MPEG can be found at htt://mpeg.chiariglione.org/.

2 An overview of MPEG standards

In the table below the list of MPEG standards is provided.

ISO No.	Acronym	Title
11172	MPEG-1	Coding of moving pictures and associated audio at up to about 1.5 Mbit/s
13818	MPEG-2	Generic coding of moving pictures and associated audio
14496	MPEG-4	Coding of audio-visual objects
15938	MPEG-7	Multimedia Content Description Interface
21000	MPEG-21	Multimedia Framework
23000	MPEG-A	Multimedia Application Formats
23001	MPEG-B	MPEG Systems Technologies
23002	MPEG-C	MPEG Video Technologies
23003	MPEG-D	MPEG Audio Technologies
23004	MPEG-E	MPEG Multimedia Middleware
23005	MPEG-V	Media Context and Control
23006	MPEG-M	MPEG Extensible Middleware
23007	MPEG-U	MPEG Rich Media User Interface
29116		Supplemental Media Technologies

MPEG-1 is the standard designed for interactive video on Compact Disc and Digital Audio Broadcasting. There are no IPMP-related technologies in MPEG-1.

MPEG-2 is the standard designed to support the transition of analogue television to digital. IPMP-related technologies can be found in the following parts:

Part 1	Systems
Part 2	Video
Part 11	IPMP on MPEG-2 Systems

[1] The National Institute of Standards and Technology (NIST) defines Digital Rights Management (DRM) as a system of Information Technology (IT) components and services along with corresponding law, policies and business models which strive to distribute and control Intellectual Property (IP) and its rights.

MPEG-4 is huge collection of multimedia related standards (currently there are 27 parts in MPEG-4). IPMP-related technologies can be found in the following parts:

Part 1	Systems
Part 11	Scene Description and Application Engine
Part 13	IPMP Extensions

MPEG-7 is a standard for description of video, audio and multimedia content. The following part is directly relevant to IPMP:

Part 5	Multimedia Description Schemes

MPEG-21 is a standard for "Multimedia Framework". It is based on the definition of Digital Item, a structured digital object with a standard representation, identification and metadata. IPMP-related technologies can be found in the following parts:

Part 1	Vision, Technologies and Strategy
Part 2	Digital Item Declaration
Part 3	Digital Item Identification
Part 4	IPMP Components
Part 5	Rights Expression Language
Part 6	Rights Data Dictionary
Part 11	Evaluation Tools for Persistent Association
Part 15	Event reporting
Part 19	Media Value Chain Ontology

MPEG-A is a collection of standards defining application-specific formats. Some of these formats provide IPMP support, namely

Part 2	Music Player Application Format
Part 4	Musical Slide Show Application Format
Part 5	Media Streaming Application Format
Part 6	Professional Archival Application Format
Part 7	Open Access Application Format
Part 9	Digital Multimedia Broadcasting Application Format

MPEG-B, -C and -D are collections of Systems, Video and Audio related standards, respectively. The following part of MPEG-B is directly relevant to IPMP:

Part 3	XML Representation of IPMP-X messages

MPEG-E is a collection of middleware standards. The following part of MPEG-E is directly relevant to IPMP:

Part 2	Multimedia API

MPEG-V is a collection of standards for the exchange of information with Virtual Worlds. Currently no IPMP support is planned.

MPEG-M is a collection of standards designed to promote the extended use of digital media content through increased interoperability and accelerated development of components, solutions and applications. All parts of this standard relate to IPMP:

Part 1	Architecture and Technologies
Part 2	Application Programming Interface
Part 3	Reference Software and Conformance

MPEG-U is a collection of standards to support a Rich Media User Interface. Currently no IPMP support is planned.

Examples of use of MPEG standards are given in the list below:

- **Video CD** is the precursor of the DVD. It uses MPEG-1 Systems, Video and Audio Layer II to store one hour of video on a Compact Disc.
- **Digital Audio Broadcasting** uses MPEG-1 Audio Layer II to broadcast stereo audio via radio.
- **MPEG-1 Audio Layer II** is also widely used in digital television set top boxes.
- **MPEG-1 Audio Layer III (MP3)** is the quasi-universal choice for portable music.
- **MPEG-2 Systems** (Transport Stream) and **MPEG-2 Video** are almost universally used for digital television set top boxes.
- **MPEG-2 Systems** (Program Stream) and **MPEG-2 Video** are almost universally used for Digital Versatile Disc (DVD).
- **MPEG-2 Advanced Audio Coding** is used in Japanese digital television set top boxes.
- **MPEG-4 Visual** (Simple Profile) is used in most mobile handsets.
- **MPEG-4 Visual** (Advanced Simple Profile) is used to compress video material on Compact Disc.
- **MPEG-4 Audio** in various versions is used in many products (portable music players, mobile handsets etc.).
- **MPEG-4 Advanced Video Coding** is being used in a broad range of products (set top boxes, mobile handsets, portable video players etc.).
- **MPEG-4 Binary Format for Scene** (BIFS) is used in Digital Multimedia Broadcasting (DMB).
- **MPEG-4 File Format** is used in a variety of application domains, notably to store and exchange video files taken by mobile handsets.
- Elements of **MPEG-4 Animation Framework eXtension** (AFX) are used in mobile games.
- **Lightweight Application Scene Representation** (LASeR) is used in mobile handsets.
- Elements of **MPEG-7** are used in several commercial applications and referenced by the TV Anytime specifications.
- **MPEG-21 Digital Item Declaration** (DID) is used in commercial products.
- Several parts of **MPEG-21** have been adopted by the Digital Media Project (DMP) for their open source Chillout® Interoperable DRM Platform.

3 Summary of MPEG IPMP-Related Technologies

Standard	Technology	Brief Description
13818-1	EMM/ECM	Special messages that can be used to convey Access Control information

13818-1/-2/-3	Copyright Identifier	A field conveying the identifier of the audio, video and audio-video stream
13818-11	IPMP-X	MPEG-2 IPMP eXtension provides the means to transmit and build an IPMP System at an MPEG-2 decoder
14496-1	IPI	The Intellectual Property Identification data set, carries information about the contents, type of content and (pointers to) rights holders.
14496-11	IPMP	Intellectual Property Management and Protection standardises IPMP-Descriptors and IPMP-Elementary Streams
14496-13	IPMP-X	MPEG-4 IPMP eXtension provides the means to transmit and build an IPMP System at an MPEG-4 decoder
21000-1	MPEG-21 Multimedia Framework: Vision, Technologies and Strategy	This Technical Report has been written to describe the MPEG-21 multimedia framework and its architectural elements together with the functional requirements.
21000-2	DID	Digital Item Declaration describes a set of abstract terms and concepts to form a useful model for defining Digital Items.
21000-3	DII	Digital Item Identification specifies how to uniquely identify Digital Items and parts of Digital Items
21000-4	IPMP Components	IPMP Components specifies how to include IPMP information and protected parts of Digital Items in a Digital Item Declaration Language (DIDL) document
21000-5	REL	The MPEG-21 Rights Expression Language allows to declare rights and permissions using the terms as defined in the Rights Data Dictionary (RDD)
21000-6	RDD	RDD is a set of terms that can be used in MPEG-21 REL
21000-11	Evaluation Tools for Persistent Association	ETPA sets out a process and plan for evaluating Persistent Association Technologies, e.g. watermarking and fingerprinting
21000-15	Event Reporting	ER specifies the syntax and semantics of • Event Report Requests (ERR) about which Events to report, what information is to be reported and to whom • Event Reports (ER) created by an MPEG-21 Peer in response to an ERR when the conditions specified by an ERR are met
21000-19	Media Value Chain Ontology	MVCO is an ontology for formalising the digital representation of Media Value Chains
23000-2	Music Player Application Format	A format for distribution of governed music
23000-4	Musical Slide Show Player Application Format	A format for distribution of governed music with slide show
23000-5	Media Streaming Player Application Format	A format for streaming governed video
23000-7	Open Access Application Format	A format for distribution of content with an REL licence expressing the intention of the Creative

		Commons licence
23000-8	Portable Video Player Application Format	A format for distribution of governed video
23000-9	Digital Multimedia Broadcasting Application Format	A format for distribution of governed DMB content
23001-3	XML Representation of IPMP-X messages	A standard XML representation for the messages used in MPEG-2 part 11 and MPEG-4 part 13
23006-1/-2/3	MPEG eXtensible Middleware	A standard for APIs of MPEG technologies (including IPMP-related technologies) integrated in a middleware

4 Descriptions of MPEG IPMP-Related Technologies

4.1 13818-1: EMM/ECM

The MPEG systems standard [1] specifies tools and format for conveying both the Entitlement Management Messages (EMM) as well as the Entitlement Control Messages (ECM). EMM is used for high level authorization and authentication of a receiver while ECM is used for event level conveyance of keys and other access information. MPEG transport and program streams include scrambling_control bits to signal whether the payload is encrypted and information in ECM is used to enable decryption. MPEG has allocated a specific PID value of '0001' to signal the presence and location of EMM while location of ECM is signalled using a descriptor associated with the program element for which the information in ECM applies. Both EMM and ECM can be conveyed using PES encapsulation or MPEG section encapsulation and MPEG does not specify any additional syntax for EMM/ECM.

Majority of the Conditional Access schemes and standards for terrestrial, cable and satellite networks are based on the MPEG specifications for EMM and ECM and these include DVB/ETSI, CEA and ANSI/SCTE specifications. These have been widely used in successful deployments currently.

Currently service providers convey the IP protection information (also called copy protection information) within the conditional access framework as this model is prevalent in US and parts of Europe.

4.2 13818-1/-2/-3: Copyright Identifier

Both the MPEG-2 video [2] and systems [1] standards specify signalling of copyrighted content at various levels. MPEG-2 video signals copyright information at a sequence or picture level for compressed video. The systems standard specifies copyright information at PES level for video or audio or data content. The MPEG Systems standard also specifies a descriptor that can be associated with any component in a program to signal both copyright and additional information. The additional information includes registration authority that has granted the copyright for the associated content.

So far these tools in both the video and systems standards have not found wide deployment in broadcast and other applications as the conditional access tools.

4.3 13818-11: IPMP-X

MPEG-2 IPMP is specified in [3] for use of IPMP tools (specified in the MPEG-4 specifications) in MPEG-2 transport or program stream framework. IPMP is specified as a forward and backward compatible framework with MPEG Conditional Access framework. IPMP tools include both conditional access and IP management and include interfaces to enable interoperability between 'domains' that use different IPMP schemes. IPMP can be signalled for an entire multiplex of services (multi-program transport stream) using the IPMP control section or for individual services (single program) or a single element of a program. IPMP tools can be signalled in a simple way to receivers that may implement a 'default' tool or IPMP can signal configuration information to receivers that may implement a tool that can be re-configured or a complete IPMP scheme can be transmitted to receivers.

4.4 14496-1: IPI

Besides enabling owners of intellectual property to manage and protect their assets, MPEG-4 Systems [4] provides a mechanism to identify those assets via the *Intellectual Property Identification Data Set* (IPI Data Set). The IPI Data Set identifies content either by means of internationally standardized numbering systems (e.g. ISRC, ISAN, ISWC-T/L, ISBN, DOI, etc.) or by privately generated key/value pairs (e.g. »Composer«/»Lohn Jennon«). The IPI Data Set can be used by IPMP systems as input to the management and protection process. For example, this can be used to generate audit trails that track content use.

4.5 14496-11: IPMP

MPEG-4's target applications range from low bit rate Internet telephones to high fidelity video and audio systems. The intellectual property management and protection (IPMP) methods required are as diverse as these applications. That is, the level and type of protection required depends on the content's value, complexity, and the sophistication of the associated business models. The MPEG-4 IPMP "hooks" framework specified in [4] has been designed with these types of conflicts and needs in mind providing application developers with the ability to construct the most appropriate domain specific IPMP solutions. While MPEG-4 IPMP "hooks" does not standardize IPMP Systems themselves, it does standardize the MPEG-4 IPMP interface. This interface was designed to be a simple extension of basic MPEG-4 systems constructs. It consists of *IPMP-Descriptors* (IPMP-Ds) and *IPMP-Elementary Streams* (IPMP-ES). IPMP-Ds and IPMP-ESs provide a communication mechanism between IPMP systems and the MPEG-4 terminal. When MPEG-4 objects require management and protection they have IPMP-Ds associated with them. These IPMP-Ds indicate which IPMP Systems are to be used and provide information to these Systems about how to manage and protect the content. Unique IPMP-Ds assigned by the MPEG-4 IPMP registration authority: www.ipmp-ra.org, where IPMP System providers can register their Systems.

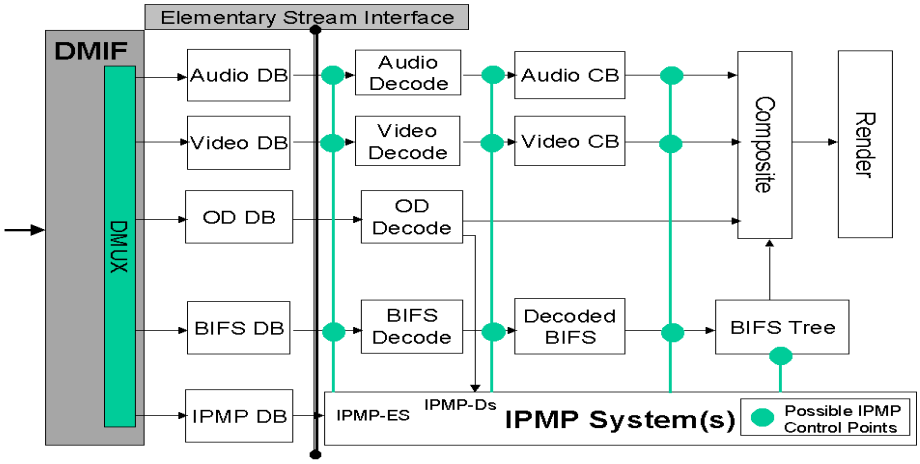

Figure 1: IPMP "hooks" Framework in the ISO/IEC 14496 Terminal Architecture

Figure 1 indicates a variety of points in the MPEG-4 terminal at which one might desire IPMP control. In general, the IPMP control points ("hooks") involve different kinds of mechanisms ranging from content access rules processing to decryption to watermarking. The actual processing of this control occurs in the IPMP System. Time-varying information such as decryption keys, sync info, etc. could be delivered to the IPMP System through a dedicated stream called *IPMP-Elementary Stream*.

Because the IPMP "hooks" framework was designed as a natural extension of existing MPEG-4 systems constructs, synchronization issues should be handled exactly as they are for any other MPEG-4 elementary streams and object descriptors. That is, if the MPEG-4 sync layer, timestamp and buffer management are designed correctly, synchronization of IPMP elementary streams and descriptors with the Audio-Visual Objects with which they are associated will follow naturally.

4.6 13818-11 and 14496-13: IPMP-X

IPMP "hooks" allows several IPMP systems to co-exist on the same Terminal. According to the chosen protected content, the IPMP System specified by the Content Owner at authoring time would be instantiated. The IPMP System itself is proprietary. However, the following issues were left open by IPMP "hooks":

- There was no standard way to specify how an IPMP System can be "hooked" in a player without previous agreement between player manufacturers and IPMP System providers;
- There was no standard mechanism to allow IPMP Systems to authenticate each other;
- There was not easy provision to replace a "broken" IPMP system.

The PMP-eXtensions, which are described next, were designed to answer the above "open questions" and to provide a more complete DRM architecture within MPEG and to do so in a secure manner.

The MPEG IPMP eXtensions are delivered in two flavours: MPEG-2 IPMP-X (Part 11) [3] and MPEG-4 IPMP-X (Part 13) [6]. MPEG-2 IPMP-X is designed to be applied to MPEG-2 based Systems and MPEG-4 IPMP-X is designed to be applied to MPEG-4 based Systems.

MPEG-4 IPMP-X (Figure 2) can be used to host any type of media protection at a varied level of granularity and complexity, as required by the specific DRM system employed to protect a given content within MPEG-4 Systems. MPEG-4 IPMP-X may protect any kind of media content

included in an MPEG-4 stream, as for example video, audio, computer graphics, text, interactive contents, etc.

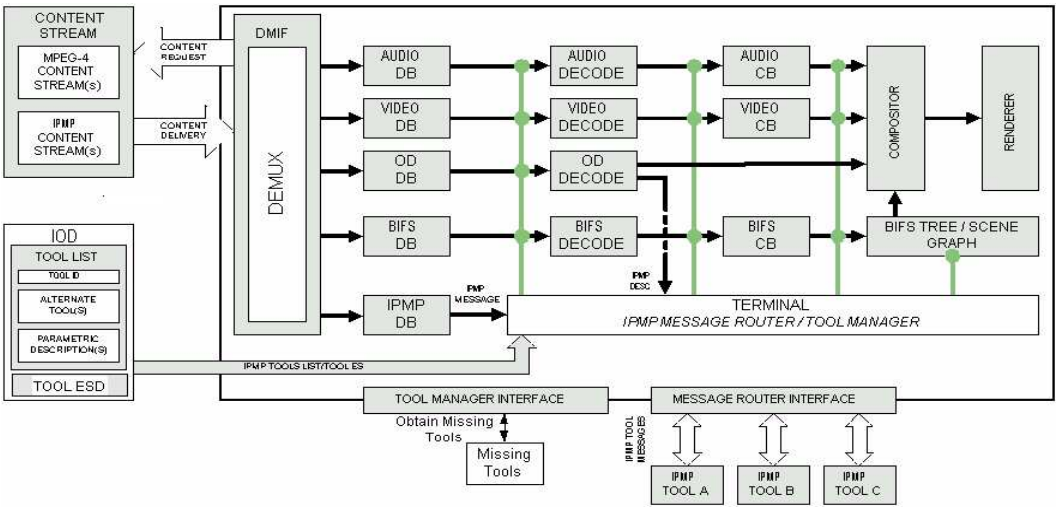

Figure 2: MPEG-4 IPMP Extensions architecture

In the IPMP eXtensions, taking in consideration the work done by OPIMA initiative, a more mature level of technology and a clearer understanding of the role of IPMP technologies made the MPEG group come out with a solution which does not need bi-lateral agreements, granting far much more interoperability between different IPMP modules (called IPMP Tools), by defining a message-based interface supporting the co-existence and communication between any pair of IPMP Tools and between them and the MPEG-4 player (Figure 2). Using normative messages, IPMP Tools can interchange any kind of information, including mutual authentication data, in order to ensure that the plugged-ins are the ones they claim to be and not "malicious", thus granting a secure operating environment.

When users request access to IPMP-X protected content, the MPEG-4 terminal processes the IPMP Tool List (Figure 2), a structure which specifies the IPMP Tools meant to govern the access to the content. These are then located, (if not present locally can be downloaded from a supplied location), and instantiated by a conceptual entity within the Terminal: the Tool Manager. Another conceptual entity, the Message Router, takes care of routing information between Tools and terminal. This communication takes place by means of normative and user-defined messages. These messages can be grouped in the following categories:

- IPMP Tool Connection and Disconnection Messages: Used to instantiate and destroy logical instances of new Tools, and to allow Tools to find out information about other Tools;
- Event Notification Messages: To provide the IPMP Tools the ability to request and get notified of events such as connection or disconnection of other Tools, watermark detection, etc;
- IPMP Processing: Defined to be used in the IPMP process covering a wide range of scenarios, like conveying keys, usage rules, to communicate with an audio or video watermarking Tool, to configure selective encryption, and so on;
- Authentication Messages: Defined to verify the trust relationships existing between two entities (Tools or Terminal), and to determine or create secure channels of communication as needed, based on the application;
- User Interaction Messages: To allow information to be exchanged between the user and an entity requiring information from the User;

- Consumption Messages: To allow an IPMP Tool to notify the terminal about its consensus to process content or not;

In summary, the key advantages brought by IPMP eXtensions can be summarized as follows:

- Interoperability: Thanks to the set of normative messages, interaction between different IPMP Tools is allowed;
- Security: Normative mutual authentication negotiation mechanisms are provided to ensure a secure operating environment;
- Flexibility: Free choice in choosing the algorithms (mutual authentication, protection such as encryption and watermarking, management, etc.) to govern the content;
- Renewability: Easy replacement of weak or old IPMP Tools.

The key benefits brought by MPEG-4 IPMP-X to content owners, end users and industry, are believed to be able to revolutionize the whole experience of access to protected content.

4.7 21000-1: Vision, Technologies and Strategy

ISO/IEC 21000-1 is a Technical Report that has been written to describe the multimedia framework, called MPEG-21 Multimedia Framework, and its architectural elements together with the functional requirements for their specification that was formally approved in September 2001 [7].

MPEG-21 aims at defining a normative open framework for multimedia delivery and consumption for use by all the players in the delivery and consumption chain. This open framework will provide content creators, producers, distributors and service providers with equal opportunities in the MPEG-21 enabled open market. This will also be to the benefit of the content consumer providing them access to a large variety of content in an interoperable manner.

MPEG-21 is based on two essential concepts: the definition of a fundamental unit of distribution and transaction (the Digital Item) and the concept of Users interacting with Digital Items. The Digital Items can be considered the “what” of the Multimedia Framework (e.g., a video collection, a music album) and the Users can be considered the “who” of the Multimedia Framework.

The goal of MPEG-21 can thus be rephrased to: defining the technology needed to support Users to exchange, access, consume, trade and otherwise manipulate Digital Items in an efficient, transparent and interoperable way.

The title “Vision, Technologies and Strategy” has been chosen to reflect the fundamental purpose of the Technical Report. This is to:

- Define a 'vision' for a multimedia framework to enable transparent and augmented use of multimedia resources across a wide range of networks and devices to meet the needs of all users
- Achieve the integration of components and standards to facilitate harmonisation of 'technologies' for the creation, management, transport, manipulation, distribution, and consumption of digital items.
- Define a 'strategy' for achieving a multimedia framework by the development of specifications and standards based on well-defined functional requirements through collaboration with other bodies.

4.8 21000-2: Digital Item Declaration

The purpose of the Digital Item Declaration (DID) specification [8] is to describe a set of abstract terms and concepts to form a useful model for defining Digital Items. Within this model, a Digital Item is the digital representation of "a work", and as such, it is the thing that is acted upon (managed, described, exchanged, collected, etc.) within the model. The goal of this model is to be as flexible and general as possible, while providing for the "hooks" that enable higher level functionality. This, in turn, will allow the model to serve as a key foundation in the building of higher level models in other MPEG-21 elements (such as Identification & Description or IPMP). This model specifically does not define a language in and of itself. Instead, the model helps to provide a common set of abstract concepts and terms that can be used to define such a scheme, or to perform mappings between existing schemes capable of Digital Item Declaration, for comparison purposes.

The DID technology is described in three normative sections:

- Model: The Digital Item Declaration Model describes a set of abstract terms and concepts to form a useful model for defining Digital Items. Within this model, a Digital Item is the digital representation of "a work", and as such, it is the thing that is acted upon (managed, described, exchanged, collected, etc.) within the model.
- Representation: Normative description of the syntax and semantics of each of the Digital Item Declaration elements, as represented in XML. This section also contains some non-normative examples for illustrative purposes.
- Schema: Normative XML schema comprising the entire grammar of the Digital Item Declaration representation in XML.

The table below gives the semantic "meaning" of the principal elements of the Digital Item Declaration Model. Please note that in the descriptions below, the defined elements in italics are intended to be unambiguous terms within this model.

Element	Definition
Container	A *container* is a structure that allows *items* and/or *containers* to be grouped. These groupings of *items* and/or *containers* can be used to form logical *packages* (for transport or exchange) or logical *shelves* (for organization). *Descriptors* allow for the "labelling" of *containers* with information that is appropriate for the purpose of the grouping (e.g. delivery instructions for a *package*, or category information for a *shelf*). It should be noted that a *container* itself is not an *item*; *containers* are groupings of *items* and/or *containers*.
Item	An *item* is a grouping of sub-*items* and/or *components* that are bound to relevant *descriptors*. *Descriptors* contain information about the *item*, as a representation of a work. *Items* may contain *choices*, which allow them to be customized or configured. *Items* may be conditional (on *predicates* asserted by *selections* defined in the *choices*). An *item* that contains no sub-items can be considered an entity -- a logically indivisible work. An *item* that does contain sub-*items* can be considered a compilation -- a work composed of potentially independent sub-parts. *Items* may also contain *annotations* to their sub-parts. The relationship between *items* and Digital Items (as defined in ISO/IEC 21000-1:2001, MPEG-21 Vision, Technologies and Strategy) could be stated as follows: *items* are declarative representations of Digital Items.
Component	A *component* is the binding of a *resource* to all of its relevant *descriptors*. These *descriptors* are information related to all or part of the specific *resource* instance. Such *descriptors* will typically contain control or structural information about the *resource* (such as bit rate, character set, start points or encryption information) but not

	information describing the "content" within. It should be noted that a *component* itself is not an *item*; *components* are building blocks of *items*.
Anchor	An *anchor* binds *descriptors* to a *fragment*, which corresponds to a specific location or range within a *resource*.
Descriptor	A *descriptor* associates information with the enclosing element. This information may be a *component* (such as a thumbnail of an image, or a text *component*), or a textual *statement.*
Condition	A *condition* describes the enclosing element as being optional, and links it to the *selection*(s) that affect its inclusion. Multiple *predicates* within a *condition* are combined as a conjunction (an AND relationship). Any *predicate* can be negated within a *condition*. Multiple *conditions* associated with a given element are combined as a disjunction (an OR relationship) when determining whether to include the element.
Choice	A *choice* describes a set of related *selections* that can affect the configuration of an *item*. The *selections* within a *choice* are either exclusive (choose exactly one) or inclusive (choose any number, including all or none).
Selection	A *selection* describes a specific decision that will affect one or more *conditions* somewhere within an *item*. If the *selection* is chosen, its predicate becomes true; if it is not chosen, its *predicate* becomes false; if it is left unresolved, its *predicate* is undecided.
Annotation	An *annotation* describes a set of information about another identified element of the model without altering or adding to that element. The information can take the form of *assertions*, *descriptors*, and *anchors*.
Assertion	An *assertion* defines a full or partially configured state of a *choice* by asserting true, false or undecided values for some number of *predicates* associated with the *selections* for that *choice*.
Resource	A *resource* is an individually identifiable asset such as a video or audio clip, an image, or a textual asset. A *resource* may also potentially be a physical object. All *resources* must be locatable via an unambiguous address.
Fragment	A *fragment* unambiguously designates a specific point or range within a *resource*. *Fragment* may be *resource* type specific.
Statement	A *statement* is a literal textual value that contains information, but not an asset. Examples of likely *statements* include descriptive, control, revision tracking or identifying information.
Predicate	A *predicate* is an unambiguously identifiable Declaration that can be true, false or undecided. Figure 1 is an example showing the most important elements within this model, how they are related, and as such, the hierarchical structure of the Digital Item Declaration Model.

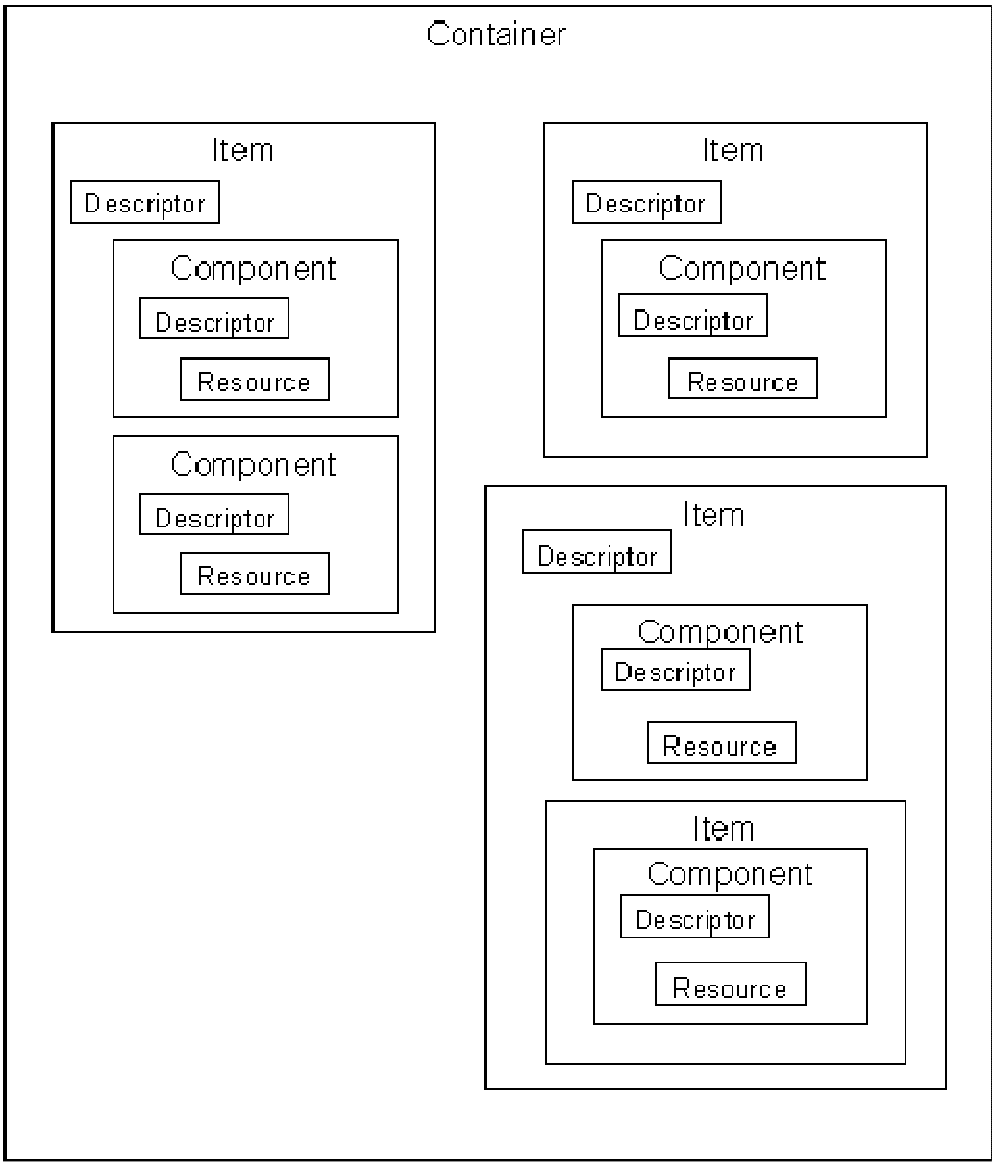

Figure 3 - Relationship of the principal elements within the Digital Identification Declaration Model

4.9 21000-3: Digital Item Identification

Identification systems are fundamental components of any commerce system. This applies to the physical world and – maybe even more so – to the digital content ecommerce environment. Various content identifiers either exist today or are under development. The use of MPEG-21 in an ecommerce environment requires that identifiers be associated with Digital Items [8]. Moreover, as Digital Items can be structured entities that may contain other entities, it will be necessary to also enable the association of identifiers with parts of Digital Items. This function is performed by ISO/IEC 21000-3, Digital Item Identification (DII). This provides a method to use existing identification schemes to identify Digital Items. However, DII is not a new identification scheme by itself. For example it does not attempt to replace the ISRC (as defined in ISO 3901) for sound recordings. Instead it relies on existing schemes (such as ISRC) and provides a uniform mechanism to transport identifiers within context of MPEG-21. Therefore the specification was developed with two issues in mind:

- The specification needs to be compatible with existing and future identification schemes; and

- The specification needs to enable use of such identifiers in the context of MPEG-21 applications.

The rationale behind this approach is that (most) identification schemes are content domain specific. It is the stakeholders in these domains that define important issues with respect with "their" identifiers, including:

- Level of Granularity;
- Scope of uniqueness;
- Persistence;
- Reference metadata;
- Resolution; and
- Governance.

If different identifiers are included within one Digital Item it is important to be able to recognise the identification schemes governing each identifier. For instance, to know that a Digital Item has an identifier "5-010356-663694" is meaningless unless it is known that this is an EAN bar code. While this is often clear from the context it cannot be guaranteed. Thus identification systems themselves have to be identified. ISO/IEC 21000-3 uses namespaces for this and two methods of providing such identifier namespaces;

- Some identifications have their own "native: namespace (e.g. the Digital Object Identifier DOI);
- For other identifier systems a Registration Authority has been established to provide a namespace for identification systems.

4.10 21000-4: IPMP Components

ISO/IEC 21000-4 [10] specifies how to include IPMP information and protected parts of Digital Items in a DIDL (Digital Item Declaration Language) document. The aim is to allow controls on the flow and usage of Digital Items throughout their lifecycle. The IPMP DIDL encapsulates and protects a part of the hierarchy of a Digital Item, and associates appropriate identification and protection information with it. The description of IPMP governance and tools is required to satisfy IPMP for a Digital Item or its parts to be accessed.

It exists in two parts:

- *IPMP Digital Item Declaration Language,* which provides for a protected Representation of the DID model, allowing DID hierarchy which is encrypted, digitally signed or otherwise governed to be included in a DID document in a schematically valid manner.
- *IPMP Information schemas,* defining structures for expressing information relating to the protection of content, including tools, mechanisms and licenses

4.11 21000-5: REL

A Rights Expression Language (REL) is a machine-readable language that declares rights and permissions. The MPEG REL, as defined by ISO/IEC 21000-5 [11], together with its profiles [12], [13], [14], provide flexible, interoperable mechanisms to support transparent and augmented use of digital resources throughout the value chain in a way that protects the digital resource and honors the rights, conditions, and fees specified for it.

The MPEG REL adopts a simple and extensible data model for a basic relationship, called a "grant", among the four basic entities:

- The principal to whom the grant is issued;
- The right that the grant specifies;
- The resource to which the right in the grant applies; and
- The condition that must be met before the right can be exercised.

A typical REL license consists of one or more grants and an issuer, which identifies the party who issued the license. Figure 1 illustrates the structure of a simple license:

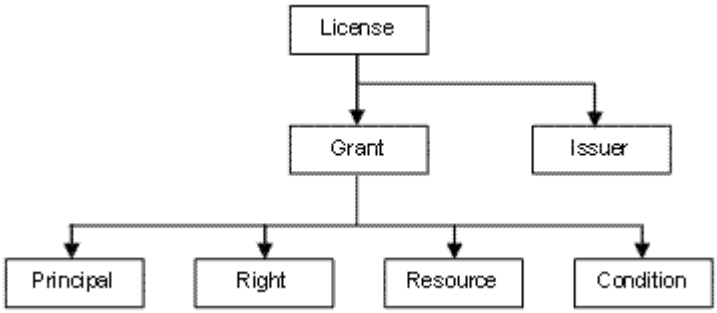

Figure 4 — Structure of a Simple License

To facilitate different applications that require different levels of complexity and flexibility in the REL and that need to meet specific needs of specific industries and user communities, MPEG has developed the following profiles:

- *MAM (Mobile And Media)*: for content and applications in the mobile and optical media domains.
- *DAC (Dissemination And Capture)*: for content and applications in broadcasting and home network domains.
- *OAC (Open Access Content)*: for content and applications in open environments, such as those defined by the Creative Commons licences.

It is important to point out that the DAC profile has been demonstrated to support the rights and conditions expressed in many other rights expression and information standards such as DVB-CPCM, OMA DRM V2.0, DTCP, AACS/CPRM/CSS, to name a few. In this sense, the REL with the DAC profile in particular can also serve as a general rights expression language for providing interoperability among those rights expression and information standards.

4.12 21000-6: RDD

The MPEG Rights Data Dictionary [15] is a standard for rights semantics. At the time MPEG decided to define the RDD standard (2001), there were many content metadata schemes already available and it was considered essential to ensure they could be incorporated into the proposed MPEG rights data dictionary. This requirement is satisfied by the MPEG RDD, use of which is intended to facilitate the accurate exchange and processing of information between interested parties involved in the administration of rights in, and use of, Digital Items. In particular it can be used for the exchange of rights expressions between different digital proprietary rights management applications.

The MPEG-21 Rights Data Dictionary (RDD) comprises a set of clear, consistent, structured, integrated and uniquely identified terms to support the MPEG-21 Rights Expression Language (REL) as specified in ISO/IEC 21000-5. A methodology and structure for the Dictionary is also

standardised, along with the method by which additional Terms can be added to the Dictionary through a Registration Authority.

The RDD is a *prescriptive* Dictionary, in the sense that it defines a single meaning for a Term, but it is also *inclusive* in that it can recognise and incorporate terms and definitions governed by organisations other that MPEG. These terms can be incorporated through an ontological process called mapping. The standard specifies an audit process so that additions, amendments and deletions to terms and their attributes can be tracked.

Finally, the MPEG-21 RDD recognises legal definitions only as terms from other organisations that can be mapped into the RDD Dictionary through the Registration Authority. Terms that are directly authorised by the RDD Registration Authority neither define nor prescribe intellectual property rights or other legal entities.

The RDD has the characteristics of a structured ontology, in which meaning, once it has been defined, can be passed on from one term to another by logical rules of association such as inheritance and opposition. In recognition of the great diversity and complexity associated with multimedia content, it is designed to represent as many different specialisations of meaning as its users require, and to show their relationships in a structured way in order to support the mapping and transformation of terms between different schemas and systems.

The MPEG-21 RDD contains about 2000 standardised terms. The majority of these are necessary for the structure of the RDD and for enabling extensibility of the Dictionary. Other terms are directly related to the use creation of REL permissions and the expression of rights ownership. Included in these terms are the fourteen rights set out here.

Adapt	Install
Delete	Modify
Diminish	Move
Embed	Play
Enhance	Print
Enlarge	Reduce
Execute	Uninstall

These terms are basic and can be specialised for more complex operations on rights protected content. A description of this specialisation process is also contained in the standard.

4.13 21000-11: Evaluation Tools for Persistent Association

MPEG-21 provides a framework within which many elements of multimedia are brought together. To handle such content a requirement for tools has been identified that can create and manage (e.g. detect or extract) an association between content and metadata pertaining to the content within MPEG-21. Tools based on the techniques known as “watermarking” and “fingerprinting” offer a means to form such associations, whereby the information can be directly embedded within or inferred from the content itself. Such tools are termed Persistent Association Technologies (PAT).

ISO/IEC 21000-11 [16] is a Technical Report providing best practices describing Evaluation Methods of Persistent Association Technologies. Users of ISO/IEC 21000-11 can conduct such evaluations using a common evaluation framework with specific test methodologies for each of the discussed persistent association technology types or paradigms. This is intended to give confidence to those relying on the results that they are:

- Appropriate tests of the technology that will predict its performance under real-world conditions and
- Comparable with results obtained from other tests conducted using the same methodology.

4.14 21000-15: Event Reporting

The Event Reporting standard [17] provides a set of technologies that can support, among others, the online retailing of copyrighted content. Event Reporting within MPEG-21 provides a standardized means for "reportable events" to be specified, detected and acted upon. Such a reportable event may relate either to the usage of a Digital Item (DI) by a Peer, or to the occurrence of Events related to the Peer itself. For example, an Event that is related to the usage of a DI could be the rendering (or PLAYing) of resources associated with a DI. Alternatively, an example of an Event that is Peer-related is when a Peer discovers (or connects to) another Peer, an action has no relation to the usage and/or manipulation of DI's.

Event reporting couples seamlessly with the existing MPEG Right Expression Language (REL) and Rights Data Dictionary (RDD) elements. For example, DI creators can instruct a peer to report when it installs, uninstalls, or executes a downloaded application. Similarly, when a peer moves, adapts, or plays a DI, a peer can also report this event.

A trust impact for Event Report recipients exists because they must have confidence in the event reports that they receive. This implies the need for information integrity and confidentiality, along with an ability to authenticate the peer that created the event report requests or event reports. Because event reporting uses the existing MPEG-21 DI infrastructure, we can apply any solution for these general DI issues to event reporting concepts as well.

4.15 21000-19: Media Value Chain Ontology

The Media Value Chain Ontology (MVCO) standard under development represents a normative core model of a knowledge domain that spans the full media value chain that can be extended to represent any number systematic specialisations of that core model to cover a broad range of content creation and management niches throughout value chains. Since the MVCO is designed to be formalised in a computer processable format such as with the Ontology Web Language (OWL), it can be used for standard computer processing anywhere. Thus, the MVCO serves to provide a common backbone for providing interoperable standard services and products (metadata, licenses, attribution etc.) such that ubiquity no longer represents a limitation to business but rather offers new opportunities for new business models and visions that can provide needed valued services and products to a broad set of interconnected value chains and niches. The MVCO and its extensions provide a pathway for all users to otherwise disparate connected niches.

4.16 23000-2: Music Player Application Format

The "Protected Music Application Format" standard [18] is a complete specification of a file format conveying protected audio resources, metadata, still images etc. The following cases are possible in addition to the unprotected case described in Music player application:

- Protected content files in mp4 file format, without Key Management components, with the default AES-128 encryption tool and MPEG-4 IPMP-X signalling in the IPMPInfoBox;
- Protected files with flexible tool selection and Key Management components (MPEG-21 IPMP and REL) using the mp21 file format with embedded mp4 content files; and

- Protected mp21 file with Key Management components (MPEG-21 IPMP and REL) but without embedded mp4 content file (variation of (b) that functions as a “license file” for an external protected mp4 content file (a).

Optional separation of protected content and license supports a broad range of "governed content scenarios" including “super distribution of protected content” and “subscription models”. The following Figure 1 illustrates the different cases and gives some examples.

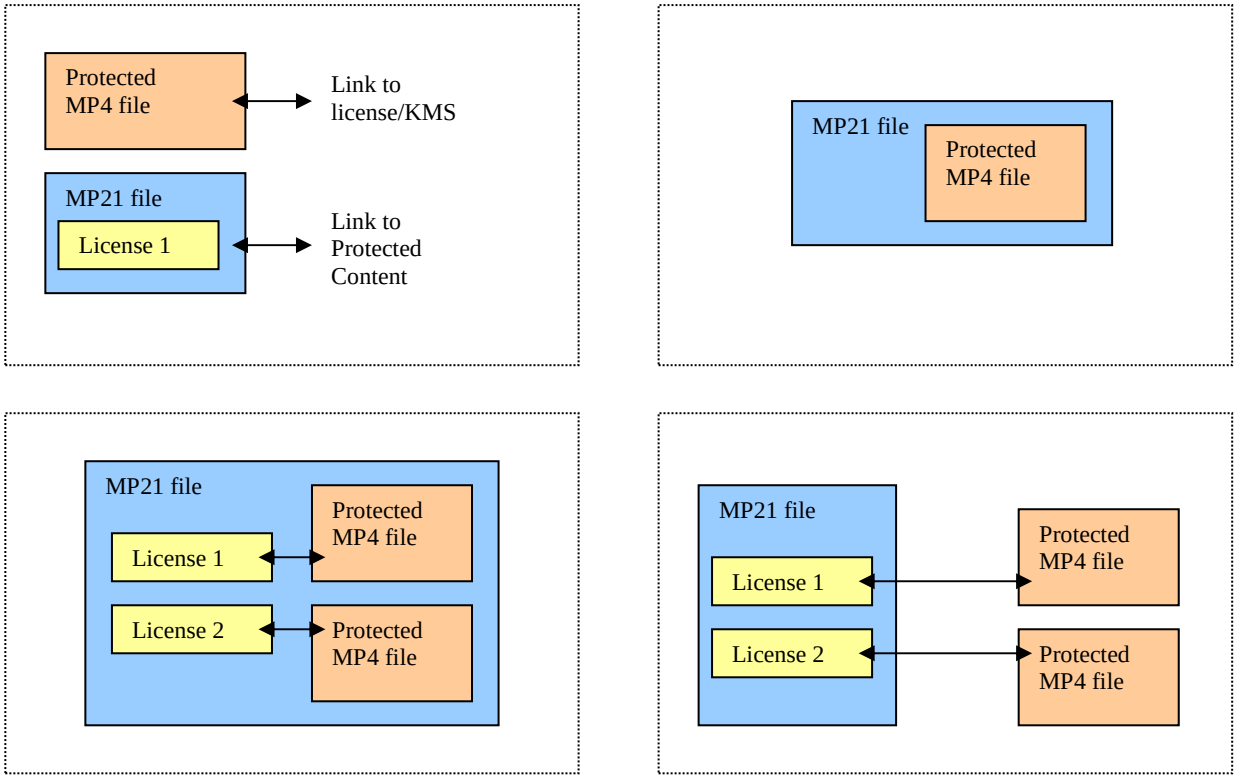

Figure 5 —Different cases illustrating the relationship of mp4 and mp21 files

4.17 23000-4: Musical Slide Show Player Application Format

The “Protected Musical slide show application format” standard [19] is a complete specification of a file format conveying protected MP3 audio resources, JPEG images, 3GPP Timed Text, and LASeR script animation with flexible protection tool selection and key management components.

Creating a Protected Musical slide show AF file involves formatting different types of media data, defining the protection and license information, and storing them into an MPEG-4 file format. Figure 2 shows an example of protected Musical slide show AF creator system architecture. MP3 audio, JPEG images, and text data are formatted as individual MP4 media tracks. Descriptions for the animation effects are stored as LASeR scene description in XML format. These resources are described in structured way using MPEG-21 Digital Item Declaration Language (DIDL) (ISO/IEC 21000-2), while the protection and license information for the protected resource is described using MPEG-21 Intellectual Property Management and Protection (IPMP) (ISO/IEC 21000-4) and MPEG-21 Rights Expression Language (REL) (ISO/IEC 21000-5).

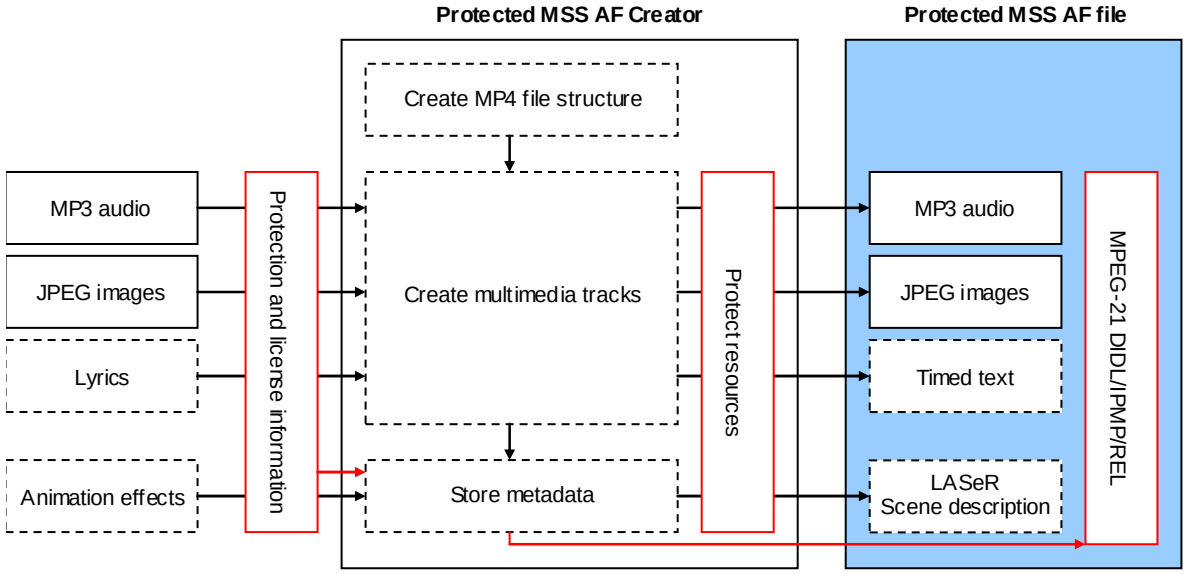

Figure 6 —Example of Protected Musical slide show AF creator system architecture

4.18 23000-5: Media Streaming Application Format

The Media Streaming Application Format (MSAF) standard [20] provides a standard format for streaming governed content which, when combined with associated protocols, leads to a full Media Streaming Player specification.

ISO/IEC 23000-5 is aimed at applications involving the distribution of governed media resources, metadata and related information over streaming channels to Media Streaming Players, possibly members of a domain in which the content can be securely distributed once stored in a file. Typical examples of such applications are IPTV, Digital Broadcasting without a return channel and video on demand.

The standard specifies how to use a set of MPEG technologies to achieve this goal, and references the data formats exchanged between a number of devices in a media streaming scenario: a Content Provider Device, a License Provider Device, an IPMP Tool Provider Device, a Domain Management Device and a Media Streaming Player.

In the most general case a Media Streaming Player obtains streaming content from a Content Provider Device using a Content Access Protocol. In order to use that content, a Media Streaming Player may need to obtain a license from a License Provider Device using a License Access Protocol. Further, to actually process the content, a Media Streaming Player may need to obtain the appropriate IPMP Tools from an IPMP Tool Provider Device using an IPMP Tool Access Protocol.

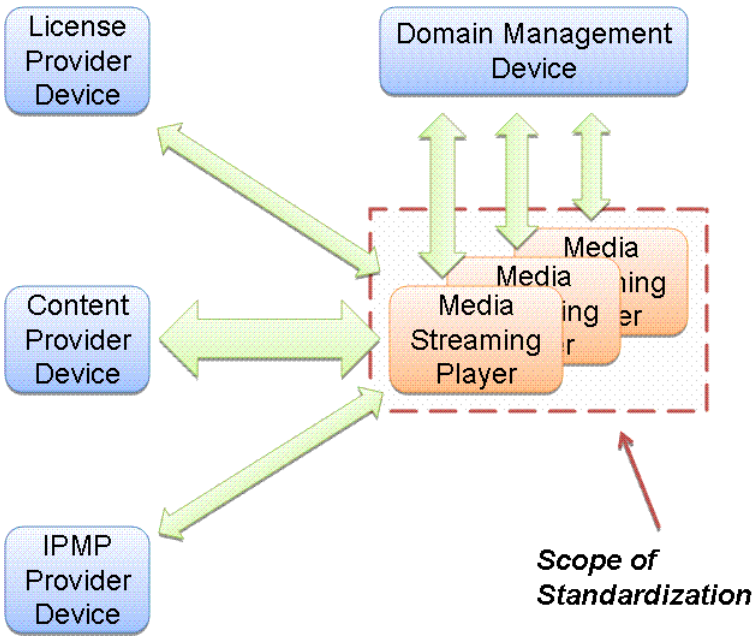

Figure 7 — Reference diagram for Media Streaming AF

The format of the media streaming content specified as part of MSAF relies on a number of MPEG technologies such as ISO/IEC 21000-2, ISO/IEC 21000-3, ISO/IEC 21000-4, ISO/IEC 21000-5, ISO/IEC 21000-9, ISO/IEC 21000-18, as well as on several MPEG-2/4 standards related to audio/video encoding, as this MAF specifies "native" resources for some application scenarios. Some of the standards mentioned above are referenced in their entirety by ISO/IEC 23000-5. Some others, however, are only used partially, and in a specific way. In order to support the operation of IPMP Tools on a device or between two different devices in an interoperable fashion, ISO/IEC 23000-5 employs the XML IPMP Messages specified in ISO/IEC CD 23001-3 XML IPMP Messages. ISO/IEC 23000-5 also employs ISO/IEC 29116 Media streaming application format protocols as the specification of a set of protocols allowing the mentioned devices to exchange information required for the establishment of a media streaming system in an interoperable way.23000-6: Professional Archival Application Format.

4.19 23000-5: Professional Archival Application Format

The Professional Archival Application Format (PA-AF) standard [21] provides a standardized packaging format for digital files. This packaging format can also serve as an implementation of the information package specified by the reference model of the open archival information system (OAIS). The OAIS reference model is a framework for understanding and applying concepts necessary for long-term digital information preservation (where “long-term” is long enough to be concerned about changing technologies). In addition, PA-AF can also be used as an intermediate or exchange packaging format for any kind of multimedia content.

PA-AF specifies the following: a metadata format to describe the original structure of digital files archived in a PA-AF file; a metadata format to describe context information related to a PA-AF file and digital files archived in it; a metadata format to describe necessary information to reverse the pre-processing processes applied to digital files prior to archiving them in a PA-AF file; and a file format for carriage of the metadata formats and digital files.

The combination of MPEG-21 File Format, MPEG-21 DIDIL 2nd Edition Profile for PA-AF, MPEG-21 DII, and MPEG-7 Creation Information Tool provides solutions to satisfy the basic

functionality of PA-AF, which is packaging Content Information in a PA-AF file. By adding MPEG-21 IPMP Components Base Profile for PA-AF, one can add functionality, such as compression, protection, and integrity checking to the PA-AF. By adding MPEG-21 REL MAM Profile, one can add license information to govern the usage of the PA-AF file. Finally, by adding MPEG-7 MDS Scheme Profile for PA-AF, one can have interoperable description of Content Information that can be exploited to implement functionality for interoperable content searching.

4.20 23000-7: Open Access Application Format

The Open Access Application Format (OAAF) standard [22] is a format to support the exchange and promotion of open contents. It is designed for the cases where users own rights to a piece of content and have an interest in releasing it in such a way that other users can freely access it. However, the users do not want to make the content public domain. Users want to release a piece of content that is governed in a "light-weight" form. This type of release is called "Open Access" and the set of technologies that support it is called Open Access Application Format (OAAF). Examples of Open Access are publicity material and teasers.

The Open Access AF is a file format It packaging different resources into a single container file and provides a mechanism to attach meta-data information, by using MPEG-7 and MPEG-21 technologies. The MPEG-21 REL is used to model the intentions of the license. MPEG-21 Event Reporting provides a feedback mechanism, which can notify the author, when a user wants to derive content or extract an item out of the container file.

Some of the application scenarios the Open Access MAF can be used for are the following:

- Release of a creative work or other material in a single package to the public ot specific persons. Additional metadata can be easily attached.
- Feedback to the author: The author can specify if he wants to get a feedback notification about the usage of his content.
- License Management is supported by the machine-readable licenses. Licenses can be browsed and searched easily. Licenses can also be generated automatically.
- Publishing of public funded research results.
- Publishing of E-Learning material. This material can be published with an attached human- or / and machine-readable license.
- Support for a variety of licenses by different organizations. E.g. the licenses provided by Creative Commons.

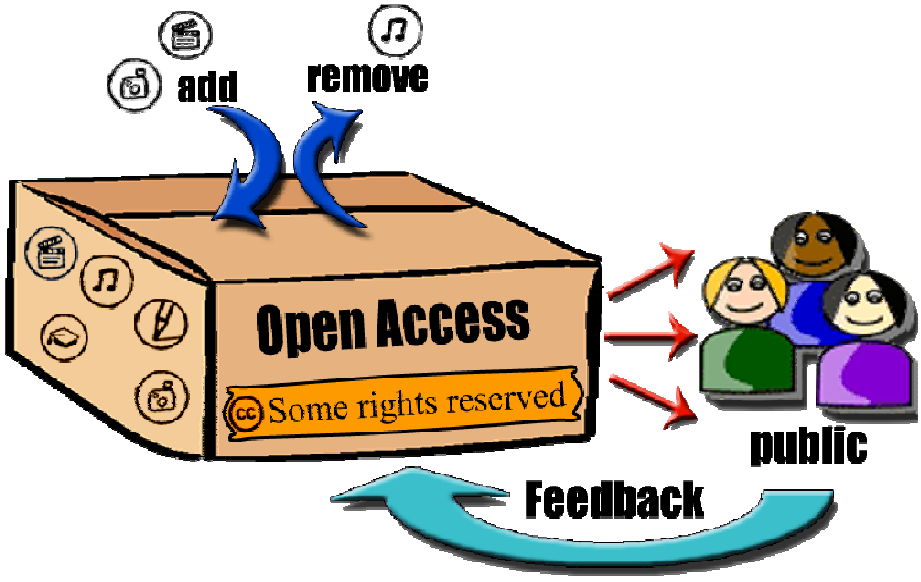

Figure 8 — Open Access Application Format scenario

4.21 23000-9: Digital Multimedia Broadcasting Application Format

The Digital Multimedia Broadcasting Application Format (DMB-AF) standard [23] specifies a file format that pertains to DMB [30], [31](i.e., T-DMB, S-DMB, DAB, and DAB+) contents and services. It integrates the existing DMB contents with appropriate additional information to facilitate storage, interchange, management, editing, and presentation of the contents in protected, governed, and interoperable ways.

DMB-AF is applicable both to storage and playback of DMB broadcast contents and to acquisition and consumption through communication networks and removable storages. Application examples of this specification include but not limited to scheduled storage and time-shifted playback of DMB contents:

- file casting through DMB data channel,
- IP media service such as DMB content portal,
- rightful interchange of DMB contents between terminals, and
- user editing or creation from DMB contents.

Regarding DRM functionality, DMB-AF uses subsets of MPEG-21 REL and IPMP Components. More specifically, protected usage of DMB contents is supported by a subset of MPEG-21 IPMP Components and licenses governing the usages are expressed according to the DAC (Dissemination and Capture) profile of the MPEG-21 REL.

4.22 23001-3: XML Representation of IPMP-X messages

The XML Representation of IPMP-X messages standard [24] specifies a set of XML messages exchanged between the components of a device in charge of the Intellectual Property Management and Protection (IPMP) operations performed when a protected resource part of a digital item is accessed.

The protection mechanisms are based on the IPMP Tool model as defined in ISO/IEC13818-11 (MPEG-2 IPMP Extensions), ISO/IEC 14496-13 (MPEG-4 IPMP Extensions) and ISO/IEC 21000-4: (MPEG-21 IPMP Components). In order to support operation of IPMP Tools on a device in an interoperable fashion, this standard complements ISO/IEC 21000-4 by defining an API for the communication between IPMP Tools and the device on which they operate, or between two IPMP Tools.

The API specified by ISO/IEC 23001-3 is based on a set of XML IPMP messages defining the format of the information exchanged between the various components on a device, or between two devices. Most of the IPMP Messages defined in this standard are a translation from the binary representation of the messages originally defined in ISO/IEC13818-11 and ISO/IEC 14496-13 into an XML representation. A number of these XML messages have been adapted in order to harmonise ISO/IEC13818-11 and ISO/IEC 14496-13 with the MPEG-21 Multimedia Framework and with ISO/IEC 21000-4 specifically. Additionally, a number of new XML messages have been defined to support extended IPMP requirements such as the separation between the IPMP algorithms and the logic enabling them to communicate with the other components in a device.

The XML IPMP Messages are a simple and natural extension of the IPMP Information Descriptors defined in ISO/IEC 21000-4. They allow dispatching the IPMP information related to a protected content element retrieved from the associated Digital Item to the modules in charge of performing the IPMP operations required to access the protected content element. Furthermore, the XML IPMP Messages provide a standard API allowing the exchange of IPMP information (e.g. decryption keys,

authentication information, licenses, etc.) between the modules – the IPMP Tools - in charge of providing access to the protected content elements (e.g. audio/visual resources).

The XML IPMP messages are grouped in the following macro-categories:

- IPMP Message Containers: the containers for IPMP Messages
- Mutual Authentication Messages: messages enabling one module to request mutual authentication with another one and to carry out the necessary steps in order to achieve it
- IPMP Tool Connection and Disconnection messages: enabling one IPMP Tool to request the instantiation as well as the disposal of another IPMP Tool
- IPMP Tool Notification Messages: enabling one component to request of being notified in case certain events occur, and conveying information about the event occurred
- IPMP Processing Messages: a set of messages enabling the exchange IPMP information ranging from licenses and decryption keys, watermarking data, etc.
- User Interaction Messages: allowing the exchange of information between an IPMP Tool and a user or vice versa
- Additional IPMP Messages: messages that on the one hand allow a greater decoupling between the IPMP algorithm implementations and the logic necessary to instantiate/initialize/manage them, and on the other do not require content providers and IPMP Tool providers to disclose the details of the IPMP modules
- Legacy Messages: messages originally defined in ISO/IEC13818-11 and ISO/IEC 14496-13 and translated to XML for the sake of completeness.

4.23 23006-1/-2/3: MPEG eXtensible Middleware

The MPEG Extensible Middleware (MXM) is a standard under development designed to promote the extended use of digital media content through increased interoperability and accelerated development of components, solutions and applications. MXM will promote the creation of a global market of applications, devices, and MXM components. As a result, we expect that innovative business models will be easily deployed.

The elements of the MXM Architecture are

1 MXM Engines, collections of specific technologies that it is meaningful to bundle together
2 MXM Engine APIs, APIs that can be used to access MXM Engine functionality
3 Orchestrator Engine, a special MXM Engine capable of creating chains of MXM Engines to execute a high-level application call such as “Play”
4 MXM Application API, the API of the MXM Orchestrator Engine
5 MXM Device, a device equipped with MXM
6 MXM Application, an application that runs on an MXM Device and makes calls to the MXM Application API and MXM Engine APIs

Figure 9 shows a general model of an MXM device

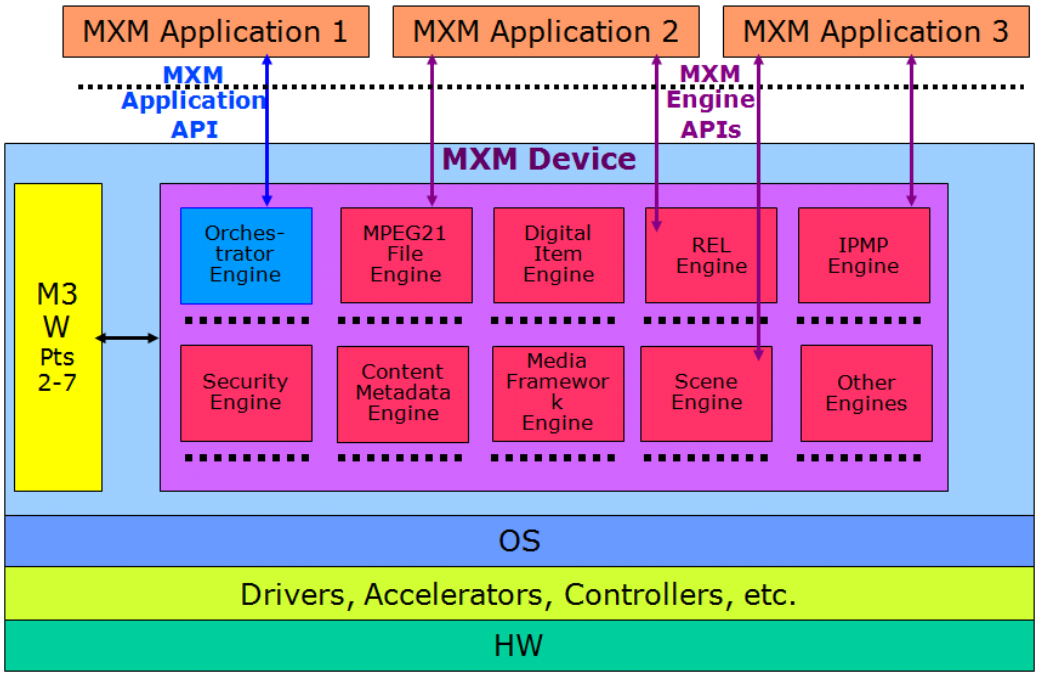

Figure 9 — Model of the MPEG Extensible Middleware

As shown in the Figure, MXM comprises of a framework hosting a number of Engines. These are containers of a specific set of MXM Technologies accessible by the MXM API specific of that Engine. As is typical of most MPEG standards, the MXM standard will only define the interfaces of the MXM Engines, named MXM Engine APIs and the MXM Orchestrator API.

In general an MXM Device can have several MXM Applications running on it (there may be other applications but these are not relevant here). Some may be "resident", i.e. they have been loaded by the MXM manufacturer and some may be temporary, i.e. they have been downloaded for a specific purpose.

When an MXM Application is executed, there may be "low-level" calls directly to some MXM Engines using the MXM Engine APIs of each specific Engines, and "high-level" calls like, say, "Play (GovernedContent)" which will be handled by the Orchestrator Engine. The MXM Orchestrator, by calling the MXM Engine APIs of specific engines, is capable of setting up a chain of MXM engines for handling complex operations, orchestrating the intervention and send/receive data to/from the particular chain of Engines that a given high-level call will trigger, thus relieving MXM Applications from the logic of handling them. Each MXM Engine will contain a specific set of MXM Technologies accessible by an MXM Application, the MXM Orchestrator and any other MXM Component in MXM, by means of its own MXM Engine API.

For instance, in the case of "Play (GovernedContent)" the Orchestrator engine could set-up the following chain:

a) MP21 File engine (e.g. open the file and extract the Digital item)
b) DI engine (e.g. extract metadata and rights information)
c) REL engine (e.g. verify if the right to play is granted)
d) IPMP engine (e.g. set up IPMP Tools to decrypt protected resources)
e) Security engine (e.g. initialise the IPMP Tools with decryption keys)
f) Content Metadata engine (e.g. present content metadata to the user)
g) Media Framework engine (e.g. demux, decode and render audio-visual resources)

... and possibly others.

5 Conclusions

Over the years MPEG has developed a range of standards that can be used by application developers to manage and protect the intellectual property associated with digital content. The standards cover a broad range of needs from the carriage of special EMM and ECM messages to convey Access Control information, to basic technologies for management and protection of content including identification of IP and representation of rights by means of a standard Rights Expression Language, to the definition of application-specific formats such as the Music Player Application Format.

For all its standards for which it was practical, MPEG has developed reference software implementations and conformance test suites.

Industry has made and continues to make use of these standards for a variety of content management and protection environments and applications.

6 References

[1] ISO/IEC 13818 Information technology -- Generic coding of moving pictures and associated audio -- Systems

[2] ISO/IEC 13818 Information technology -- Generic coding of moving pictures and associated audio -- Video

[3] ISO/IEC 13818 Information technology -- Generic coding of moving pictures and associated audio -- IPMP on MPEG-2 Systems

[4] ISO/IEC 14496 Information technology -- Coding of audio-visual objects -- Systems

[5] ISO/IEC 14496 Information technology -- Coding of audio-visual objects -- Scene Description and Application Engine

[6] ISO/IEC 14496 Information technology -- Coding of audio-visual objects -- IPMP Extensions

[7] ISO/IEC 21000 Information technology -- Multimedia Framework -- Vision, Technologies and Strategy

[8] ISO/IEC 21000 Information technology -- Multimedia Framework -- Digital Item Declaration

[9] ISO/IEC 21000 Information technology -- Multimedia Framework -- Digital Item Identification and Description

[10] ISO/IEC 21000 Information technology -- Multimedia Framework -- IPMP Components

[11] ISO/IEC 21000 Information technology -- Multimedia Framework -- Rights Expression Language

[12] ISO/IEC 21000-5:2004/Amd 2:2007, MAM (Mobile And optical Media) profile

[13] ISO/IEC 21000-5:2004/Amd 3:2008, DAC (Dissemination And Capture) profile

[14] ISO/IEC 21000-5:2004/Amd 3:2008, Open access content (OAC) profile

[15] ISO/IEC 21000 Information technology -- Multimedia Framework -- Rights Data Dictionary

[16] ISO/IEC 21000 Information technology -- Multimedia Framework -- Evaluation Tools for Persistent Association

[17] ISO/IEC 21000 Information technology -- Multimedia Framework -- Event reporting

[18] ISO/IEC 23000 Information technology -- Multimedia Application Formats -- Music Player Application Format

[19] ISO/IEC 23000 Information technology -- Multimedia Application Formats -- Musical Slide Show Application Format
[20] ISO/IEC 23000 Information technology -- Multimedia Application Formats -- Media Streaming Application Format
[21] ISO/IEC 23000 Information technology -- Multimedia Application Formats -- Professional Archival Application Format
[22] ISO/IEC 23000 Information technology -- Multimedia Application Formats -- Open Access Application Format
[23] ISO/IEC 23000 Information technology -- Multimedia Application Formats -- Digital Multimedia Broadcasting Application Format
[24] ISO/IEC 23001 Information technology -- MPEG Systems Technologies -- XML Representation of IPMP-X messages
[25] ISO/IEC 23004 Information technology -- MPEG Multimedia Middleware -- Multimedia API
[26] ISO/IEC 29116 Information technology -- Supplemental Media Technologies -- Media Streaming MAF Protocols
[27] Carlos Serrão, José Miguel Salles Dias, Panos Kudumakis, "From OPIMA to MPEG IPMP-X: A standard's history across R&D projects", pp. 972-994, EURASIP, Signal Processing: Image Communication Journal, Special Issue on European Projects in Visual Representation Systems and Services, Vol. 20, Issues 9-10, October-November 2005.
[28] Niels Rump, “Can digital rights management be standardized?” pp. 63-70, IEEE Signal Processing Magazine, Vol. 21, Issue 2, Mar 2004.
[29] Jack Lacy, Niels Rump, Talal Shamoon, Panos Kudumakis, “MPEG-4 Intellectual Property Management & Protection (IPMP) Overview & Applications”, AES 17th International Conference on “High Quality Audio Coding”, Florence, Italy, Sept. 2 - 5, 1999.
[30] DMB Portal - http://www.t-dmb.org
[31] WorldDMB Forum - http://www.worlddab.org
[32] Ian S. Burnett, Fernando Pereira, Rik Van de Walle, Rob Koenen (eds.), “The MPEG-21 Book”, Wiley, 2006.
[33] Fernando Pereira, John R. Smith, Anthony Vetro (eds.), Special Section on MPEG-21, IEEE Transaction on Multimedia, vol. 7, no. 3, pp. 397-479, June 2005.
[34] Ian Burnett, Rik Van de Walle, Keith Hill, Jan Bormans and Fernando Pereira. “MPEG-21: goals and achievements”, Multimedia, IEEE Volume 10, Issue 4, pp.60–70, Oct-Dec 2003.
[35] Xin Wang, Zhongyang Huang, Shenmei Shen, “DRM Standard Activities”, in Multimedia security technologies for digital rights management, edited by W. Zeng, H. H. Yu and C.-Y. Lin, Academic Press, 2006.