DRM Interoperability in Networked environments

David P. Maher & Anahita D. Poonegar
Intertrust Technologies Corporation

ABSTRACT

This paper explores technical and business solutions to the DRM interoperability problem. The lack of interoperability between devices and services using DRM technology is a complex problem that needs to be resolved in order to bring about widespread acceptance of legitimate electronic media distribution systems. In today's world, content, service and device providers usually adopt a single DRM technology that creates a closed system or "silo". While this is fine from a distribution standpoint, content distributed in one silo cannot cross over to a silo that uses a different technology. This is a real problem in a world accustomed to DVDs and CDs playing on all devices. This paper examines fundamental interoperability problems plaguing all participants in the electronic content distribution ecosystem – from consumer to content provider, device maker, service provider, aggregator, and technology vendor – and offers innovations in framing the problem and pragmatic suggestions to remove existing barriers that are restricting growth.

The Coral Consortium is a group focused on standardizing a DRM-agnostic interoperability framework. It is tasked with developing an architecture specification that accommodates current and future use cases for migrating content between devices that support different proprietary DRM platforms. Coral is preparing a set of specifications for "interfaces" that contain recipes for communicating between distinct DRM systems. In some cases, Coral may recommend interoperability based on bi-lateral agreements between ecosystem members. In cases where it is efficient to do so, Coral can recommend codec or format interoperability. This paper also examines the critical problem of "managing state" as rights are transferred between different DRM systems.

Intertrust has worked closely with the Coral Consortium from an early stage. It recently presented its NEMO (Networked Environment for Media Orchestration) reference technology to the Consortium. NEMO achieves interoperability via a service-oriented architecture across multiple network tiers (including WANs, LANS, PANs, and home networks).

1 INTRODUCTION

Digital Rights Management (DRM) technologies have come of age. This is substantiated by their inclusion in a growing number of devices and services for the CE, mobile, and enterprise markets. On the one hand, consumers have benefited greatly from the proliferation of DRM-enabled content, as it has made large catalogs of previously unavailable digital media accessible for legitimate distribution and use. On the other hand, because most DRM platforms and services developed are proprietary, in order to use their content with any degree of flexibility, consumers are often forced to choose a single, monolithic DRM hardware and/or software platform with its affiliated service providers. Furthermore, once they have made this decision, consumers are then burdened with the need to ensure that all their subsequent electronic media purchases are compatible with their system of choice. This lack of interoperability between the different technology and service provider environments is a step backward for consumers who have become accustomed to using content on physical media (i.e., CDs & DVDs) *anywhere, anytime,* simply by inserting a disc into a compliant disk drive.

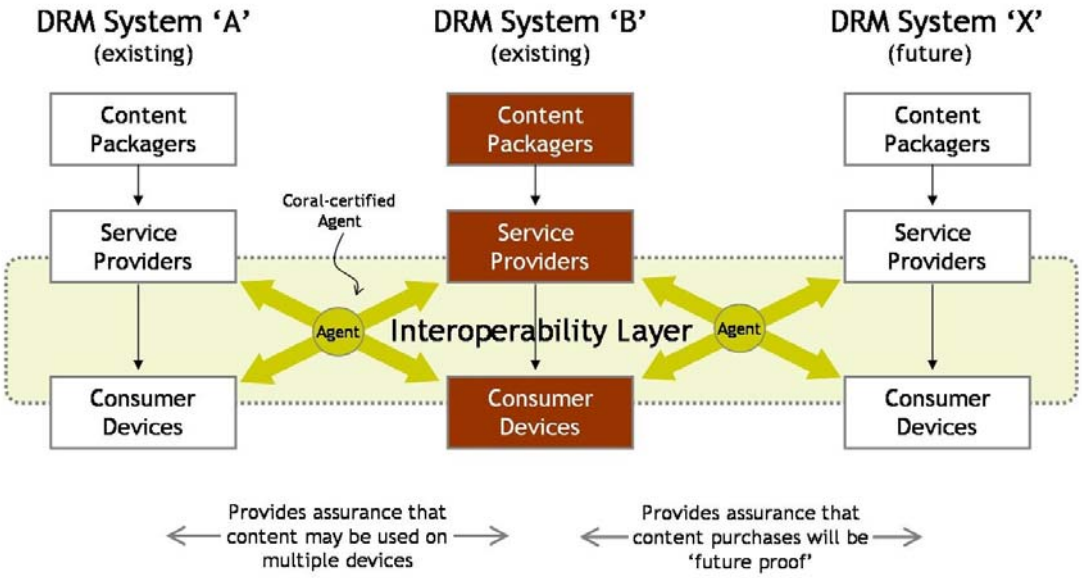
The convergence of IT, CE, and mobile technologies is causing consumers to seek greater content portability to play their catalog of licensed content on their home networks, car media system, and portable devices such as mobile phones, PDAs and media players. Unfortunately, unprotected content (perhaps acquired legally through shared P2P networks) provides this functionality without enforcing rights holder interests, whereas protected content (acquired through legitimate media distribution services), typically cannot provide such ubiquitous access. With the proliferation of broadband, network connected devices (i.e., Bluetooth and WiFi-enabled), and the growing popularity of hard-disk based media players, consumers are now beginning to embrace the notion of electronic media. However, until DRM-enabled media is made portable and consumer friendly, pirated media, especially from illegal P2P file sharing networks will continue to exceed the popularity of legitimately-sourced alternatives.

2 PROBLEM: INTEROPERABILITY BETWEEN DRM SYSTEMS

In a highly competitive environment, DRM and content protection technology providers submit to the conflicting needs of keeping margins low and usability high by retaining control of as many aspects of their product design as possible. This has resulted for the most part, in proprietary systems that are unable to communicate with other proprietary technology systems. The problem is further compounded when other interested value chain players have conflicting requirements of either controlling their technology environments (especially true among service providers such as cable companies, ISPs and portals), or of wanting a standardized format within which to publish all their content for different business models.

It would appear that the simplest workaround the problem of non-interoperability between proprietary DRM systems would be to create a universal, end-to-end DRM system that is appropriate for all aspects of the value chain. Unfortunately, this is infeasible for several reasons. One complicating factor is that different vertical markets (mobile, IT, etc.) and value chain participants (content, service, technology providers, and consumers) have distinct technology requirements, and therefore may need to optimize different aspects of a DRM system. Another complication arises from the sheer number of participants to be involved – encompassing a multitude of companies and interests. Although large open standardization efforts have been undertaken, standards in these areas are usually slow to mature. Finally, competitive differences between established proprietary technology providers may impede the adoption of a universal solution, should one be developed.

A more practical approach is to focus on standardizing interoperability - while allowing a common standard to evolve separately for the various DRM systems. To do this, an *Interoperability Layer* can be created where DRM components that have been developed for each specific platform can interact - regardless of whether these systems are open, closed, proprietary, etc. Accordingly, packaging components, service components, and end-user device components can all be optimized for their function and in keeping with their stakeholders' requirements.



Using the NEMO Interoperability Layer to Bridge DRM 'Silos'

In order to succeed, an interoperability layer needs to:
a) accommodate solutions that are in current deployment;
b) accommodate potential future technologies;

c) provide a bridge between deployed solutions that may not be ready today; and

d) provide a framework that tackles DRM interoperability at all layers of the DRM "stack" – from authentication and link-level protocols to intelligent service-to-device and device-to-device interfaces.

This approach bypasses the requirements dilemma cited above, and maximizes the likelihood of success, by allowing technology providers to control their implementations and by providing content and service providers with a common "dashboard" for content distribution. Meanwhile, consumers benefit from a uniform user experience that satisfies their need for flexible use of content among multiple devices.

3 SOLUTION: STANDARDIZING INTEROPERABILITY IN THE CORAL CONSORTIUM

The Coral Consortium is a cross-industry consortium that allows content owners, distributors, device makers, and software providers the opportunity to work together to ensure that existing and emerging DRM products can interoperate. It also evolved to address usability difficulties currently facing consumers of digital content by enabling interoperability between different content formats, devices, and content distribution services. Coral's primary objective is to forge agreements on the precise interface specifications, core services, and general interoperability scenarios that must be supported. Given the very different requirements of each of the value chain participants, this is not a small endeavor.

Based on a number of real-world DRM interoperability scenarios, and taking into account the different requirements of the value chain participants, Coral is developing a set of specifications that relies on devices leveraging *web-based* and *local services* to solve interoperability conflicts. These specifications focus on bridging gaps between disparate DRM systems and safeguarding against mismatches that are common when communicating between them. In building its solution, Coral is accepting submissions from companies participating in the consortium.

4 TRUSTED CORAL INTERFACES USING NEMO TECHNOLOGY

Intertrust's Networked Environment for Media Orchestration (NEMO) is a reference technology that the company has presented to Coral towards building a DRM interoperability platform. NEMO enables interoperability by creating service-oriented architectures (SOAs) to provide proprietary services with a means to communicate and request one another's operations, without needing to know anything about the proprietary workings of the services.

4.1 NEMO Descriptions for Services Architecture

NEMO provides specifications for implementing five key components of this infrastructure that are: *web standards-based service interface descriptions; service description advertisements; service and device discovery interfaces; trust management among NEMO nodes; and core services*.

4.1.1 Web standards-based service interface descriptions

NEMO services typically publish interfaces in the form of data and protocols, to let potential clients know what is required to make well-formed requests. The information on the interfaces can include security requirements (i.e., whether the requests should be encrypted and/or signed, and what algorithms and keys should be used); authorization requirements (i.e., policy on who is allowed access to the service and what credentials are required); supported data formats; and supported DRM technology.

In addition to describing web standards-based service interface descriptions, NEMO also describes capabilities, trust policies, and authorization policies. Entities that request a service's operations also describe their own capabilities in their requests (e.g., the requesting platform's capabilities with regard to DRM, format, memory, security protocol support, etc.). Requests may also include device credentials and certification information such as, "this requesting entity is a device that meets XYZ certification criteria as certified by ABC authority" (e.g., services may publish policies that require such certification credentials).

4.1.2 Service description advertisements

NEMO specifies guidelines for implementing advertisements of service description via registries or peer-to-peer (P2P) mechanisms.

4.1.3 Service and device discovery interfaces

NEMO specifies interfaces necessary for discovery of services and devices that can work in a heterogeneous environment. To be as efficient as possible, NEMO takes advantage of existing web-service and device standards that are associated with service publication (e.g., UDDI, UPnP), service description (WSDL), secure conversation and security policy, credential certificates, and others.

NEMO provides a layer that entities can use to become what is known as NEMO peers. These entities may actually be disparate types of devices, services, applications, etc, but in the NEMO framework, they all may become NEMO peers that can use SOA concepts to communicate in a standard manner.

NEMO promotes the use of peer services to manage format, DRM, and other types of incompatibilities. NEMO also includes certain core or framework maintenance services required for managing NEMO peer personalization, credential management, or key management. Furthermore, NEMO encourages the creation of new types of services that are made possible simply because of the NEMO peer communication interfaces -

services such as content rights locker services, proxy services for non-NEMO devices, gateway services between home and wide area networks, etc. In general, services that make up the NEMO framework can range from large web-services to mid-size gateway services, to small services that exist within portable devices. Any NEMO peer can be both a service and a client. This is completely consistent with the DLNA (Digital Living Network Alliance) vision of nodes or devices being both content sources and sinks.

After NEMO interfaces are well-formed and the core services are in place, we are in a position to tackle the DRM and format interoperability problem created by disparate content distribution services, supported formats, and DRM technologies. Common or standard NEMO interfaces are used to hide service incompatibilities. NEMO services are put into place to aid in service discovery, format or DRM exchange, etc.

4.1.4 Trust management among NEMO nodes

The NEMO framework is built on the notion of NEMO "nodes" that interact via specific request/response protocols. These protocols are used for the exchange and verification of credentials, and any other information required for nodes to establish mutual trust. Such trust is always established in the context of what the nodes are trying to accomplish. For example: node A may trust node B to render low resolution video, but not to render HD content. A node is a software agent that may both use and provide services: it can publish its capabilities for other nodes to use, and it can also request other nodes to do something it cannot do by itself (e.g., finding content, finding a license service).

Any type of device or service may form such a node; examples of nodes include consumer electronics equipment, networked services, and software clients.
These nodes can use service description advertisement and discovery. This enables them to pose requests for specific functionality and to discover services that support the requested functionality in a way consistent with the requesting node's capabilities. NEMO-enabled services and clients publish their capabilities, interfaces, policies, and platform specifics via standard publication methods, including for example, UDDI. Services that support one DRM system will use NEMO interfaces to communicate interoperation requirements – such as specific types of credentials and policy – to another service or application that supports a different DRM system.

4.1.5 Core services: core services required to support the framework, such as membership, personalization of NEMO nodes, provisioning of licenses.

This simple set of features lays the groundwork for interoperable content transfer and rights acquisition.

4.2 Examples of NEMO services

Some examples of NEMO services for interoperability in consumer media are:

- Content discovery services – these help finding services that deliver content in desired formats
- License interoperability services – these receive a trusted proof of possession of one DRM license as input, and provide a new license in another, different DRM format.
- Content interoperability services – these deliver content in formats that a content provider trusts.
- Content management and locker services – these services may reside on the Web or within a user's home network. When a user acquires a new device, this service will seek to update the user's content library by acquiring new content licenses and copies of content in the form required by the new device - automatically or on demand.
- Device gateways – these services act as NEMO proxies for devices that are not NEMO-enabled and may reside in the Internet or on a local home network.

In short, content distribution within a NEMO framework occurs via a rich, interconnected set of services into which any content provider may publish its content. The framework supports a heterogeneous world of client platforms and devices. From the consumer point of view, NEMO can facilitate format and DRM transparency to the extent desired by value chain participants.

4.3 How NEMO request-response works

High-level overview of a typical request-response scenario:

1. *A node poses a service discovery request. The request may include information about the capabilities of the requestor's platform and/or environment, including credentials used for managing trust relationships;*
2. *NEMO Service discovery finds a published NEMO service (or an orchestration of services) that meets the requested service description and is consistent with the requestor's environment. Note that this could be a local service or a remote one;*
3. *A NEMO service description is returned to the requestor that indicates the NEMO interfaces, capabilities, and trust/authorization policies of the candidate service;*
4. *The requestor poses a specific request to this service based on these interfaces and policies. Requests will be signed and/or encrypted and will include requestor credentials necessary for compliance with service trust and authorization policies*
5. *The service checks that the request is consistent with its interfaces and policies, acts upon the request, and returns a NEMO response message.*

5 CONCLUSION

DRM interoperability is a very real problem for consumers as well as other members of the content distribution value chain. This problem is now reaching a critical stage as broadband access has become increasingly ubiquitous, and consumers acquire multiple devices capable of viewing digital media. Historically, consumers have grown to expect that their purchased media should be available on any device, anytime, and anywhere. If legitimate, rights-managed content services cannot provide the flexibility to transfer content seamlessly and transparently between all devices, consumers will begin to turn away from these services. In a worst-case scenario, the growing acceptance of licensed content will be at risk, and consumers will return - perhaps irreversibly - to unlicensed, illegal file sharing networks.

The Coral Consortium is working towards an interoperability solution that leverages web-based and local services to solve interoperability conflicts. With NEMO-based services, consumers will be able to seamlessly and transparently transfer content among devices - regardless of which DRM systems are involved. By introducing a standard DRM interoperability layer, NEMO is uniquely suited as a solution to the interoperability problem. This provides an architecture that is easy to implement, allows technology providers to retain control over their existing systems, and only requires minimal modifications from existing service providers.