Governed Media Distribution based on Nonrestrictive DRM

H. Castro, M. T. Andrade, A. P. Alves

INESC Porto, Rua Dr. Roberto Frias 378, 4200-465 Porto, Portugal,
e-mail: hcastro@inescporto.pt

Abstract

The growing pervasiveness of broadband Internet expands both the range of rich media assets that can be delivered as well as the universe of possible receivers. This in turn, opens the door for the creation of new forms of delivering rich media content, establishing a diversity of associated value chains and Business Models (BMs).
The full adoption of this new medium is something that is yet to be accomplished. It has been stalled by the hesitation of the key players in the content production and distribution industry which is closely related to the technical and legal difficulties in dealing with the free file sharing phenomenon.
Their strategy for the adoption of the Internet medium has generally involved the employment of restrictive DRM enforcing technology to preserve pre-Internet (legacy) operating modes.
Current approaches, within this context, have aimed at agilizing and facilitating the full adoption of this new medium by providing efficient, interoperable DRM enforcing tools to harness its power. However, the current resistance to DRM adoption, by some major Web media distributors, does not foretell a bright future for the use of restrictive DRM schemes for Internet based delivery of digital goods.
New solutions are thus required to enable the creation of new BMs, taking advantage of the opportunities offered by broadband Internet. In this context, the work described here proposes an alternative approach to the use of DRM, aiming at optimizing content distribution and usability and promoting content usage governance. The logic behind this proposal is based on the use of DRM schemes that favor content governance over rigid access restriction. These changes permit the development of new BMs which are very much inline with upcoming Internet businesses.
This work was developed within the framework of the European R&D project ENTHRONE.

Keywords

ENTHRONE, P2P, Content Governance, DRM, Rich Media, MPEG-21.

1 Introduction

The current trend of restrictive DRM abandonment, by some major Web media distributors indicates that these schemes may not be the most suited for Internet media delivery. ENTHRONE [1], like many other initiatives [7] [8], has relayed on such schemes.
This work proposes a modified approach to DRM employment within ENTHRONE, which favors content governance over rigid access restriction. The proposed changes allow the development of more versatile BMs, and thus are an added value.

This paper is organized as follows: section 2 provides an analytical overview of ENTHRONE‘s secure distribution architecture focusing on its overall efficiency and it’s appropriateness for some noteworthy emerging use cases. Section 3 pinpoints the limitations of ENTHRONE-like, restrictive DRM architectures from the viewpoint of business models and user demands and expectations. Section 4 describes the proposed solution to overcome the identified limitations. This solution can be seen as an alternative or complementary approach for the system’s distribution architecture. It is

based on the use of P2P, Event Reporting and DRM schemes, which privilege content governance over rigid access restriction.

2 ENTHRONE

2.1 Introduction

ENTHRONE (IST-038463) is an Integrated Project partially funded under the E.U. Framework Programme 6 for R&D, under the Thematic Priority "Information Society Technologies". ENTHRONE proposes an integrated management solution covering the entire audio-visual service distribution chain, including protected content handling, distribution and terminal reception. It aims at delivering an open and flexible end-to-end architecture that permits versatile new BMs, enabling business actors to enhance their services, better satisfying users' expectations. For that purpose the project extensively employs MPEG-21 for Digital Item declaration, usage environment description, DRM, data communication and content adaptation.

2.2 Secure Distribution Architecture

Within ENTHRONE, content is delivered under a licensing scheme. The access to it requires the existence of a valid license. Licenses consist of metadata associated to the content. They specify and condition the type of operations that can be performed upon the content and who is entitled to perform them.

ENTHRONE's content protection architecture is built around key based scrambling of digital content and a Key Management System (KMS). Content scrambling enforces the need for a scrambling key to access content, whilst the KMS ensures that only valid licensees can access the scrambling key. To assure that only license granted usages of content take place, the system relies on the use of smartcard certified terminal software. Additionally, the end-user of the content is assumed to be at home, possessing multiple multimedia-enabled devices from where content can be accessed. This leads to the notion of a Home Domain (HD) and all the requests are seen as being generated by the HD.

The two main components of the KMS are the License Server (LS) and the Smartcards (SCs). The former is responsible for issuing and delivering licenses, which are used in consumer devices that require access to protected content. The LS knows the content scrambling key (CSK) of each Digital Item (DI). Such CSKs are inserted by it in the licenses, which are made available after license purchasing.

According to the MPEG-21 principles adopted in ENTHRONE, content is transacted in the form of Digital Items (DIs). At the conceptual level, a DI is a package of interrelated multimedia resources together with associated descriptions (e.g. rights descriptions, etc), including the respective Digital Item Declaration (DID). Part 2 of the standard (Digital Item Declaration Language, DIDL) specifies a standardized method based on XML Schema, for declaring the structure of DIs. This XML file is the DID, which typically carries metadata or binary resources. It describes the composition of the DI in terms of resources, as well as of its structure in terms of the interrelationships among its several constituents.

Accordingly, when content is produced, its DID is also created. This DID, named the *sharing DID*, carries the LS's license, (named *sharing license*), which grants the LS the right to generate licenses for end-users. The CSK, carried in the license, is encrypted with the public key of the LS.

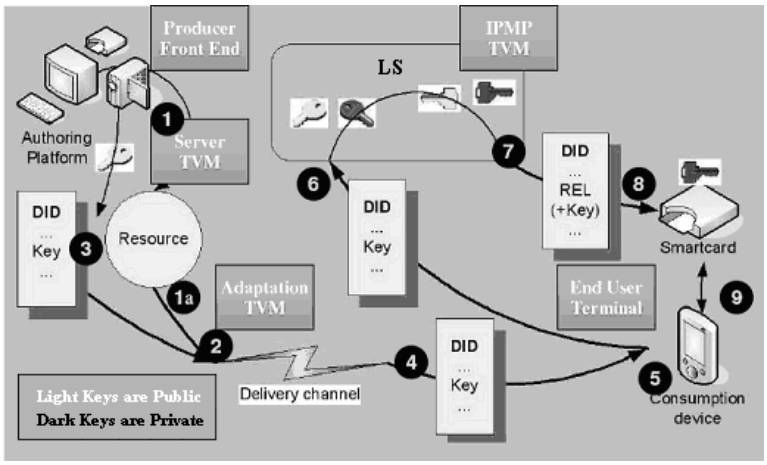

Figure 1 – ENTHRONE KMS Architecture (extracted from [2])

For an end-user to access content within his Home Domain (HD), he must first obtain the respective CSK, through the purchasing of a *domain license* from the LS. Thus the HD must send the *sharing DID* to the LS. The LS will retrieve the CSK from the contained *sharing license*, produce the *domain license* (containing the CSK, protected with the HD's public key) and deliver it to the user's HD. It will then be possible at the HD to access the content. This process is exemplified Figure 1.

The independence of the presented process from the content delivery mechanism allows it's reutilization in different delivery and consumption scenarios. This and the secure nature of content consumption in ENTHRONE, permits the safe direct sharing of content between HDs, whatever the exchange medium. In this way, ENTHRONE allows/expects that HDs engage in extra-Enthrone P2P sharing of encrypted digital content, what will contribute to ease the workload of content servers.

3 Present Limitations to Reliability, Business Models and Usages

3.1 Systemic Reliability Limitations

ENTHRONE's envisioned architecture presupposes the division of "bandwidth costs" between the central content servers (CCSs) and the individual HDs through sharing of media assets between the later. Still ENTHRONE provides no support for those activities. This strategy would likely involve the HD's engagement into extra-ENTHRONE P2P interaction, which will render the system dependent on external structures. The general unreliability of such structures, and of the content they deliver, will easily become a systemic week point which degrades user experience. This will drive users back to the content servers invalidating ENTHRONE's planned media sharing plans.

An analysis of the use cases defined in ENTHRONE [6], reveals that if the previously mentioned options for DI sharing are employed, the system's performance for some of them (Education Content Delivery, Professional High Quality Video Contribution) may be harmed, given the demands imposed by the distribution of large volume media assets, and by the small interval of content usefulness.

It would be beneficial if the HD-2-HD sharing of DIs was maintained and supported by a reliable ENTHRONE managed infrastructure, monitoring and enforcing a fine grain transfer of information between HDs, diminishing bandwidth strains and increasing content availability and overall service quality.
ENTHRONE can do this by providing a system which collects, and supplies the HDs with DI tracking data, and by technically enabling the HD-2-HD content retrieval.

3.2 Business Models and Usages Limitations

This chapter presents two plausible and hypothetic use cases/business models where the usage of content governance and open distribution is exploited, as opposed to a simple restrictive access policy. A brief analysis then presented, on the limitations presently imposed by ENTHRONE's secure distribution architecture to their full adoption.

3.2.1 Usage and Business Scenarios

Governed and Paid P2P Download of Unencrypted Video (1)
Video@Request is a paid video on demand internet service. It offers users the possibility to choose from a vast library of video content, purchase the media asset they desire and download it. The video content is distributed in an unencrypted way, but the video data is watermarked (in an individualized way), and attached to the video data itself is content governance related metadata. The removal of the associated information implies a loss of content quality.
The trusted proprietary software applications which allow the consumption of this video format do not restrict or condition content access to the presence of any license, even if they do exist at the system center. Still the rendering software collects information regarding the usages to which the content is subjected and reports this information back to the system's Content Governance Center (CGC).
Through the analysis of the received reports the CGC will be able to detect patterns of legitimate or abusive usage, to trace the original (legitimate) content leakage points, and to gather information on user behavior. Using such data a content producer or distributor is able to take action either to optimize its operation or to legally combat illegitimate use of its content *a posteriori*.

Open Broadcast of Advertisement Sponsored Internet TV (2)
OpenInternetTV is a free internet TV service, which any user can access trough certified terminal software. The TV content contains both shows and inline advertisements. Attached to the video stream descriptive metadata is also sent, which prompts the terminal software for event reporting information regarding user behavior.
The terminal software gathers information regarding, for instance, the user preferred types of content, the number of times a specific content is replayed (after initial reception), the advertisements which arouse most interest on the user (for instance by

watching if the user replays it or increases the sound volume during the commercial), etc. The gathered information is sent to a CGC for collection and analysis with the objective of using it for overall system optimization and user satisfaction.

3.2.2 Analysis

ENTHRONE's secure distribution architecture and access permission approach presupposes that value is directly derived from DI access permission selling and imposes a strict access granting policy.

Nonetheless, there are informational goods and services, whose distribution could be more attractive if performed in an opened manner, with revenue collection not from direct sale of content access rights but, from associated services or goods.
Furthermore, it would be, in any case, advantageous if content usage information is feedback to the content rights owners. Such a content usage monitoring system would allow the producers and distributors to have a detailed knowledge (or possibly control), of their product's production/diffusion/consumption circuit. This information could then be used for purposes such as fighting rights infringement, improving consumer satisfaction, etc.

Usage and business scenarios as those presented above have their enforcement impaired by ENTHRONE's adopted access granting strategy, given the lack of support for alternative forms of access policies (in both scenario 1 and 2), and the lack of support for content governance or the extraction of value from such governance (in scenario 2).
Accordingly, ENTHRONE would greatly benefit from the introduction of governance and consequent agility in terms of content access policies and gain derivation.

4 Proposed Solution

4.1 Conceptual Approach

A change in ENTHRONE's content diffusion structure is necessary to increase the overall content availability, minimize the bandwidth load on all systems entities and create new businesses opportunities. That change must provide support for reliable sharing of DIs (and DI tracking data) between HDs. P2P exchange should be adopted for this task. If centrally monitored, it is efficient and scalable. Furthermore, DIs should be shared in a fragmented manner so as to permit a more efficient retrieval from multiple simultaneous sources.

The system must also provide centralized content governance facilities, which will handle, among other tasks, the mentioned DI tracking operations. Such facilities, with the added supervising capacities they provide, also allow the supporting of alternative and more complex DRM schemes and business models

For the implementation of the mentioned additions, standard, interoperable and open tools should be employed, to assure intersystem interactivity and maximum user satisfaction. The MPEG-21 standard is a normative open framework for multimedia declaration, delivery and consumption for the usage of all delivery/consumption chain players. It possesses the necessary tools and presents very fitting characteristics for

tasks at hand and is thus the chosen solution, notably its part 15, the Event Reporting specification [3].
MPEG-21 Event Reporting provides a standardized format for describing so-called events reports, and event report requests. The key concepts of this standard are 1) the events, which consist on the occurrence of reportable activities; 2) the event report (ER) which consists on the standard representation of an event as specified by the related event report request (ERR); and 3) the ERR, which is defined as "a request to report an event".

4.2 Architectural Requirements

Some extra tools and entities are necessary to add P2P DI retrieval and monitoring and governance capability.

Besides the previously introduced *sharing DID* and *domain DID*, a new, centrally managed and distributed MPEG-21 DID, is necessary, for the transport of DI tracking data, the *p2p DI fragment tracking DID* (*p2pTrck DID*). It will carry information mapping specific DI fragments to the HDs which supply them, as well as ERRs (regarding content usage), to be complied with by the terminal equipment.
A new entity must be added to ENTHRONE, for the governance of DI usages, the Content Governance Centre (CGC). It will handle the DI tracking activities, specify the ERR data and manage its feedback, using it for the production and maintenance of the *p2pTrck DID*.

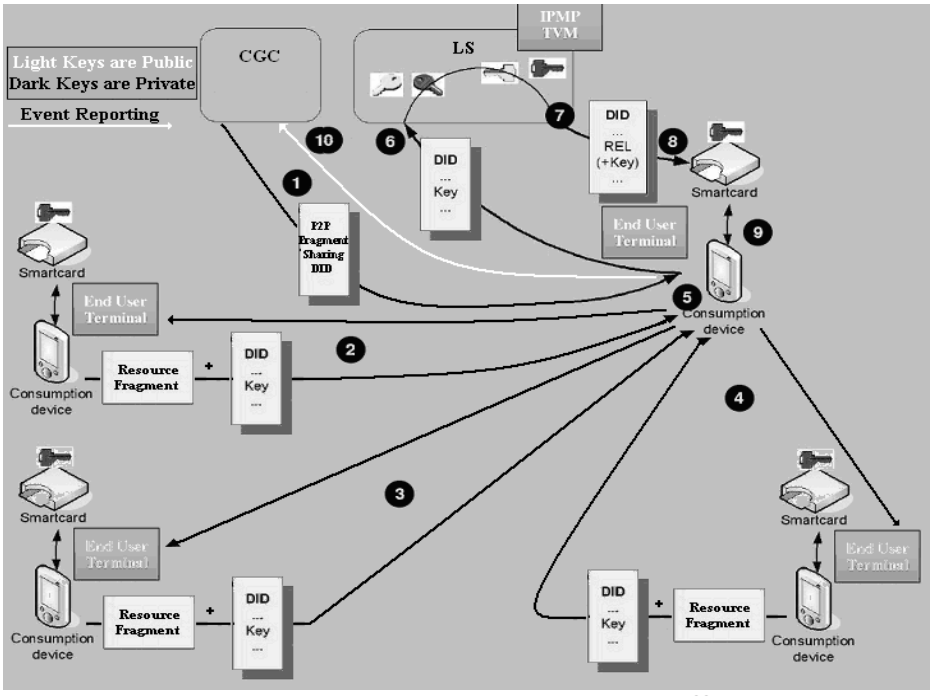

Figure 2 - Governed P2P DI Fragment Diffusion

When a DI is desired the local HD obtains an updated *p2pTrck DID* from the CGC, and employs its data to retrieve the appropriate *sharing DID* and all the fragments of the DI from the relevant HDs. It then contacts the LS to obtain/purchase its specific *domain DID* in order to obtain the CSK.

The DI is locally stored for relaying, and, complying with the ERR metadata in the *p2pTrck DID*, the HD will inform the CGC, and the later will update the appropriate *p2pTrck DID*. This process is depicted in **Error! Reference source not found.**.

Step 1 represents the retrieval of the *p2pTrck DID*. Steps 2, 3 and 4 represent the retrieval of all DI fragments and reconstitution of the DI. Steps 6, 7, 8 and 9 represent the retrieval of the *domain DID*. Step 10 represents the sending of the ER metadata to the CGC. Content decryption and consumption will be the final stage.

Furthermore, the CGC may require the HDs to report on a variety of other events. Such information may advantageously be used for multiple purposes such as, *a posteriori* digital rights enforcement, service optimization, gains maximization or customer satisfaction maximization. This will enable the supporting of complex and more open DRM schemes and business models.

The points below, present a more detailed vision of the necessary extra components.

CGC Sub-System and System's Operation

The CGC is responsible for the generation, distribution and maintenance of the *p2pTrck DID*, as well as for coordinating the system's Event Reporting sub structure.

The CGC is to be a server module apart of the ENTHRONE system's centre (ESC). When a DI is "inserted" in the system a *content DID*, which declares it, is generated by the Content Producer (CP) and uploaded to the ESC. That DID will indicate if the represented DI is subjected to P2P distribution. In such a case, at DI insertion time, the ESC will inform the CGC, and the later will initiate a new *p2pTrck DID*, which will store the all tracking data of the DI and its fragments.

At content consumption time the ESC will determine if a user requested DI is under P2P distribution and if so it will retrieve the appropriate *p2pTrck DID* form the CGC and send it to the terminal side, where it will be used to locate and retrieve the DI fragments. Upon copy of any DI fragment, in compliance with the MEG-21 ERR metadata in the *p2pTrck DID*, that operation is reported back to the CGC, which updates the corresponding *p2pTrck DID*.

Furthermore, the ERR metadata can prompt the feedback of other reports regarding content rendering, manipulation, and consumption preferences, etc. At the CGC this data may be used for rights infringement monitoring, user and usage profiling and other purposes, aiming at promoting consumer faithfulness and optimizing gains.

P2P DI Fragment Tracking DID

This DID will be the standard MPEG-21 vehicle of ERR and DI tracking metadata between the CGC and the HDs. Bellow is an example of a *p2pTrck DID* in Figure 3.

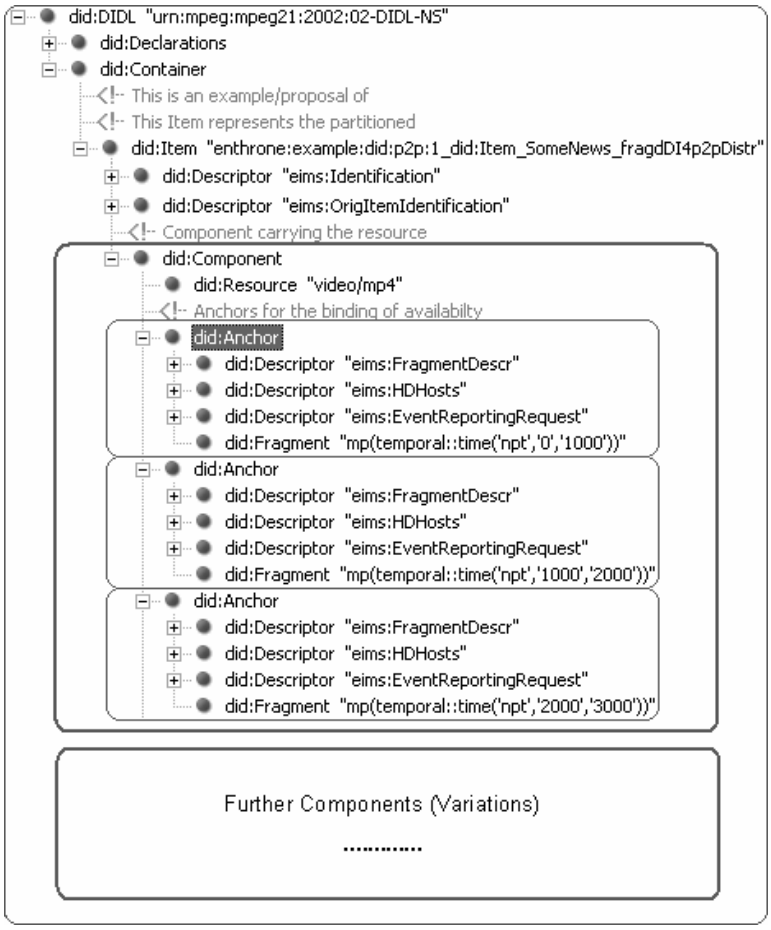

Figure 3 – P2P DI Fragment Tracking DID Structure

Such a DID represents a DI which is the partitioned version of the original DI. In the presented example the enclosing DI is identified by "*enthrone:example:did:p2p:1_did:Item_SomeNews_fragdDI4p2pDistr*". It carries two descriptors:

- eims:Identification – which carries the system wide unique identification of the present DI.
- eims:OrigItemIdentification – which carries the system wide unique identification of the DI of whom this DI is a fragmented version

Each Component child of the Item represents a technical variation of it (all of which have semantically equal content), and contains a Resource element referencing the original media asset. It also caries an Anchor element for each DI fragment.

Anchors use MPEG-21 part 17 [4] metadata to specify a range (the fragment) within the asset identified by the Resource within the parent Component, and employ Descriptor elements to bind it to information regarding the fragment's serial number (Descriptor eims:FragmentDescr), the available HDs for its P2P delivery (Descriptor eims: HDHosts) and the ERR metadata (Descriptor eims: EventReportingRequest, MPEG-21 part 15 [3]) to be complied with by the terminal.

5 Conclusions

This work describes an approach to media content distribution which aims at providing a framework for the support of new business models where revenues can be obtained through means other than selling of licenses, whilst providing efficient utilization of resources and addressing users' expectations. In particular it presents an extension to the architecture and functionality of the ENTHRONE project through the introduction of, standard MPEG-21 based, intertwined P2P content diffusion, monitoring and governance. It provides the system with powerful, scalable, standard and interoperable tools which enable it to support a vast range of more complex and flexible content distribution modes, DRM schemes and business models. It also allows rights owners and content deliverers to have a broader more pervasive and detailed knowledge, as well as control, of the chain of DI diffusion and consumption for a longer period of the DI's useful lifetime.

6 Acknowledgements

This work was in part supported by the EC under the FP6-IST programme. The authors would like to thank their colleagues of the ENTHRONE project for their fruitful collaboration in the development of the work here described.

7 References

[1] ENTHRONE Web Site (2004), http://www.ist-enthrone.org/, (Accessed 28 February 2008)
[2] Enthrone Consortium (2007), "*D14i: MPEG-21 IPMP and DMP compliance tools*", Enthrone Deliverable.
[3] MPEG-21 (2006), "*ISO/IEC FDIS 21000-15:2006(E) MPEG-21 - Part 15: Event Reporting*".
[4] MPEG-21 (2006), "*ISO/IEC FDIS 21000-17:2006(E) MPEG-21 - Part 17: Fragment Identification of MPEG Resources*".
[5] MPEG-21 (2005), "*ISO/IEC FDIS 21000-2:2005(E) MPEG-21 - Part 2: Digital Item Declaration*".
[6] Enthrone Consortium (2007), "*D02: Pilot architecture and services definition*", Enthrone Deliverable.
[7] iTunes Store Web Site (2008), http://www.apple.com/itunes/store/, (Accessed 28 February 2008)
[8] Napster 2.0 Store Web Site (2008), http://free.napster.com/, (Accessed 28 February 2008)