An Introduction to Interoperable Digital Rights Locker

Eric Diehl
Technicolor
Rennes, France
eric.diehl@technicolor.com

Arnaud Robert
The Walt Disney Company
Burbank, USA
Arnaud.robert@disney.com

ABSTRACT
This document introduces the concept of an Interoperable Rights Locker which uses two elements: a digital rights locker that manages the consumer rights and a single interoperable format which enables portability. This concept is the most advanced model of DRM interoperability. The concept is illustrated by Disney's KeyChest system.

Categories and Subject Descriptors
D.2.11 [**Software Engineering**]: Software Architectures – *Domain-specific architectures;* K.5.1 [**Legal Aspects of Computing**]: Hardware/Software Protection – *Licensing, Proprietary rights*

General Terms
Security

Keywords
Digital Rights Management, DRM, rights enforcement, rights locker

1. INTRODUCTION
Interoperability of Digital Rights Management (DRM) is a very popular topic, and has been for quite some time [4]. Consumers expect to have a digital media experience that is as flexible and seamless as the DVD model: buy anywhere, play anywhere. While they serve a necessary business imperative, current implementations of DRM systems are perceived by consumers as limiting and frustrating.

The lack of interoperability and capabilities of current DRM solutions affect all stakeholders: consumers, device manufacturers, distributors [1], and content providers.

There are really two solutions: make DRM a standard or make DRMs interoperable. The former has a substantive set of issues from technology, security, and business standpoints. So there is clearly a need to have an interoperable solution and one that fulfills four goals [5]:

- Transfer content between devices implementing different DRM systems.
- Consistent usage rights between DRM systems in a predictable and understandable way for the customer.
- The different DRM systems must trust each other.
- Customers must have the ability to play content beyond the existence of a particular distributor or technology provider.

DRM'10, October 4, 2010, Chicago, Illinois, USA.

2. RELATED WORKS
The first initiative that worked on interoperability was initiated by the Digital Video Broadcasting group (DVB) in the 90s. DVB standardized the format of the video selecting MPEG2 as both the codec and container. After many years of collaborative work, DVB issued the DVB SimulCrypt standards [3] . In fact, DVB fully defined the content protection layer as illustrated by Figure 1. DVB defined the scrambling algorithm used to protect the essence: DVB Common Scrambling Algorithm (DVB-CSA), then defined two types of licenses: Entitlement Control Messages (ECM), and Entitlement Management Messages (EMM). DVB's definition of ECM and EMM is limited to a minimum:

- The header to be able to parse the stream and extract the right data packet
- The size of the ECM and EMM

DVB does not define the internal structure of ECM and EMM, neither their protection. Each Conditional Access System provider manages them in its own proprietary way. Each CAS uses its own internal format, its own encryption scheme and its own key management system.

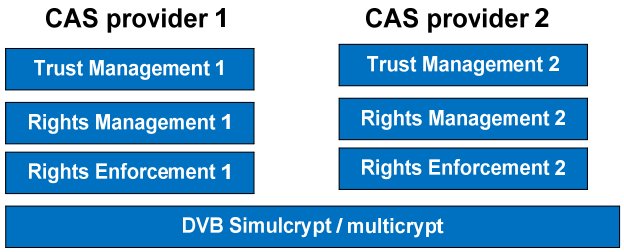

Figure 1. DVB interoperability scheme

Lesson: Using one unique common format and scrambling algorithm for the essence does not reduce the overall security of the system and is a potential success factor.

The second notable initiative is CORAL [7]. CORAL is a consortium of several tens of members. Founded by Intertrust, Philips, Matsushita, Samsung, Sony, and Twentieth Century Fox Film Corporation [7], CORAL issued its first specifications on November 2005 and the final set in October 2007.

CORAL interoperability is built on top of two main elements:

- a framework that ensures security and manages trust
- a pivot description of usage rights, so called Rights token

Although there are have been different initiatives to define a common Rights Expression Languages (XrML, ODRL), most DRMs use their own language to describe the usage rights. Furthermore, DRMs do not all support the same usage rights. This has a consequence that, when passing from one DRM to another one, resulting usage rules may be altered and likely more restrictive than original ones. To solve this issue, CORAL uses a pivot format. Every piece of CORAL-protected content has a 'license' described in a common "lingua franca". The license, named *Rights Token,* contains the following mandatory information: *Principal P, Resource R and Usage model U*. Coral splits the handling of content into three phases:

- The acquisition phase that uses the DRM independent Rights Token. When content provider creates the Coral-protected content, it generates a Right Token describing the usage rights that will be associated to the content. This Rights Token will be attached to the Content License in the DRM native license
- The consumption phase that is based on DRM native licenses.
- The mediation phase: When a consumer acquires protected content, a rights mediator translates the associated Rights Token (found in the DRM native license) into a license compatible with the DRM of the targeted player. The same content may be accessible by devices using different DRM, each using its own license format. Each time, the rights mediator will translate the Rights Token into corresponding license.

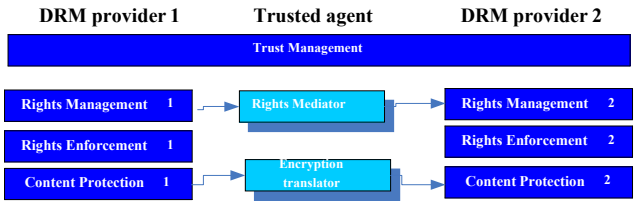

Figure 2. Interoperability through translation

CORAL's approach, sometimes called intermediation approach, is extremely simple. Device A supports only DRM A. Device A is requested to play content protected by DRM B. Device A asks a trusted agent to translate content and content license so that it is protected by DRM B. First, the trusted agent verifies that the operation is authorized. Then, in its secure environment, the trusted agent translates the license of DRM A into the equivalent license of DRM B, and descrambles the content and re-scrambles it with the bulk encryption of DRM B. It returns the same content but protected by DRM B. The latter operation may be skipped if local agents enable it: for instance, content may be descrambled, re-scrambled using a dedicated link protection system and re-scrambled using the sink DRM technology algorithm. Note that if local agents are not allowed (or able) to perform local re-scrambling, the content has to be re-acquired entirely, which is someties seen has one of the major Coral's drawbacks.

Lesson: The use of a "lingua franca" that defines the rights is mandatory for interoperability.

All these initiatives and requirements have led to a new concept: the Interoperable Rights Locker.

3. CONTRIBUTION

The Interoperable Rights Locker is mainly anchored on three pillars:

- An online repository of the usage rights acquired by the customer: the digital rights locker or DRL
- A unique Rights Expression Language that describes the usage rights
- An interoperable format: a common file format for the media essence, describing the container, the codecs, the scrambling algorithm(s) and metadata

Figure 3 illustrates the principle of Interoperable Rights Locker using the four-layer model [2]. Each content asset is protected by a common content protection layer, in other words every client implements the same descrambler. The usage rights are stored inside the digital rights locker server using a single Rights Expression Language. Furthermore, the digital rights locker securely stores the keys which were used to scramble content assets. Each client uses its own proprietary DRM license system.

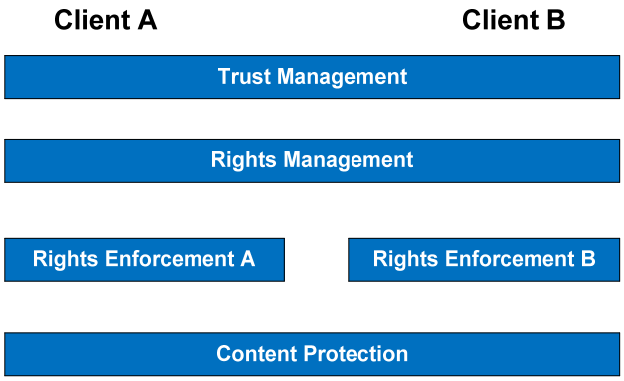

Figure 3. 4 layers for Interoperable Rights Locker

3.1 The actors

The main actors/roles of the Interoperable Rights Locker are:

- Content owner provides the content asset.
- Distributors offer content assets to consumers.

- Packager prepares the piece of content for distribution.
- The Digital Rights Locker records the rights granted to a consumer by Distributors.
- The Device renders, if authorized, the protected content
- The DRM license server generates and provides the DRM license that will manage access to the content asset.

3.2 Preparation phase

To use an Interoperable Rights Locker, a content owner enrols at the digital rights locker. Once enrolled, the content owner registers its pieces of content into the digital rights locker. When the content is registered, a secret key, here after called Control Word (CW) is randomly generated, used to scramble the content and is securely stored inside digital rights locker with other characteristics of the content.

To take advantage of the digital rights locker, a distributor must be enrolled. This allows registering consumers and to create or update consumers' usage rights. The usage rights define the consumption conditions such as subscription, electronic-sell through (EST), Video On Demand (VOD), rental, play once, and so on. Usage rights can also define the set of devices authorized to access the asset.

3.3 Viewing content

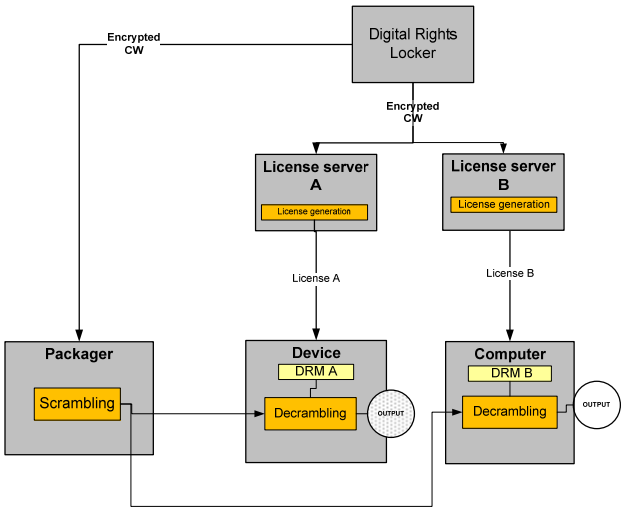

Figure 4. Simplified schematic of Interoperable Rights Locker principle

Let us assume Alice purchased from the distributor the rights to view a movie "M" on all her registered devices in a sell through transaction model. She owns a mobile device that supports DRM A and also owns a computer that supports a different DRM, DRM B. The distributor can record with the digital rights locker the fact she purchased an EST license for her mobile device and her computer.

Alice then receives a protected media file containing the movie "M". When she plays the movie on her mobile device, the DRM A client requests a license using a URL obtained from the content or a default URL. The URL points to the digital rights locker that has information about the movie M and Alice. Given that the request is coming for Alice and from her mobile device, the digital rights locker requests the license server A to generate a license for Alice's device with the usage rights and CW corresponding to movie "M". License server A packages this information into its proprietary license format and sends it to the mobile device. The DRM A client opens the license, validates the user and the rights and if all is validated, provides CW to the descrambler and Alice can view movie "M".

When Alice wants to play back the same movie "M" on her computer, the DRM B client must now request a license. Using the same flow as previously described, once the rights are validated, the license server B will generate a license containing the CW and access rights information to the DRM B client on the computer. The DRM B client validates the access rights and provides CW to the descrambler; Alice can now watch the same movie "M" but this time on her computer.

Now that the main flow is established, let us describe an interesting use case. Let's assume that a movie is offered in an early release window at a premium, and after a few months it is made available in a traditional window. The content protection requirements for the two offerings will most likely differ in certain aspects and therefore the viewing devices for the two offerings will have different DRM clients. For illustration purposes, let's say that DRM A meets the requirements of the early window, and DRM B meets the requirements of the latter window (note: it is understood that DRM A also meets the requirements of the latter window). . Per our stated principles, the asset is packaged using the single interoperable format. During the early release period the digital rights locker will only allow license server of DRM A to issue licenses and once the movie becomes available in the second window, the digital rights locker will allow the license server of DRM A or B to issue licenses. The transition from premium content to usual content therefore does not require repackaging the movie, thanks to the single interoperable format as well as the role of the digital rights locker.

Figure 5 provides a different view of the interactions between the different actors adding the distributor. The distributor has to register in the digital rights locker to participate and only registered distributors can communicate with the digital rights locker. Similarly, only registered license servers may query rights and obtain control words (CWs). The trust management layer ensures a granular management of authorized parties. Furthermore, it facilitates secure exchange of information between the players.

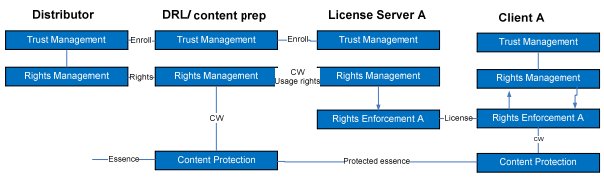

Figure 5. Interaction between Interoperable Rights Locker actors

4. AN EXAMPLE: KEYCHEST

The Walt Disney Company designed an Interoperable Rights Locker system: KeyChest [6]. The presentation will disclose more details about this first implementation of Interoperable Rights Locker.

5. CONCLUSIONS

The Interoperable Rights Locker architecture offers many advantages, amongst which:

- Offers consumers a trusted place where their rights are stored and managed;
- Simplified preparation of assets across the distribution chain;
- Flexibility in access rights and business models;
- Ease of integration with the distributors via simple APIs;
- Ease of implementation for device manufacturers (they have nothing specific to do);
- No dependency on DRM providers, allowing access to assets to survive any one being disappearing;
- No dependency on distributors, allowing access to assets to survive one being no longer active;
- Support for un-tethered (off line) consumption.

6. REFERENCES

[1] Center for Content Protection 2008. Technology Issues on the Use of DRM.

[2] Diehl, E. 2008. A Four-Layer Model for Security of Digital Rights Management. *Proceedings of the 8th ACM workshop on Digital rights management* (Alexandria, Virginia, USA, October 2008), 19-28.

[3] DVB 2002. ETSI TS 101 197 : DVB SimulCrypt; Head-end architecture and synchronization. ETSI.

[4] Koenen, R.H., Lacy, J., MacKay, M. and Mitchell, S. 2004. The Long March to Interoperable Digital Rights Management. *Proceedings of the IEEE*. 92, 6 (2004), 883-897.

[5] Safavi-Naini, R., Sheppard, N.P. and Uehara, T. 2004. Import/export in digital rights management. *Proceedings of the 4th ACM workshop on Digital rights management* (2004), 99-110.

[6] Smith, E. 2009. Disney Touts a Way to Ditch the DVD. *Wall Street Journal*.

[7] Welcome to Coral Consortium. *http://www.coral-interop.org/*. Accessed: 01-11-2008.