

# Definition of Standards-Based Building Blocks for Multimedia Content Management

Silvia Llorente, Jaime Delgado, Xavier Maroñas, Jonathan Florido

*Distributed Multimedia Applications Group (DMAG),*

*Departament d'Arquitectura de Computadors (DAC),*

*Universitat Politècnica de Catalunya · UPC BarcelonaTECH,*

*C/Jordi Girona, 1-3, 08034 Barcelona*

{silviall, jaime.delgado, xmaronas, jflorido}@ac.upc.edu

<http://dmag.ac.upc.edu>

*Corresponding author*

Name: Silvia Llorente

e-mail: [silviall@ac.upc.edu](mailto:silviall@ac.upc.edu)

Phone: +34 93 401 74 09

Fax: + 34 93 401 19 11

**Abstract** – The emergence of new ways of rendering multimedia content from a multiplicity of devices like tablets, smartphones, consoles or smart TVs, opens a complete set of new opportunities for multimedia services providers. It is important that the development of those disruptive services is done in an interoperable way. Existing service-oriented middleware platforms and recently developed standards devoted to the definition and implementation of complex multimedia services may speed up its development. In this context, the identification of different content management scenarios including the high level functionalities they require is an important aspect to be able to implement services in a flexible and interoperable way. Use of standards and standards-based architectures will be a key aspect to combine services offered by different providers. In this paper we propose the definition of standards-based building blocks based on the high level functionalities required by content management and distribution scenarios. This will facilitate provision of complex new services specially focused, but not limited to, the management and distribution of multimedia content.

Keywords: Standards, Building Blocks, MPEG-M, MIPAMS, Android, Demonstration

## 1 Introduction

There are different scenarios for content distribution depending on issues such as if access to content has to be controlled, if content usage has to be reported or if licensing for content consumption is required. In [27], the authors analyzed different possible multimedia content management and distribution scenarios, identifying the high level functionalities needed by them. These functionalities are Authentication, Authorization-based content access control, Content management, Licensing, Protection, Search, Storage and retrieval and Tracking. Based on this

analysis, in this paper we go a step further proposing the definition of these identified functionalities as Standards-Based Building Blocks (SB3).

The leading objective behind the definition of SB3 is to describe other application scenarios where content handled is represented as multimedia content. To do so, multimedia content management scenarios are taken as a starting point, identifying the standards related to the corresponding SB3. Once this is done, other application scenarios could be also described in terms of SB3, identifying the standards applying to each of them. The relationship between all application scenarios considered (e-health [5] [35], e-learning [36] or e-government [32]) and the multimedia content management scenarios is the use of standards. The main aim is to identify similar operations for each SB3, independently from the scenario described, the field of application or the standards used. In this paper we focus on the multimedia content management scenarios, the description of other application scenarios will be derived from this work.

So, the foremost difference with the ideas presented in [27] is the definition of SB3. It also includes the identification of existing standards for each of them and the mapping with different initiatives in the multimedia content management scenarios and services as described below.

To illustrate how SB3 could be applied to different environments we have selected scenarios and standards applying to e-health, e-learning, e-government and chemical processing. We have identified scenarios where modules similar to SB3 are defined and also complex services that could be modeled by means of SB3 as briefly described next.

Regarding e-health, the use of SB3 allows describing scenarios to provide patients with mechanisms to securely store and manage their medical information. In this sense, there are specific standards for the representation of electronic health records, like HL7 Clinical Document Architecture (CDA) [1] or ISO 13606-1 [19] and specific applications based on the representation of health information as multimedia information [5] [35], where the building blocks could be used.

With regard to learning, an almost direct application of SB3 is the management of digital learning materials. This is done by means of learning management systems. In [36], the authors describe how to manage interoperability between learning content management systems. To do so, they define the system interface framework both for application and administration layers. In particular, the module Access Control is required, which is also a requirement for content management scenarios identified in [27]. In this sense, the description of such a module can be considered as a similar, but simpler and more specific concept, than SB3.

On the other hand, building blocks can be also used not only as independent modules, but also as part of a more complex system. In such a system, it is possible to define services that make use of different SB3 that when working together accomplish a complex task. So, the use of SB3 in services permits the application of Service Oriented Architecture (SOA) concepts [10] to the definition and implementation of business scenarios based on the blocks defined. As an example, [9] presents how to model a collaborative learning

framework using SOA, using UML models and defining learning processes by means of Business Process Management (BPM) [11]. Other fields where similar concepts have been applied are e-government [32] or chemical process modeling [8].

The rest of the paper is organized as follows. First, we describe the background of this paper, which consists on MPEG-M standard [13] and the Multimedia Information and Protection Management Systems (MIPAMS) middleware architecture [4]. MPEG-M is a new standard coming from the MPEG Standardization Group [14], whose aim is to develop complex multimedia services using MPEG-based technologies with a high level of abstraction. MIPAMS is a middleware architecture implementation developed by the Distributed Multimedia Applications Group (DMAG) [7]. It implements several standards-based modules to provide secure content management and distribution of multimedia content. Afterwards, the section 3 describes the concept of Standards-Based Building Blocks (SB3), related to the different content management scenarios where they appear. Then, we identify the different SB3, indicating the standards applying to each of them. After that, we describe SB3 operations. These operations are mapped to both MPEG-M and MIPAMS, comparing functionality and scope. Next, we describe the scenario for mobile devices identified in [27] using SB3. We also show how it could be implemented using both MPEG-M and MIPAMS, as presented in the MPEG-M forum. Next, we describe an e-health scenario, showing how secure access to and modification of electronic health records can be done by means of SB3. Finally, some conclusions and future work is presented.

## **2 Background**

In this section, we discuss the background standards and standards-based platforms for the definition of services and modules to provide complex multimedia services. They are the basis for SB3 (the detailed description of them is in section 3).

### **2.1 MPEG-M: Multimedia Service Platform Technologies (MSPT)**

MPEG-M (ISO/IEC 23006) [13] [25] [34] is an initiative of the MPEG standardization group (ISO/IEC JTC1 SC29/WG11). It defines a suite of standards that are being developed for enabling the easy design and implementation of media-handling value chains. The main aim behind the different parts of this standard is to provide a set of middleware Application Programming Interfaces (API), elementary service protocols and formats and service aggregation mechanisms to facilitate the creation of content management and distribution systems that can be interoperable between them. The definition of common API's, protocols and interfaces will permit the integration and use of services implemented by different organizations so that service providers can offer users a plethora of innovative services towards the seamless integration of

personal content creation and distribution, e-commerce, social networks and Internet distribution of digital media.

MPEG-M standard has two editions. In its first edition [34], it is referred as MPEG Extensible Middleware (MXM), and it specifies an architecture (Part 1), an API (Part 2), a reference software (Part 3) and a set of protocols which MXM Devices had to adhere (Part 4).

In its second edition [25], it is referred as Multimedia Service Platform Technologies (MSPT), and it maintains the architecture and design philosophy of the first edition, but stressing its Service Oriented Architecture (SOA) character. SOA has been specially applied to parts 4 (Elementary Services) and 5 (Service Aggregation) of the standard. Part 4 defines elementary services providing basic functionality for implementing any content distribution scenario and part 5 describes how to aggregate services. The services to aggregate could be those present in part 4. New elementary services should be described following the guidelines defined in part 4 and registered with the mechanism defined in part 5. By new services we mean those not present in part 4.

More specifically, the second edition of MPEG-M is subdivided into the following five parts:

- Part 1 - Architecture: Specifies the architecture that is part of an MPEG-M implementation;
- Part 2 - MPEG Extensible Middleware (MXM) Application Programming Interface (API): specifies the middleware APIs;
- Part 3 - Conformance and Reference Software: specifies conformance tests and the software implementation of the standard;
- Part 4 - Elementary Services: Specifies elementary service protocols between MPEG-M applications;
- Part 5 - Service Aggregation: Specifies mechanisms enabling the combination of elementary services and other services to build aggregated services.

Part 1 describes the MPEG-M architecture, its elements and Application Programming Interfaces (APIs) that enable MPEG-M compliant devices to be interoperable even if different manufacturers implement them. An MPEG-M device is a device equipped with MPEG-M engines. It can have several MPEG-M applications running on it such as an audiovisual player or a content creator combining audio-visual resources with metadata and rights information.

Part 2 specifies a set of APIs, which are the gateway to the MPEG-M middleware – providing access to its technology engines as specified in Part 1 – for any application running on an MPEG-M device.

Part 3 is about the conformance and reference software. The APIs and the Elementary Services are given in MPEG-M Part 2 and MPEG-M Part 4, respectively.

Part 4 specifies Elementary Services (ES) and their protocols. They are the key elements in achieving services interoperability in the MPEG-M ecosystem.

Part 5 specifies how ESs and perhaps other existing Aggregated Services (ASs) should be combined to build new ASs. To do so, it provides a methodology which defines the basic steps for the definition of ASs.

The combination of the different parts of MPEG-M standard, especially parts 4 and 5, covers the content management and distribution scenarios identified and described in section 3. For instance, DRM-enabled (DRM stands for Digital Rights Management) content access control scenario would make use of the Authenticate User, Authorize User, Create License, Store License, Search Content and Store Event Elementary Services. With the aggregation of these services it is possible to define the buyer point of view of this scenario, as described in part 5 of the standard [15]. It is worth noting that any of the described scenarios have a buyer (content consumer) and seller (content producer or distributor) use cases. In this sense, the Elementary Services needed to implement each of them will be different although the aggregation will be always done in a similar way.

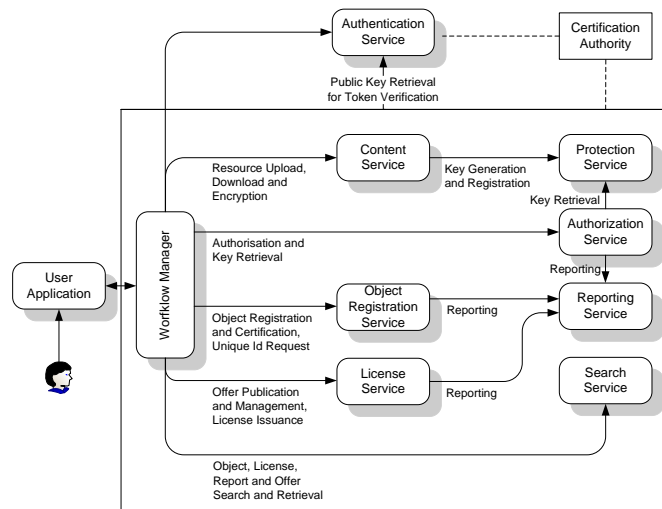
Several members of the DMAG are co-editors of this standard series, having contributed work done in MIPAMS, which is described in section 2.2, and other different research projects for the development of this standard.

## **2.2 MIPAMS: Multimedia Information Protection And Management System**

This section describes MIPAMS (Multimedia Information Protection And Management System), a service-oriented content management platform, developed by the DMAG (Distributed Multimedia Applications Group). It is mainly intended for applications where management of rights over digital multimedia content is required.

The MIPAMS architecture is based on the flexible web services approach, as it consists of several modules and services that provide an important part of the functionality needed for governing and protecting multimedia content. The main advantage of having service-oriented DRM functionality relies on the possibility of decoupling it into different subsystems depending on the needs of the application that is going to be implemented, while being able to share the same common services between different applications with different requirements, thus reducing costs.

Figure 1 depicts the MIPAMS architecture, for which we provide a general overview of its components and the different services being offered next.



**Fig. 1.** MIPAMS Architecture overview.

Authentication Service (ATS) is needed to authenticate the identity of users. It generates SAML (Security Assertion Markup Language)-based tokens [30] that identify MIPAMS users. Any service in the MIPAMS architecture will require a token argument to be provided in order to authenticate users. Tokens are digitally signed by the ATS, so that they can be checked for authenticity and integrity by the receiving service.

Authorization Service (AS) checks whether a user owns any appropriate license that grants him the right to perform a requested action (e.g., play) over a digital object. The authorization is based on the license based authorization mechanism defined in [16]. After positive authorization and if content is encrypted, Authorization Service (AS) requests corresponding encryption keys to Protection Service (PS) and returns them to the requesting application.

Content Service (CS) enables applications to upload and download digital resources such as audio or video files, text documents, etc. Those resources can be optionally encrypted under request. If encryption is selected, the protection keys will be first requested to the Protection Service (PS) and then registered back into PS, once encryption is performed.

License Service (LS) deals with rights offers and license issuance over digital objects, which include the rights and conditions that can be acquired by users over some digital content. They are defined by contents' rights holders, which include content creators. Licenses are expressed using MPEG-21 Rights Expression Language [16].

Object Registration Service (ORS) permits the registration of digital representations (i.e. digital objects) of multimedia content (comprising content and metadata). This information is packaged using the MPEG-21 Digital Item XML-based format [17]. ORS registers and digitally signs objects so that they can be later checked for authenticity and integrity.

Protection Service (PS), as introduced before, generates encryption keys upon request, registers encryption keys associated to uniquely identified content and provides the encryption keys for protected content to the AS.

Reporting Service (RS) collects usage reports regarding object registration, license issuance and positive authorizations. Those reports may be used for computing statistics as well as for billing or tracking purposes. From the information stored it is possible to generate standards-based representations like MPEG-21 Event Reports [18].

Search Service (SS) enables applications to perform accurate searches amongst metadata in the MIPAMS system. It can be used for searching content, licenses, offers or reports or a combination of them.

Workflow Manager (WM) may be an integral part of the User Application (UA) or otherwise be located in the server part (e.g. web portal, brokerage service) to reduce the UA complexity. It controls access to the rest of services inside MIPAMS architecture, like license issuance, authorization, content upload, etc.

User Application (UA) is a player, edition tool, browser or any other means managed by the user to deal with the digital content, for instance registering or accessing it. It may have an internal trusted module to locally enforce DRM features.

Finally, there is a need for having a recognized Certification Authority (CA), which issues credentials for the different Components and Actors in the system, as X.509 [12] certificates and private keys for the different architectural components.

MIPAMS platform has also been successfully used in the implementation of e-health applications [5] [35], just substituting the licensing and authorization services by ones based on XACML policies. We have taken advantage from the rest of services in the platform, whilst demonstrating its versatility. The service oriented nature of MIPAMS has also proved to be very useful for the integration of external platforms as also described in [28]. Another application scenario considered was Social Networks, as presented in [6] [26].

## **3 Proposed Standards Based Building Blocks (SB3)**

### **3.1 Introduction**

The high level functionalities of content management scenarios identified in [27] helped us in the definition and classification of the proposed Standards Based Building Blocks (SB3). In the rest of the section, we describe SB3 requirements are identified, we summarize content management scenarios and their high level functionalities. Based on this information, we identify the SB3, describing their functionality, the standards applying to each of them and the operations identified for each one.

### 3.2 Content Management Scenarios

To provide secure management and distribution of multimedia content, we have identified some scenarios. They are briefly described next, ordered by their level of complexity:

- **Content licensing:** There is a license associated to content, but neither protection nor access control is required. This is the case for Creative Commons [2] licenses over content.
- **Content licensing and authorization-based content access control:** The access to content is authorized based on permissions owned by the user.
- **DRM-enabled content access control:** The content is encrypted and decryption is authorized only if user owns an appropriate permission.
- **DRM-enabled content access for mobile devices:** The same as the previous one, but oriented to mobile devices.

These scenarios need some basic building blocks or high level functionality to be implemented. They are summarized next:

- **Authentication:** Users and software components need to be authenticated when accessing a system, since permissions need to be bundled to them.
- **Authorization-based content access control:** Content access and usage is controlled by checking that users own a suitable license. If content access is for free, authorization can be used to check if reporting is required. Otherwise, authorization is needed for billing users according to content usage.
- **Content management:** The representation of content generally uses a specific format to facilitate packaging and registration so as to be uniquely identified in the system. Registered content can be easily referenced from permissions.
- **Licensing:** Permissions applicable to content usage need to be formalized through licenses when content is acquired. Even if licenses are used, content could be provided for free, while licensing conditions would serve for requiring, e.g., reporting of content usage.
- **Protection:** Different mechanisms can be used to protect content when access to it is not open (e.g. encryption, watermarking, compression or a combination of mechanisms).
- **Search:** Users need a way to find content in order to acquire it or to prove its registration. Filling content metadata is vital to offer such functionality.
- **Storage and retrieval:** Users should be able to retrieve content from wherever it is stored if they own the appropriate usage rights.
- **Tracking:** Content owners often want to be informed about content usage, and sometimes bill according to the real usage. Therefore, content usage needs to be registered. Other operations, like content creation may be also reported for informative purposes.

Each scenario makes use of different building blocks from the ones identified. The correspondence between them is as follows. Content Licensing scenario involves Content Management, Search, Licensing and Tracking. Content Licensing and Access Control adds Authorization-based access control and



optional Storage and retrieval to the previous scenario. Finally, DRM-enabled content access control, including mobile version, adds the Protection to the previous scenario, using the complete set of SB3 defined. Authentication is required in all the scenarios.

### 3.3 Definition of the Building Blocks

The main requirement for the building blocks defined is that they should be as generic as possible, in order to facilitate interoperability and provide flexibility. In this way, the application of the building blocks concept to other business environments working with different kinds of multimedia content will be easier.

As described in section 1, there are several business areas where these concepts are applied, like e-health [5] [35], e-learning [36] or e-government [32]. So, the objective is to define them for the multimedia scenarios identified and then broaden its scope to other areas.

In order to define the building blocks mentioned in subsection 3.1.1, well-known standards in the area of application of each of them have been used, so we will refer to them as Standards-based Building Blocks (SB3) from now on. It is worth noting that, if other business environments have to be supported, the corresponding standards may be added in the same way as the ones presented below. In the building blocks definition we are mainly considering multimedia content management for the multimedia industry, but, as already explained, this is not the only field of applicability.

The SB3 identified for the definition of content management scenarios are listed in Table 1, together with a brief description and the standard or standards each one refers to. It is worth noting that Access Control and Licensing are inside the same SB3, as their functionality is closely related, as access control can only be done after the definition of licenses or permissions. Using these SB3, any of the scenarios described in subsection 3.2 can be defined.

**Table 1.** Standards-based building blocks.

<b>Building Block</b>	<b>Description</b>	<b>Related Standard(s)</b>
Access Control and Licensing	Defines content usage rights and conditions through permissions in order to formalize content purchase. It is worth noting that, although a license can be applied to content usage, content may be provided for free. It also controls that user can access to content based on the permissions she owns.	MPEG-21 REL ODRL XACML MPEG-21 CEL
Authentication	Checks that users and software components are able to access the rest of components of the system. This SB3 has to be invoked before any other SB3.	SAML 2.0
Content Management	Represents and identifies content in a specific format to facilitate packaging and registration.	MPEG-21 DID MPEG-21 DII MPEG-21 IPMP Dublin Core Application-dependent metadata

Protection	Protects content using encryption mechanisms when content access is not open.	Encryption Algorithms MPEG-21 IPMP
Search	Provides searching functionality based on different metadata associated to content and licenses.	MPQF SQL
Storage and Retrieval	Provides access to content after positive authorization, that is, user owns the appropriate rights.	Sockets-based HTTP FTP
Tracking	Stores information about different events occurred regarding content registration, licensing and content usage.	MPEG-21 ER

*Legend:*

MPEG-21 REL: ISO/IEC IS 21000-5 Rights Expression Language [16]  
ODRL: Open Digital Rights Language [38]  
XACML: eXtensible Access Control Markup Language [31]  
MPEG-21 CEL: ISO/IEC IS 21000-20 Contract Expression Language [20]  
SAML v2.0: Security Assertion Markup Language [30]  
MPEG-21 DID: ISO/IEC IS 21000-2 Digital Item Declaration [17]  
MPEG-21 DII: ISO/IEC IS 21000-3 Digital Item Identification [21]  
MPEG-21 IPMP: ISO/IEC IS 21000-4 Intellectual Property Management and Protection [22]  
MPQF: MPEG Query Format [23]  
SQL: Structured Query Language [24]  
HTTP: HyperText Transfer Protocol [39]  
FTP: File Transfer Protocol [33]  
MPEG-21 ER: ISO/IEC IS 21000-15 Event Reporting [18]

### 3.4 SB3 Operations

Each SB3 provides several operations to make use of the functionality they provide. They are listed in Table 2, including a brief description of its operation and the standards used for its implementation.

**Table 2.** SB3 operations.

Building Block	Operation	Description
Authentication	Login	Allows user to enter the system with her credentials that can be username and password, a SAML authentication request or other method required. In response, a SAML authentication response is generated, which proves user identity in front of the rest of services.
Access Control And Licensing	Permission Creation	It is used to create permissions over digital objects assigned to users inside the system. MPEG-21 REL and XACML are the standards currently supported to express permissions.
	Permission Revocation	It is used to revoke an existing permission, which will not authorize user actions any more.
	Authorization of User Actions	Checks if user has permission to perform a specific action over a digital resource. This authorization depends on the language used for expressing permissions. Both MPEG-21 REL and XACML authorization mechanisms are currently supported.
Content Management	Content Creation	Stores the information (metadata, structure, relationship) associated to one or more digital resources. MPEG-21 DID

		is used for the formalization of digital objects. MPEG-21 IPMP is also used when security of the digital object structure is required.
	Content Deletion	Removes the information associated to a digital object. Associated permissions are removed or revoked.
Protection	Key Storage	Generates and stores an encryption key associated to a digital resource / object.
	Key Retrieval	Retrieves an encryption key associated to a digital resource / object. This operation can only be done after positive authorization.
Search	Search	Performs searches over different types of information in the system, digital objects, offers, licenses or reports, according to the parameters passed. SQL queries have been implemented.
Storage and Retrieval	Resource Storage	Uploads a digital resource (image, video, audio, document, etc.) associated to a digital object. Sockets, FTP and HTTP solutions for content storage and retrieval have been implemented.
	Resource Retrieval	Downloads a digital resource (image, video, audio, document, etc.) associated to a digital object.
Tracking	Activity Report Creation	Stores the information associated to the operations occurred in the system, like object creation, permission creation or authorization of actions. MPEG-21 ER is used to describe the activities done in the system.

### 3.5 Mapping SB3 to existing initiatives

In order to prove the appropriateness / correctness / completeness of the SB3 identified, we provide in the following subsections the mapping of the different SB3 to MPEG-M and MIPAMS. Doing so, we will be able to implement content management and distribution case studies presented in section 4.

Specifically, two mappings are provided. The first one maps MPEG-M elementary services to SB3 operations. The second one maps MIPAMS platform services and operations to SB3 operations. Finally, a complete comparison of the operations provided by MIPAMS, MPEG-M elementary services and SB3 proposed operations is done.

#### 3.5.1 Mapping SB3s to MPEG-M part 4 Elementary Services

MPEG-M Part 4 Elementary Services (ISO/IEC 23006-4 Information Technology – Multimedia Service Platform Technologies – Part 4: Elementary Services) specifies Elementary Services (ES) and their protocols, which are key elements in achieving services interoperability in the MPEG-M ecosystem. Nevertheless, ESs are mainly based on MPEG standards. With the definition of SB3s the intention is to go a step further, considering not only MPEG standards, but also other standards like ODRL [38] or XACML [31] for permission definition and authorization.

This section describes the mapping of the SB3s defined in section 3.3 to the Elementary Services defined in MPEG-M Part 4 Elementary Services (ES). The correspondence between each SB3 operation and the corresponding

Elementary Service is listed in Table 3. In this case, several ESs are needed to provide the complete functionality supported by a SB3. So, the mapping between both becomes more complex, although still possible.

**Table 3.** Correspondence between SB3 and Elementary Services.

<b>SB3</b>	<b>Operation</b>	<b>Elementary Service</b>
Authentication	Login	Authenticate User
Access Control and Licensing	Permission Creation	Create License, Store License, Identify License (optional)
	Permission Revocation	Revoke License
	Authorization of User Actions	Authorize User
Content Management	Content Creation	Create Content, Store Content, Identify Content (optional), Process Content (optional, needs to be specialized to use it)
	Content Deletion	Revoke Content
Protection	Key Storage	Associated to Create Content
	Key Retrieval	Associated to Authorize User
Search	Search	Search Content, Search License
Storage and Retrieval	Resource Storage	Store Content
	Resource Retrieval	Post Content, Deliver Content
Protection	Key Storage	Associated to Create Content
	Key Retrieval	Associated to Authorize User
Tracking	Activity Report Creation	Store Event

### 3.5.2 Mapping SB3 to MIPAMS modules

This section describes the mapping of the building blocks defined in the subsection 3.5.1 to the services conforming MIPAMS platform. The correspondence between each SB3 and the corresponding MIPAMS Service is listed in Table 4.

**Table 4.** Correspondence between SB3 and MIPAMS Services.

<b>SB3</b>	<b>MIPAMS Service</b>
Access Control and Licensing	Authorization Service
Access Control and Licensing	Licensing Service
Authentication	Authentication Service
Content Management	Object Registration Service
Protection	Protection Service
Search	Search Service
Storage and Retrieval	Content Service
Tracking	Reporting Service

As it can be seen, there is almost a one-to-one correspondence between building blocks and MIPAMS services. Therefore, it would be easy to convert MIPAMS services into the proposed SB3.

### 3.5.3 Mapping SB3 Operations to MIPAMS operations

In this section, we define how SB3 operations map to MIPAMS Services' operations. For each operation, we provide the MIPAMS service it corresponds, the name of the operation in MIPAMS, the corresponding SB3 together with the

operation and a brief description of its functionality. Operations provided by MIPAMS services are implemented using existing standards. The specific standard used to implement each operation is indicated in the corresponding operation description. The complete mapping is listed in Table 5.

**Table 5.** Correspondence between SB3 and MIPAMS Services' operations.

<b>MIPAMS Service and operation</b>	<b>SB3 and operation</b>	<b>Description</b>
Authentication - login	Authentication - Login	Allows user to enter the system with her credentials. In response, a SAML v2.0 token is generated, which has to be passed to the rest of operations, which check its validity before execution.
Authorization - authorize	Access Control and Licensing - Authorization of User Actions	Checks if user has an appropriate license to perform an action over a digital resource. The authorization algorithm used is the one defined by MPEG-21 REL.
Licensing - createLicense	Access Control and Licensing - Permission Creation	It is used to create offers or licenses inside the system. If license creation is requested, it is checked that the corresponding offer exists. The format used for the serialization of the license is MPEG-21 REL.
Licensing - revokeLicense	Access Control and Licensing - Permission Revocation	It is used to revoke an existing license, which will not authorize user actions any more.
Protection - storeKey	Protection - Key Storage	Generates and stores an encryption key associated to a digital resource / object.
Protection - retrieveKey	Protection - Key Retrieval	Retrieves an encryption key associated to a digital resource / object. This operation can only be done after positive authorization.
Registration - sendObject	Content Management - Content Creation	Stores the information associated to one or more digital resources using the MPEG-21 DI format. For the definition of specific metadata, different standards depending on scope of the application implemented. The most basic one used is Dublin Core.
Registration - deleteObject	Content Management - Content Deletion	Removes the information associated to a digital object. Associated offers and licenses are also removed.
Reporting - saveER	Tracking - Activity Report Creation	Stores the information associated to the operations occurred in the system, like object creation, license creation or authorization of actions.
Search - executeSearch	Search - Search	Performs searches over different types of information in the system, digital objects, offers, event reports, according to the parameters passed.
Content - storeResource	Storage and Retrieval - Resource Storage	Uploads a digital resource (image, video, audio, document, etc.) associated to a digital object.
Content - retrieveResource	Storage and Retrieval - Resource Retrieval	Downloads a digital resource (image, video, audio, document, etc.) associated to a digital object.

### 3.5.4 Relationship between MIPAMS and MPEG-M

MIPAMS implementation and set up was previous [37] to the description of the Multimedia Service Platform Technologies (MSPT), also known as MPEG-M (ISO/IEC 23006), standardization initiative. MPEG-M is formed by several parts (5 at the present moment), whose aim is to define how devices, services and users interact in order to manage digital content.

Regarding MPEG-M, part 4 defines elementary services that can be combined to provide complex services. Some of them are already developed in MIPAMS, as shown in Table 6, where the equivalence between MIPAMS modules operations, SB3 operations and MPEG-M elementary services is shown. MIPAMS has also been used for the implementation of content management scenarios presented in subsection 3.2. These scenarios combine operations from different MIPAMS modules by means of the Workflow Manager module. This approach is closely related to another part of MPEG-M, part 5 (ISO/IEC 23006-5 Aggregated Services), whose aim is the definition of guidelines for the composition of complex services from elementary and external services.

**Table 6.** Correspondence between SB3 Operations, MIPAMS Operations and Elementary Services.

<b>SB3 and operation</b>	<b>MIPAMS Service and operation</b>	<b>Elementary Service (s)</b>
Authentication - Login	Authentication - login	Authenticate User
Access Control and Licensing - Authorization of User Actions	Authorization - authorize	Authorize User
Access Control and Licensing - Permission Creation	Licensing - createLicense	Create License, Store License, Identify License
Access Control and Licensing - Permission Revocation	Licensing - revokeLicense	Revoke License
Protection - Key Storage	Protection - storeKey	Associated to Create Content
Protection - Key Retrieval	Protection - retrieveKey	Associated to Authorize User
Content Management - Content Creation	Registration - sendObject	Create Content, Store Content, Identify Content, Process Content
Content Management - Content Deletion	Registration - deleteObject	Revoke Content
Tracking - Activity Report Creation	Reporting - saveER	Store Event
Search – Search	Search - executeSearch	Search Content, Search License
Storage and Retrieval - Resource Storage	Content - storeResource	Store Content
Storage and Retrieval - Resource Retrieval	Content - retrieveResource	Post Content, Deliver Content

## 4 Case Studies

### 4.1 DRM-enabled content access for mobile devices

This section describes how to implement one of the scenarios described in subsection 3.2. In particular, the scenario implemented is the one devoted to mobile devices, as it covers all the functionality provided by the SB3s, adapted to the specific features of mobile devices.

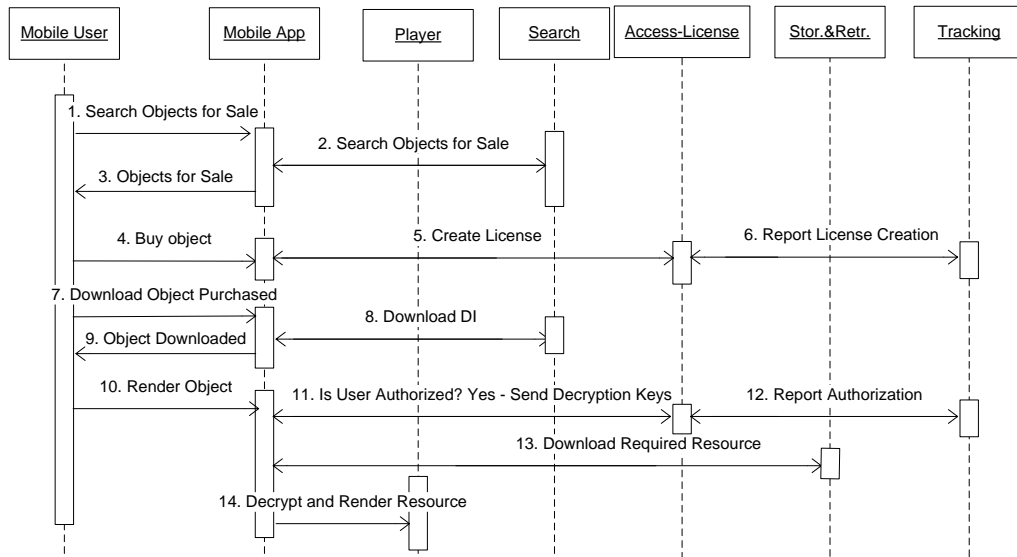
This scenario may have two different points of view, the one from the content distributor or seller and the one from the content purchaser or buyer. We will describe here how to implement the buyer point of view. In [29], a complete description of seller point of view can be found. The rest of the section describes the buyer use case. Afterwards, an implementation of this scenario that was developed as a demonstration to the MPEG committee of how to provide MPEG-M Aggregated Services over the MIPAMS platform is shown.

#### *4.1.1 Multimedia content management use case*

Figure 2 shows a sequence diagram to indicate the order of the operations that can be done using the mobile application from the buyer point of view. Operation order is as follows:

1. User selects Search option to look for the objects on sale. They can be filtered by Title and Creator.
2. Mobile App (MA) sends object search request to the Search module. Then, Search module sends the search result to the MA.
3. Objects on sale are presented to the user.
4. User selects an object from the ones presented. She has to select an offer from the ones provided by seller in order to purchase the object.
5. MA asks for license creation to Access Control and Licensing module.
6. Access Control and Licensing sends a report to Tracking module informing of the license creation.
7. User downloads object she has purchased to render its content.
8. MA requests Digital Item to Search module.
9. User receives object.
10. User wants to render the object.
11. Before rendering resource, MA asks Access Control and Licensing module for user authorization. If authorization is positive, keys for rendering content are provided.
12. Access Control and Licensing module sends a report to Tracking module informing of authorization.
13. User requests a resource, MA gets it from Storage and Retrieval module.

14. The received resource is decrypted and shown to the user. If user is not authorized, then the resource is not shown and user is informed of this fact. The login operation is omitted but it should be done before step 1.



**Fig. 2.** Object search, purchase, authorization and rendering on the mobile application.

#### 4.1.2 Implementation of the scenario using MIPAMS and MPEG-M

The use case presented in subsection 4.1 corresponds to the aggregated service described in subclause 6.4.3 of the standard ISO/IEC 23006-5 (buyer scenario). We have adapted it to describe how this scenario can be implemented when the user application is a mobile application, describing the interactions between the different SB3s needed to provide it. Specifically, it defines how a user can search for some content in the platform, purchase and render it into the mobile device after positive authorization (based on the license she has purchased).

For the implementation of the scenario, it is worth noting that only MIPAMS considers the specific application implemented (UA module) as part of its modules, but in this case standards usually do not apply. SB3 do not take into account user applications, as it is difficult to find standards for them, especially if they are platform-dependent. The user application is out of the scope of the MPEG-M standard, only Elementary Services and its aggregation is defined.

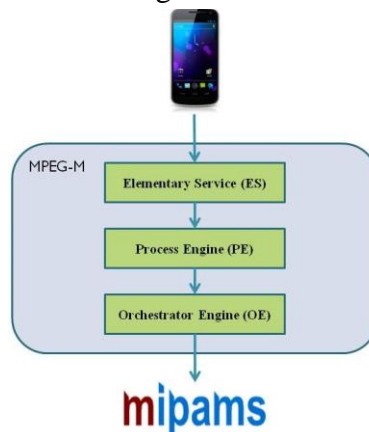
In order to provide the use case described in section 4.1, it is needed a running platform which supports the services required. In our case, we have implemented the mobile application scenarios adding an MPEG-M interface over MIPAMS operations. We implemented it in this way in order to demonstrate that the software provided by the standard could be integrated with an existing platform, thus providing interoperability with other platforms implementing MPEG-M.

The developed application [3] makes use of some Elementary Services in order to build an Aggregated Service that represents the buyer scenario described in the standard. The Elementary Services used are:



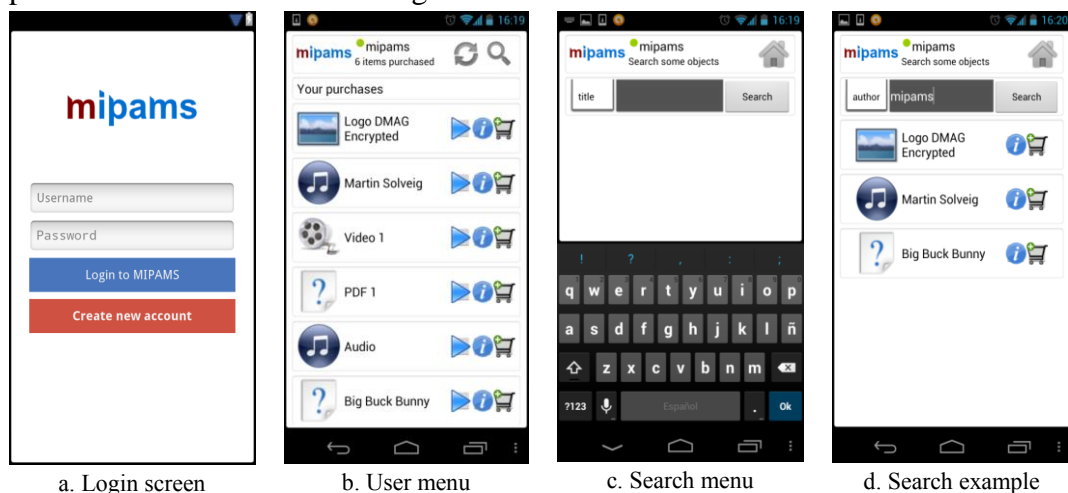
- Authenticate user in front of MIPAMS.
- Search license between the ones available in the system.
- Present license, showing the information it contains.
- Create license for a specific user and object.
- Authorize user, which checks if user has an appropriate license to perform a right.
- Render content after positive authorization.

In order to implement the Aggregated Service, we are providing a MPEG-M interface for MIPAMS. In other words, applications will call MPEG-M Elementary Services that will map to the MIPAMS services to be executed. The application architecture is shown in Figure 3.



**Fig. 3.** MIPAMS connection with MPEG-M.

The functionalities of the application implemented are presented below. Some screenshots and an explanation are provided. The login screen is depicted in Figure 4.a. It allows to login into MIPAMS by providing a username and a password. It also allows creating a new user.




**Fig. 4.** Some application screenshots.

When the user is logged in, the user menu is shown. The menu contains an action bar indicating the username, the number of items the user has purchased, a search icon and a refresh icon. The user menu is depicted in Figure 4.b.

The screen displays the content the user has already purchased in a scrollable list. The user can render the objects (with a previous license based

authorization) and get the metadata of both the purchased Digital Item and its licenses. The refresh icon allows getting again the purchased items.

By pressing the search icon, a new screen is displayed. A search bar allows the user to search by author or title of the content. When the user presses the search button, the results are shown in a scrollable list like the user menu. For each result of the search, the user can display either the information about the content or the information of the licenses that can be purchased. The search menu and an example of search result are depicted in Figure 4.c and 4.d.

The  icon displays the metadata of a Digital Item. It is accessible from both the user menu and the search menu. The information of the Digital Item and the resources it contains is presented as follows:

- At the top of the screen, the Digital Item information is presented. The information shown is title, creator, description and creation date.
- The information related to the resources contained in the object is presented below. The information presented for each resource is title, description and file format.

The licenses of the object can also be displayed if the “View licenses” button is pressed. The corresponding screenshot is shown in Figure 5.b.

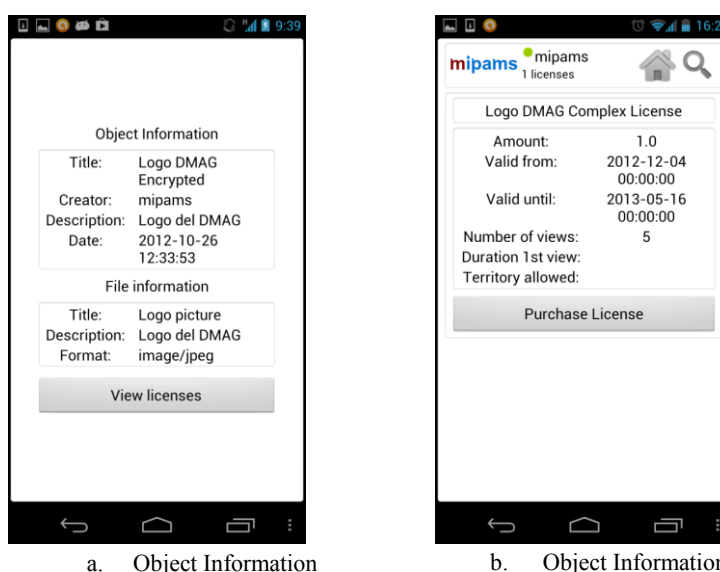



Fig. 5. Object and license information screen.

The  icon displays information about the licenses of the object. If the icon is pressed in the user menu, it displays the information about the licenses the user has purchased for this item. Otherwise, if the user presses the button from the search menu, it shows all the licenses associated to this object that can be purchased. The licenses are presented in a scrollable list with the following information:

- License title.
- The cost of purchasing the license. Different currency could be defined.
- A time interval in which the license is valid (i.e. the interval in which the user is able to render the content).
- The maximum number of times a user can view the content.

- The territory where rendering the content is allowed.
- The time interval in which the render is available from the first time the user started to render it (i.e. two days since the first view).

When the user presses the ▶ icon from the user menu, an authorization request is performed. The authorization grants the access to the content if there is at least one license that allows the user to render this object. If the authorization is positive, the content is downloaded and the default Android player opens the file to render it. An example of authorization and content rendering is depicted in Figure 6.

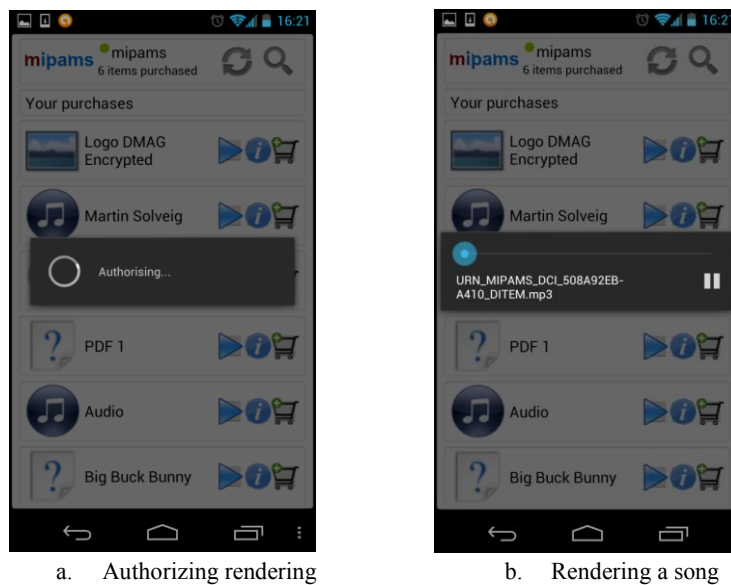


Fig. 6. Authorizing content rendering and rendering content in Android player.

## 4.2 Secure access to and modification of electronic health records

This section describes how secure access to protected electronic health records can be modelled with SB3. In this scenario, a user wants to access to the information contained in an electronic health record and modify it, adding new data. Furthermore, a role based access control (RBAC) approach has been followed, where the privacy (or access control) policies are based on roles rather than on specific users.

This idea was presented in [5] [35], where the issue of protection of patient's privacy was discussed. So, the objective is twofold. From the one hand, show that SB3 can be used not only for modelling multimedia content related scenarios. From the other hand, to show how SB3 are also usable for other research areas, like privacy protection in e-health.

### 4.2.1 e-health use case

Figure 7 shows a sequence diagram to indicate the order of the operations required to access and modify an Electronic Health Record (EHR) when the user has the needed permissions. These permissions are based on the role of the user, which may be different depending on the time of the day, the location, etc. For

example, a nurse may have the role ‘Nurse’ during the morning, but may become ‘Emergency Nurse’ during the night. In the second case, she will be allowed to access information from EHR's that do not correspond to their usual patients, due to its work in emergency turn. Operation order is as follows:

1. User has to log into the system in order to get the information regarding their credentials at that specific moment, specially her current role.
2. The EHR editor invokes login operation from the Authentication module and returns the result of the request. In this case, the user is authenticated.
3. The user is informed that she has been authorized.
4. The user wants to load an EHR to check for some results.
5. The EHR editor asks for authorization of access to the EHR to the Access Control and Licensing module. In this case, the user is authorized.
6. The user operation is tracked, sending a report to the Tracking module, which informs that the access has been granted to the user, including the EHR, the time and other information to facilitate future tracing of operations.
7. The access is granted to the user and the decryption key is returned.
8. Then, the editor asks for the complete EHR to the Storage and Retrieval module.
9. The editor decrypts the corresponding parts of the EHR depending on the user permissions and role.
10. The EHR allowed parts are shown to the user.
11. The user wants to add new information to the EHR.
12. The EHR editor asks for authorization of modification of the EHR to the Access Control and Licensing module. In this case, the user is authorized.
13. The user operation is tracked, sending a report to the Tracking module, which informs that the modification has been granted to the user, including the EHR, the time and other information to facilitate future tracing of operations.
14. The modification is granted to the user and the decryption key is returned.
15. Then, the editor adds the information to the EHR and encrypts it again, including the new element.
16. The editor sends the new EHR to the Storage and Retrieval module.
17. The user is informed that the modification has been done and that the EHR is stored.

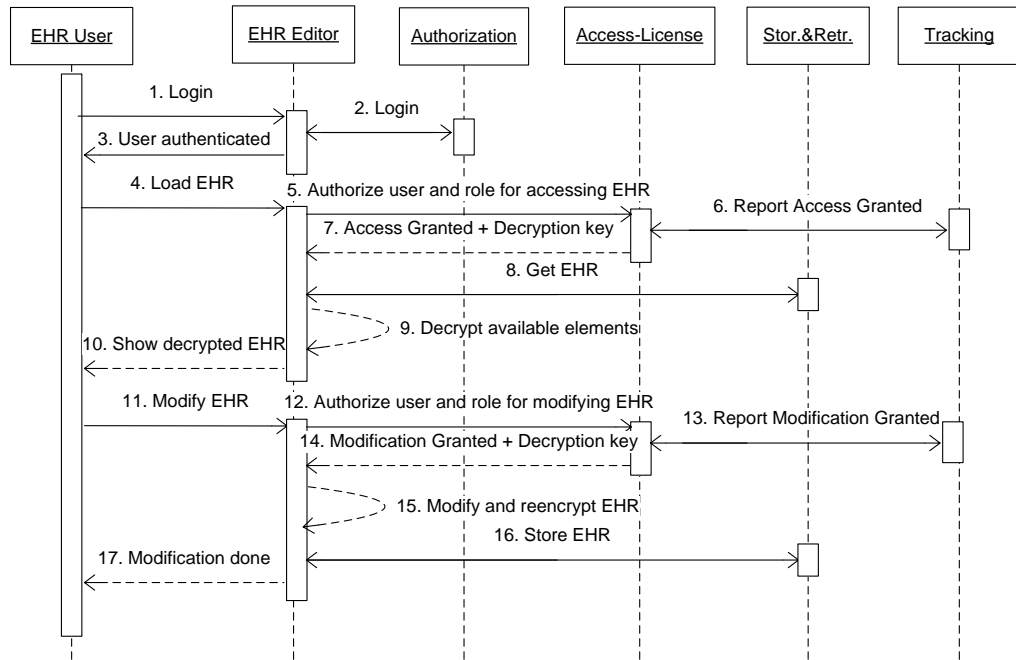


Fig. 7. Protected EHR access and modification.

## 5 Conclusions and Future Work

The emergence of new multimedia content consumption models thanks to connected smart devices (e.g. smartphones, smart TVs, consoles, etc.) adds a higher level of complexity to the development of services supporting these models. These content consumption models are covered by the ones described in [27], which are namely Content Licensing, Content Licensing plus authorization-based content access control or DRM-enabled content access control, which also considers mobile devices.

The recently approved MPEG-M [13] standard series provides with the tools for supporting these and newly described scenarios, thanks to the abstraction level and flexibility offered by Elementary and Aggregated Services. Nevertheless, two different drawbacks can be found in this standard at the present moment: The almost exclusive usage of MPEG technologies and the current absence of running platforms supporting it. To solve the first of these drawbacks, this paper proposes the definition of Standards Based Building Blocks (SB3), some basic building blocks described according to the high level features required by the content consumption scenarios analyzed in [27]. The main aim of SB3 is to identify different standards for each building block, in order to support not only content consumption scenarios, but also other application scenarios like learning management systems [36], health related information representation [5] [35] or e-government [32]. Another aspect, like interoperability between the standards identified for each building block could be further studied. To overcome the second drawback, a demonstration of how MPEG-M services are able to run over an existing platform, MIPAMS, is also described. In this sense, we present the

implementation of one of the scenarios defined in the standard from an Android mobile application. The back office functionality is provided by MIPAMS platform, accessed through an MPEG-M interface.

To show how to apply SB3 to other scenarios different from multimedia, an e-health use case describing how privacy can be preserved when accessing and modifying EHR's is described.

Next steps following this work may include the identification of new standards for each building block. Moreover, future work will continue with the definition and implementation of different application scenarios, like the one for e-health presented, based on the building blocks identified, without forgetting interoperability issues.

### *Acknowledgements*

This work has been partially supported by the Spanish government through the project "Protección, búsqueda e interoperabilidad de contenidos multimedia: Nuevas técnicas y aplicaciones" (PBIInt) (TEC2011-22989).

## **References**

1. ANSI/HL7. (2010). HL7 Clinical Document Architecture (CDA), Release 2.0.
2. Creative Commons. (2013). <http://creativecommons.org/licenses/>.
3. Delgado, J., Florido, J., Llorente, S. (2013). M28138: MPEG-M demo based on the MIPAMS platform, Input contribution to the 103th MPEG meeting held in Geneva in January 2013.
4. Delgado, J., Torres, V., Llorente, S., Rodríguez, E. (2011). Rights management in architectures for distributed multimedia content applications. In: Trustworthy Internet, Springer, 2011, ISBN 978-88-470-1817-4.
5. Delgado, J., Llorente, S., Rodríguez, E. (2012). Digital Rights and Privacy Policies Management as a Service. Consumer Communications and Networking Conference (CCNC), IEEE, Digital Object Identifier: 10.1109/CCNC.2012.6181035, Page(s): 527 – 531.
6. Delgado, J., Rodríguez, E., Llorente, S. (2010). User's Privacy in Applications provided through Social Networks. Second ACM Workshop on Social Media (WSM 2010)
7. Distributed Multimedia Applications Group (DMAG). (2013). <http://dmag.ac.upc.edu/>.
8. Eggersmann, M., Kausch, B., Luczak, H., Marquardt, W., Schlick, C., Schneider, N., Schneider, R., Theißen, M. (2008). Work Process Models. Collaborative and Distributed Chemical Engineering, LNCS 4970, pp. 126–152, 2008. Springer-Verlag. [http://link.springer.com/chapter/10.1007/978-3-540-70552-9\\_7](http://link.springer.com/chapter/10.1007/978-3-540-70552-9_7).
9. Fang Fang, C., Chien Sing, L. (2009). Collaborative learning using service-oriented architecture: A framework design, Knowledge-Based Systems, Volume 22, Issue 4, May 2009, Pages 271–274, Artificial Intelligence (AI) in Blended Learning — (AI) in Blended Learning, <http://www.sciencedirect.com/science/article/pii/S0950705109000185>.
10. Gartner. (2013). Definition of Service Oriented Architecture (SOA). <http://www.gartner.com/it-glossary/service-oriented-architecture-soa/>.
11. Gartner. (2013). Definition of Business Process Management (BPM). <http://blogs.gartner.com/it-glossary/business-process-management-bpm-2/>.
12. Internet Engineering Task Force (IETF) (2002) RFC 3280 Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile.
13. ISO/IEC. ISO/IEC 23006, Information Technology – Multimedia Service Platform Technologies – MPEG-M.
14. ISO/IEC JTC1 SC29/WG11, MPEG. (2013). The Moving Picture Experts Group, <http://mpeg.chiariglione.org/>.

15. ISO/IEC. (2013). ISO/IEC IS 23006:5 – Part 5: Service Aggregation.
16. ISO/IEC. (2004). ISO/IEC IS 21000:5 – Part 5: Rights Expression Language.
17. ISO/IEC. (2005). ISO/IEC IS 21000:2 – Part 2: Digital Item Declaration.
18. ISO/IEC. (2006). ISO/IEC IS 21000:15 – Part 15: Event Reporting.
19. ISO 13606-1. (2008). Medical informatics – Electronic healthcare record communication – Part 1 Reference Model.
20. ISO/IEC. (2013). ISO/IEC IS 21000:20 – Contract Expression Language (CEL). Approved as International Standard. Publication pending.
21. ISO/IEC. (2003). ISO/IEC IS 21000-3 – Part 3: Digital Item Identification.
22. ISO/IEC. (2006). ISO/IEC IS 21000-4 – Part 4: Intellectual Property Management and Protection.
23. ISO/IEC. (2008). ISO/IEC IS 15938-12 – Part 12: Query format.
24. ISO/IEC. (2011). ISO/IEC 9075-1:2011 – Part 1: Framework (SQL/Framework)
25. Kudumakis, P., Sandler, M., Anadiotis, A.-C., Venieris, I., Difino, A., Wang, X., Tropea, G., Grafl, M., Rodríguez-Doncel, V., Llorente, S., Delgado, J. (2013). Signal Processing: Image Communication, Elsevier Press, October 2013. DOI Bookmark: <http://dx.doi.org/10.1016/j.image.2013.10.006>.
26. Llorente, S., Rodríguez, E., Delgado, J. (2010). Secure Management of Social Networks Applications Data. Proceedings of the 8th International Workshop for Technical, Economic and Legal Aspects of Business Models for Virtual Goods.
27. Llorente, S., Delgado, J., Rodríguez, R., Torres-Padrosa, V. (2013). Standards-based Architectures for Content Management, IEEE Multimedia, IEEE, October - December 2013 (volume 20 number 4), ISSN: 1070-986X, DOI Bookmark: <http://doi.ieeecomputersociety.org/10.1109/MMUL.2012.58>.
28. Maroñas, X., Llorente, S., Delgado, J. (2011). Management and distribution of rights governed live cultural events. Proceedings of the 9th International Workshop for Technical, Economic and Legal Aspects of Business Models for Virtual Goods.
29. Maroñas, X., Llorente, S., Rodríguez, E., Delgado, J. (2012). Implementing mobile applications with the MIPAMS content management platform, Mobile multimedia communications: 7th International ICST Conference MOBIMEDIA 2011: Cagliari, Italy, September 5–7, 2011: revised selected papers, Pages 266-280. ISBN: 978-3-642-30418-7.
30. OASIS. (2005). Security Assertion Markup Language (SAML). <http://saml.xml.org/>.
31. OASIS. eXtensible Access Control Markup Language (XACML) v2.0. (2005). <http://www.oasis-open.org/specs/index.php#xacmlv2.0>.
32. Palkovit, S., Wimmer, M.A. (2003). Processes in E-Government – A Holistic Framework for Modelling Electronic Public Services, EGOV 2003, LNCS 2739, pp. 213–219, 2003. Springer-Verlag.
33. Postel, J., Reynolds, J. (1985). File Transfer Protocol (FTP). <http://www.ietf.org/rfc/rfc959.txt>.
34. Rodríguez Doncel, V., Delgado, J., Chiariglione, F., Preda, M., Timmerer, C. (2010). Interoperable digital rights management based on the MPEG Extensible Middleware, Multimedia Tools and Applications, vol. 53, no. 1, pp. 303-308.
35. Rodríguez, E., Delgado, J., Alcalde, G. (2011). Protection of patients' privacy by means of standard technologies. Proceedings of the 9th International Workshop for Technical, Economic and Legal Aspects of Business Models for Virtual Goods.
36. Simon, B., Retalis, S., Brantner, S., (2003). Building Interoperability among Learning Content Management Systems, WWW 2003, May 20-24, 2003, Budapest, Hungary, <http://www2003.org/cdrom/papers/poster/p107/p107-simon.html>.
37. Torres, V., Rodríguez, E., Llorente, S., and Delgado, J. (2004). Architecture and Protocols for the Protection and Management of Multimedia Information. Second International Workshop on Multimedia Interactive Protocols and Systems. MIPS 2004. November 16-19. Grenoble (France). Lecture Notes in Computer Science (LNCS), Vol. 3311, pp. 252–263. Springer Berlin Heidelberg New York. ISBN-10: 3-540-23928-6. ISSN: 0302-9743.
38. World Wide Web Consortium (W3C) Community and Business Groups. (2002). Open Digital Rights Language (ODRL) version 1.1. <http://www.w3.org/TR/odrl/>.

39. World Wide Web Consortium (W3C). (1999). Hypertext Transfer Protocol - HTTP/1.1. <http://www.w3.org/Protocols/rfc2616/rfc2616.html>.