DRM and Access Control architectures interoperability

Eva Rodríguez [1], Jaime Delgado [1], Adrian Waller [2], Darren Price [2] and Peter de Waard [2]
[1] Universitat Politècnica de Catalunya, Departament d'Arquitectura de Computadors,
Campus Nord, Mòdul D6, Jordi Girona 1-3, E-08034 Barcelona, Spain
[2] Thales Research and Technology (UK) Ltd., Worton Drive, Reading RG2 0SB, U.K.
E-mail: *evar@ac.upc.edu*

Abstract - *Digital objects are managed in a controlled way through the complete value chain by DRM systems. Access Control Frameworks manage access by users to resources. This paper presents a solution that enables users of both systems to work collaboratively. It is based on the definition of an interoperability Broker that provides users of both systems with transparent access and use of content taking into account users' roles and content usage rules. It consists of modules that provide interoperability between digital rights and access control rules, between protected digital objects and digital resources and to manage the user's roles in both systems.*

Keywords – *Digital Rights Management, Access Control, Collaborative Working*

1. INTRODUCTION

This paper presents a solution for Digital Rights Management (DRM) and Access Control Frameworks (ACF) interoperability. Firstly, the DRM and ACF architectures developed by the authors are presented. The DRM architecture enables the management of multimedia information in a controlled way through the complete digital value chain taking into account DRM and protection. The ACF manages access by users to resources (e.g. applications or data). Secondly, a solution is proposed that enables users of both systems to use digital content in a controlled way. This solution is based on a 'Broker' that provides interoperability between DRM and ACF access control rules, between digital objects and digital media and between protection information associated to digital resources of both systems. Moreover, the Broker manages the users' roles in both systems. Finally, a virtual collaboration scenario is presented to illustrate the two architectures interoperating.

2. DIGITAL RIGHTS MANAGEMENT INITIATIVES

The digital object creation process combines the protected digital assets with their related metadata. These objects can be governed by licenses expressed according to a Rights Expression Language (REL) and protected by means of different protection techniques, such as encryption (the most used). The governed digital objects are distributed to the different actors of the value chain. Finally, DRM players consume digital objects according to the terms and conditions specified in the associated licenses. Some participants of the distribution chain, as content creators or distributors, may want to monitor usage of their copyrighted material. Hence, DRM systems support the sharing of information about events related to content and peers that interact with the content.
Nowadays, there are several initiatives that specify a DRM system or the set of elements that make up a DRM system. Among the most relevant initiatives in the area we can find the MPEG-21 standard[1], Open Mobile Alliance (OMA) DRM[2], Windows Media DRM[3] and Apple Fairplay[4].

3. DRM ARCHITECTURE

This section presents the DMAG-MIPAMS architecture[5][6], sketched in Fig. 1, that we have developed to manage multimedia information taking into account DRM and protection.
This architecture aims to enable the management of multimedia content through the complete content value chain, from content creation to consumption by end users, including adaptation and distribution of content. DMAG-MIPAMS is a service-oriented DRM platform and all its modules have been devised to be implemented using the web services approach, which provides flexibility and enables an easy deployment of the modules in a distributed environment, while keeping the functionality independent from the programming language and enabling interoperability. Next sections present the functionality of each of the defined modules.

3.1. Content Server

The Content Server enables users to browse/select content, provides the content that the users request to user applications, and adds metadata to received raw content from providers and registers and stores the created digital objects.

3.2. Supervision Server

The Supervision Server authenticates and supervises actors and system components and manages event reports about content consumption.

Authorized licensed use limited to: UNIVERSITAT POLITÈCNICA DE CATALUNYA. Downloaded on July 07,2010 at 11:19:38 UTC from IEEE Xplore. Restrictions apply.

3.3. Governance Server
The Governance Server provides functionality for the creation and storage of licenses, online license-based authorisation and translation of licenses between different rights expression languages.

3.4. Protection Server
The Protection Server provides functionality for the protection of digital objects and for the generation, storage and delivery of protection keys and protection information.

3.5. Trusted Client
The Trusted Client module provides functionality for the creation and editing of digital objects, and for retrieving event reports, rights expressions, and protection and processing information.

4. ACCESS CONTROL FRAMEWORKS

ACFs manage access by users to resources (e.g. applications or data) for multiple systems or networks. They are particularly useful for Virtual Organisations (VOs), which are an ad-hoc integration of resources across organisational boundaries to support collaborative working. Characteristics of VOs include:

- Resources are owned by multiple organisations with multiple policies.
- Policies may need to be set up on demand, and may change over time at short notice.
- No common administrative point, security architecture or security mechanisms exist across the VO (one technical solution cannot be enforced).

Typically, access control is managed separately for individual systems. However, for VOs this can be impractical, both from an administrator's and end user's point of view (e.g. having to remember many passwords). ACFs deal with this problem by providing a simplified and consistent approach. Examples include Kerberos[7], Liberty Alliance[8] and WS-Federation (Web Services-Federation)[9]. Some are aimed at multiple scenarios, but many are tailored to particular requirements. E.g., in grid computing the requirement is, typically, to involve administrators as little as possible by delegating management to users. However, other scenarios may require more centralised control.

A common feature of ACFs is the use of "tokens" (e.g. attribute and authorisation certificates[10] [11], or generic policy tokens such as KeyNote[12] or Security Assertion Markup Language (SAML)[13]). Tokens provide users with the means to prove they have the rights to perform a certain action, without the need for direct involvement of central administrators. Most ACFs use only one token format, however, some use gateways to convert between different formats. These gateways handle the heterogeneity in formats and mechanisms that can exist amongst the organisations involved in a VO. WS-Federation[9] is a notable example that makes use of this concept.

5. ACCESS CONTROL ARCHITECTURE

We have developed an ACF (illustrated in Fig. 1) designed for VOs and multimedia data (note that this architecture is patent pending). We assume that data may be highly sensitive, leading to significant constraints on its use and an ACF that differs from previous work (albeit based on WS-Federation[9] to some extent). Similarly to the DRM architecture, the components have been designed using a WS approach, where "Servers" are WSs and "Agents" are WS clients. A prototype implementation has been produced using WS and SAML tokens. Each component is briefly described in the following subsections.

5.1. User and Service Agents
These agents intercept requests from users to access services, and ensure that authorisation is in place by communicating with the Servers to obtain and provide authorisation tokens to Service Agents.

5.2. Network Access Server
This server accepts authenticated requests to access its network and, if acceptable, returns an authorisation token in return. It acts as a token gateway by accepting requests from users in other networks using those networks' formats, and returning a token in its own network's format.

5.3. Application/Data Access Server
This server accepts Network Access Server tokens together with a request to access an application or data item. If acceptable, it returns a token in return, which can then be provided to the Service Agent.

5.4. Auditing Server
This server keeps a record of all access to services by users for auditing purposes, and to allow rapid revocation (see below).

5.5. Enforcement Server
This server uses information from the Auditing Server to immediately revoke access to services that a user is no longer permitted to access.

6. INTEROPERABILITY BETWEEN DRM AND ACCESS CONTROL ARCHITECTURES

Digital objects are managed in a controlled way by both DRM systems and ACFs. This section presents a solution (illustrated in Fig. 1) that enables users of both to work collaboratively.

Authorized licensed use limited to: UNIVERSITAT POLITÈCNICA DE CATALUNYA. Downloaded on July 07,2010 at 11:19:38 UTC from IEEE Xplore. Restrictions apply.

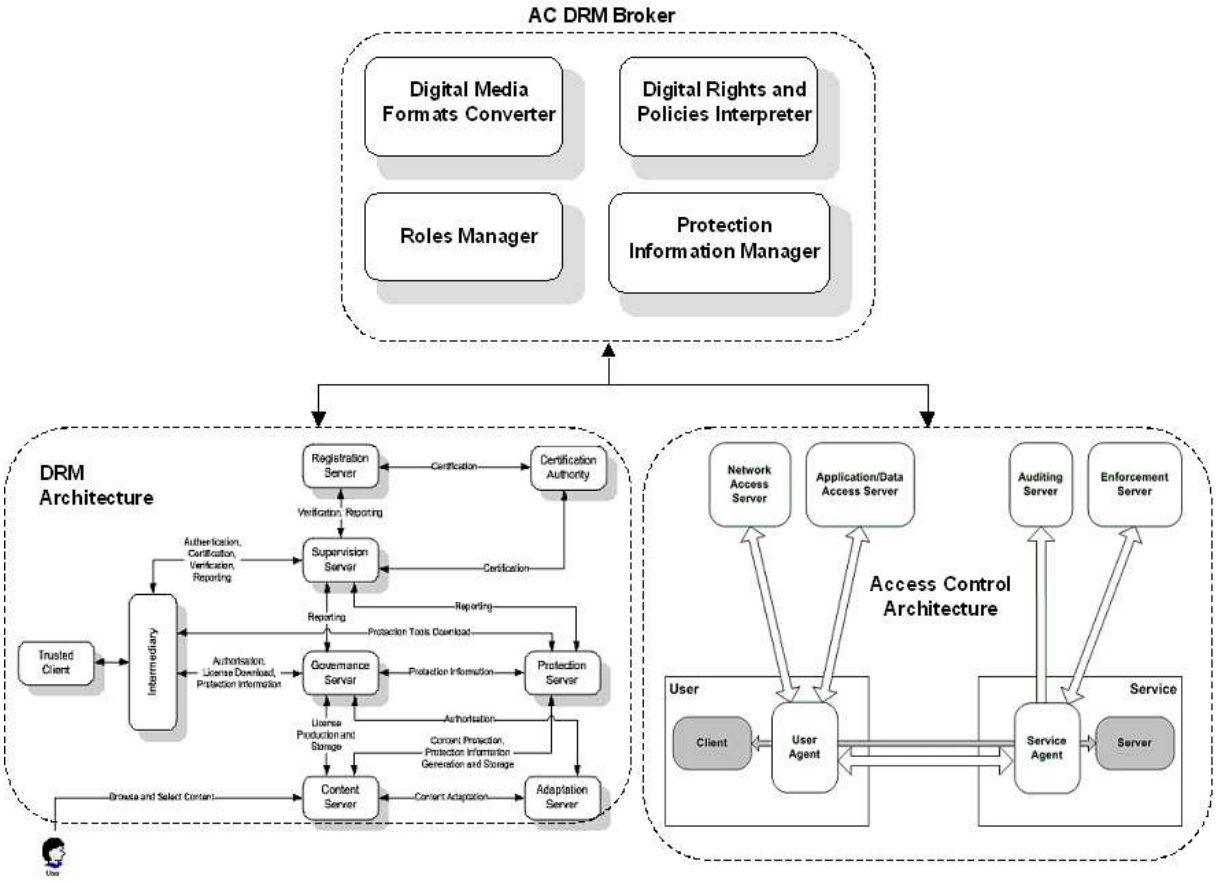

Fig. 1. DRM AC Broker

It is based on an interoperability Broker that provides users of both systems with transparent access and use of content taking into account users' roles and content usage rules.

The Broker consists of modules that provide interoperability between digital rights and access control rules, between digital objects and digital media and between protection information. Moreover, the Broker manages users' roles in both systems.

The modules of the Broker are detailed below.

6.1. Digital Media Formats Converter

In the DRM architecture, content is packaged and delivered to users within Digital Objects, defined according to the MPEG-21 Digital Item Declaration Language[14]. In the ACF, the content is distributed encrypted to the users of the system, without being packaged in any digital object. The Broker provides functionality to enable interchange of content and digital objects between the systems.

6.2. Digital Rights and Policies Interpreter

In the DRM architecture, licenses govern the content. A license grants to a user or group of users the sanction to exercise a right against a resource if a set of conditions have been previously fulfilled. In the ACF, access to content depends on defined access control policies that authorise a group of users (depending on their roles) to perform a set of actions over a set of resources. The Broker enables interoperability between licenses and access control policies through the generation of licenses and policies to govern content in both systems and by interpreting them to perform authorisation decisions for operations requested by users of both systems.

6.3. Protection Information Manager

In the DRM architecture, Digital Items are protected and information regarding the protection tools used is associated to the items. A Digital Item can be protected at any level of granularity, from a complete Digital Item to a specific digital resource. In the ACF, digital resources are protected as a whole using a pre-defiend algorithm. The Broker manages protection information and the protected content in both systems.

6.4. Roles Manager

The Roles Manager module manages the roles of users of the DRM and ACF architectures. In both, authentication of users involves the identification of users and assignment of roles to them. The Broker

Authorized licensed use limited to: UNIVERSITAT POLITÈCNICA DE CATALUNYA. Downloaded on July 07,2010 at 11:19:38 UTC from IEEE Xplore. Restrictions apply.

validates provided tokens and translates the user's roles (contained in the tokens) between the systems.

7. APPLICATION SCENARIO

We present a VO scenario to illustrate the two architectures interoperating. In the scenario, several organisations, including 'Aa' and 'Bb', have set up a VO using the combined architectures to allow them to work together on a project to design and produce a new 'widget'. This VO includes a shared repository (situated on Aa's network) that stores protected data which is downloadable by anybody, but can only be used according to the associated licences. Example use cases are given below for the widget design phase. Similar controls can be enforced for review and production phases (not shown here due to space constraints).

Use Case: Alice (an authorised Aa Designer) edits the design document.

- Alice authenticates herself to the Network Access Server on Aa and requests to activate her Designer role. The Server verifies she is allowed to, and returns a token for this role.
- Alice authenticates herself as a Designer to the Data Access Server on Aa using this token, and requests access to the design document. This Server asks the Governance Server to retrieve the relevant licences and check that access is allowed. It then requests a decryption key from the Protection Server and returns it to Alice.
- Alice decrypts the document and edits it.

Use Case: Alice stores the design document

- Alice contacts the Protection Server to apply protection to the updated document.
- Alice contacts the Governance Server to create the licenses for this document. Licences for Designers and Project Managers are created and stored by the Governance Server, to restrict access to these roles only.
- Alice formats the protected data into a new Digital Item using the Content Server, and stores it back on the shared data repository.

8. CONCLUSION

This paper proposes a solution for enabling Digital Rights Management (DRM) and Access Control architectures interoperate. The presented solution is based on the definition of a Broker designed to manage the user's roles in both systems and to facilitate interoperability between digital rights governing digital objects in the DRM architecture and access control rules in the Access Control Framework. The Broker also will manage protected digital objects and digital resources for both architectures. Finally, in order to illustrate how both architectures interoperate a virtual collaboration scenario is presented. In this scenario several organisations have set up a VO to allow users of both systems to work together on a project to design and produce a new widget.

ACKNOWLEDGEMENT

This work has been partly supported by the VISNET-II European Network of Excellence co-funded under the European Commission IST FP6 program (IST-1-038398) and by the Spanish Administration (DRM-MM project, TSI2005-05277).

REFERENCES

[1] MPEG-21 standard, http://www.chiariglione.org/mpeg/standards/mpeg-21/mpeg-21.htm
[2] Open Mobile Alliance (OMA), Digital Rights Management V2.0, http://www.openmobilealliance.org
[3] Windows Media DRM, http://www.microsoft.com/windows/windowsmedia/forpros/drm/default.mspx
[4] Apple Fairplay, http://www.apple.com/itunes/
[5] Torres, V., Rodríguez, E., et al. Use of standards for implementing a Multimedia Information Protection and Management System. In Automated Production of Cross Media Content for Multi-Channel Distribution (AXMEDIS 2005). IEEE Computer Society, 2005, 197-204.
[6] Torres, V., Delgado, J., et al. An implementation of a trusted and secure DRM architecture. In On the Move to Meaningful Internet Systems 2006: OTM 2006 Workshops (IS'06). Lecture Notes in Computer Science, vol. 4277. Springer-Verlag, 2006, 312-321.
[7] IETF Network Working Group, "The Kerberos Network Authentication Service (V5)", RFC 1510, September 1993.
[8] Liberty Alliance, "Liberty ID-FF Architecture Overview", Version 1.2.
[9] IBM and Microsoft Corporations, "Federation of Identities in a Web Services World", joint White Paper, Version 1.0, July 8, 2003.
[10] IETF Network Working Group, "An Internet Attribute Certificate Profile for Authorization", RFC 3281, April 2002.
[11] IETF Network Working Group, "SPKI Requirements", RFC 2692, September 1999.
[12] IETF Network Working Group, "The Keynote Trust-Management System Version 2", RFC 2704, September 1999.
[13] N. Ragouzis et al., "Security Assertion Markup Language (SAML) V2.0 Technical Overview", OASIS Draft, February 2007, sstc-saml-tech-overview-2.0-draft-13.
[14] ISO/IEC, ISO/IEC 2nd Edition IS 21000-2 – Digital Item Declaration

Authorized licensed use limited to: UNIVERSITAT POLITÈCNICA DE CATALUNYA. Downloaded on July 07,2010 at 11:19:38 UTC from IEEE Xplore. Restrictions apply.