Project DReaM

An Architectural Overview

White Paper

Authors: Gerard Fernando, Tom Jacobs, and Vishy Swaminathan

September 2005

Table of Contents

1. Introduction

DReaM is a Sun Labs initiative to develop a Digital Rights Management (DRM) solution focusing on open-standards-based-solutions. Where the market requirement is for proprietary solutions, DReaM integrates with these solutions thereby providing openness and interoperability that meets customer requirements.

There is no question that the market for Digital Rights Management (DRM) software is booming. According to market research company Jupiter Research, the DRM market will grow to $274 million by 2008 from just $36 million in 2003. Researchers at Sun Labs are convinced that today's DRM applications only scratch the surface of the possibilities, and that the market for DRM technology is heavily constrained by the lack of an open, scalable and dynamically adaptable solution.

There is a widely held false perception that DRM technology focuses solely on preventing the unprincipled from getting something for nothing—a way to keep people from swapping music files and copying DVDs illegally. What's lost in this view is that DRM technology also provides the means to introduce services—not just for Hollywood but also for businesses and even for individuals. DRM provides improved levels of content protection that directly protects the content during its entire lifetime rather than simply managing file level access (such as portals).

Sun is determined to unlock the full potential of the DRM market. DReaM is an initiative to leverage the methodology of Service Oriented Architectures (SOA) and introduce rights management services that leverage open standards and support cross-service capabilities. The majority of the DRM market today is for the protection of music files and film clips. In addition to supporting these applications, DReaM goes far beyond by addressing content protection needs of other market categories, including Business and Life.

1.1 Vision and Goals

Sun Labs researchers have introduced a structured approach to analyzing DRM market opportunities based on three critical variables:

- **Number of content producers**: Traditional DRM applications such as protection of music and film have relatively few content providers. The potential applications in the *business* and *life* categories will involve far broader sources of content. The belief is that eventually everyone will become a producer in addition to being a consumer.
- **Binding of licenses**: DRM - and conditional access system (CAS) - solutions today only permit licenses to be bound to devices. As *business* and *life* applications evolve, it will be essential to provide more flexible models where licenses can be assigned to individuals, based on their identity or their role in an organization or family. An example of such negotiability might be a government agency's ability to revoke document access/viewing privileges for terminated contractors who might have had documents stored on their computers/laptops.
- **Dynamicity of licenses**: Today's DRM and CAS solutions only enable licenses to be assigned in a mostly static mode. For example, cable subscribers are issued a key that enables them to receive cable

broadcasts. To enable new *business* and *life* applications, the assignment will have to become more dynamic, so that new services or even components of services can be authorized and changed in real time. An example of such dynamicity would be the case where a business might grant a consultant rights to view and modify certain confidential documents only to decide later to terminate the consultant and revoke the previously granted rights and thereby render the confidential documents unusable.

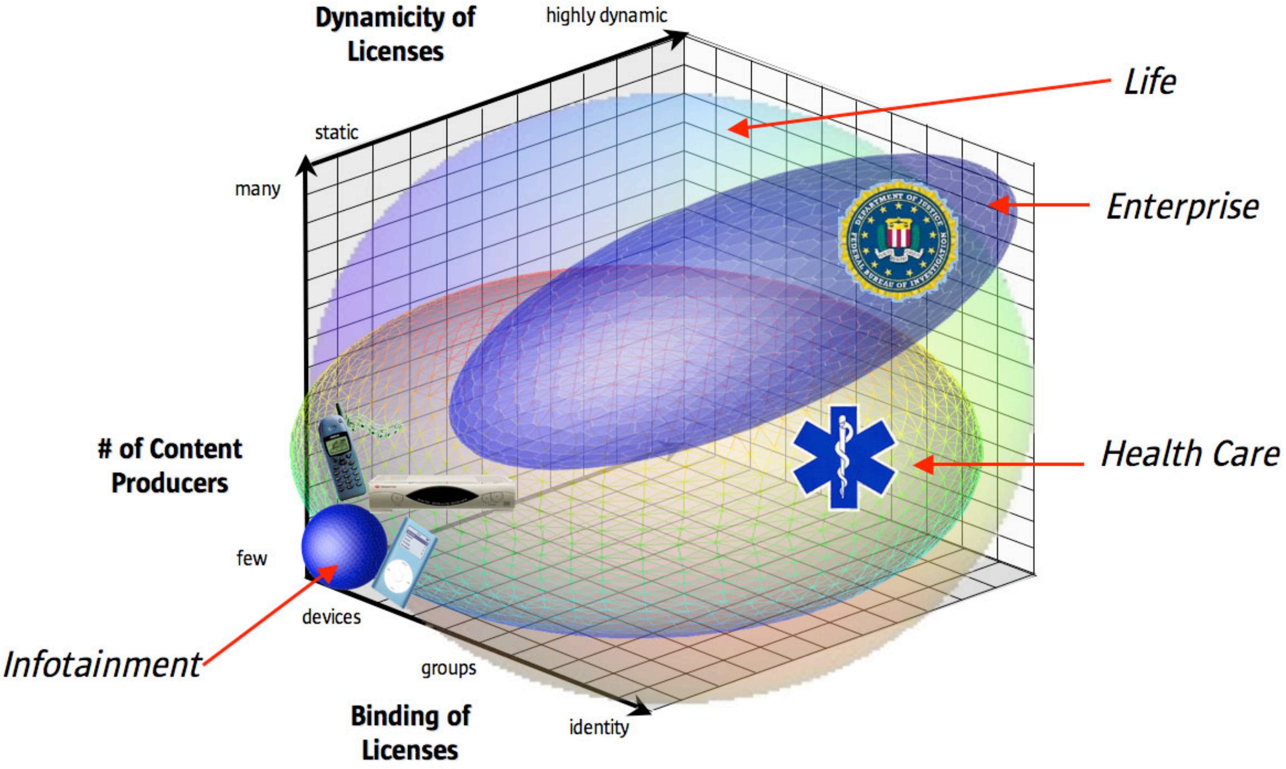

Figure 1 Cartesian Graph of DRM Usage Models

1.2 Expanding the Scope of DRM: Business, Life and Content

The need for DRM and content protection systems is somewhat well appreciated in the case of protecting revenue generating music and movies covered by copyright. Beyond that domain, we see important and even more promising markets for DRM systems in the categories of “business” and “life”. All of these industries are important with marketplace needs that will mature at different rates.

- In the “**business**” category, DRM can be used to control access to sensitive documents or to introduce new revenue generating services to customers such as training-on-demand. Business applications include corporate/enterprise, health-care, medical, and financial services as well as government and military models. In the health care field, DRM could be used to manage access to patient medical records. Unauthorized individuals would not be allowed access while privileged primary caregivers could easily make records accessible to those who need access. Employing a role-based model, emergency care providers could easily gain access if they possessed proper credentials.

- In the **"life"** category, DRM can be used to monetize or simply to control access to content, or even to control the behavior of objects. For example, a photography hobbyist could use DRM to sell the rights to individual photos on a per-use basis or to share pictures of their child's birthday party among family and friends while protecting privacy. Another example might be a home owner who might wish to share access to their home surveillance cameras with law enforcement officials on a restricted basis.
- The **"content/infotainment**" category refers to content generated by Hollywood and other similar entities that provide an asymmetric model of work flow. Content is generated, authored, protected and packaged at a few locations. The content is then distributed for subsequent consumption to a large number of consumers. Today there are significant deployments of conditional access systems (CAS) that are designed to handle limited content access scenarios where the consumption is immediate (like broadcast TV). It is possible to consider CAS as providing a subset of the functionality of DRM systems.

1.3 How DReaM Disintermediates Rights Management Solutions

The DReaM architecture supports the separation of rights management system components, which is the systematic decoupling of authentication, licensing, rights management and protection technologies. This disintermediation enables the choice and selection of these technologies independent of each other without compromising the integrity of the solution. Key elements of disintermediation in the DReaM architecture include:

- Separation of rights management from the content protection systems. Usage rights are defined in a separate license management system that would be facilitated by DReaM. This allows for the unmodified use of players and DRM clients already installed on devices without inheriting their limitations and shortcomings. As a result, a wide variety of usage models that are not supported by today's system suppliers can be supported in a DReaM disintermediated solution.
- Separation of identity and authentication services from individual hardware devices. Instead of merely authenticating the device on which content can be viewed, identity can be bound to a smart card (e.g., Java Card^{tm}) for personalization in DRM systems. This allows us to bind content rights to individuals (or roles) instead of devices.

1.4 An Inter-operable Framework for Content Protection Services

The DReaM architecture is an open framework for rights management in which individual component services can be mixed and matched. The fundamental concept is that DRM/CAS systems need not be monolithic end-to-end systems that can only be delivered by a single supplier employing only a limited set of pre-defined components. DReaM-based systems can be optimized as end-to-end solutions or hybrid systems with components sourced from multiple suppliers (partners and competitors).

1.5 The Importance of Being Open

Central to the DReaM solution is the concept that open standards will be critical to the success of any DRM architecture deployed, irrespective of whether it is deployed in “content,” “business,” or “life” applications. The proprietary end-to-end model typically works with the formats, codecs, and devices chosen by a single technology supplier. In the case of CAS, systems fall into a range from being partially open to totally proprietary. CAS systems that are based on the DVB (Digital Video Broadcast) Simulcrypt specification are partially open, though even these solutions rely upon totally proprietary components which effectively lock-in the CAS supplier. The DReaM solution will be able to interoperate with such CAS systems. Proprietary technology limits options by locking customers into specific formats and suppliers and thereby reduces the ability of service providers and content owners to take advantage of new and emerging technologies.

The open alternative increases flexibility by basing products on industry standards that are publicly available. By leveraging open standards, companies can deliver solutions that provide content and format neutrality and increase flexibility for service providers and content owners. The goal of the DReaM solution is to:

- Work with virtually any type of content needed, including text, audio, and video
- Span a wide range of device types and operating systems
- Work with multiple file formats and codecs
- Control access to content independent of the delivery medium, whether it is a physical or a digital connection, the Internet, CD-ROM, TV broadcast, DVD, Flash memory, etc.
- Support a range of business models, including subscription-based or fee-based service models, to provide flexibility for service providers

1.6 Open Source Versus Royalty Free

The term "open source" simply means that source code is made available to others in the community under specific use and license terms. Open source does not by default mean "free" unless explicitly stated, since the technology that the source code implements may infringe patents. Even when source code itself is declared "free," there may be technology patents that levy use or royalty fees.

For example, in the case of MPEG-21/REL, this Rights Expression Language (REL) specification was developed in an open standards body (ISO); however, it is widely presumed to be heavily encumbered technology that has been offered for commercial use with onerous licensing terms.

1.7 DRM Versus CAS

The electronic distribution of content offers new types of services for customers and provides new business opportunities for content providers. The acceptance of these new distribution models may depend on robust mechanisms to protect the interests of the various stakeholders in the value chain. Additionally, there are multiple models which are relative to how the digital service is being delivered (e.g., broadcast, download, or on-demand). CAS is intended to handle limited content access scenarios where the consumption is immediate. By contrast, DRM protects the content during its entire lifetime. In many ways, CAS is a degenerate form of DRM. Occasionally, people refer to Rights Management Systems (RMS) as something separate from DRM or CAS. RMS has been associated with the protection and management of other content types such as documents and data files aside from media data types. RMS may be as simple as CAS in as far as allowing viewing or not, or as complex as DRM where you can enforce more complicated rights such as restricted access to certain parts of the document/data, disallow modification, printing, or copying of data out of the files.

1.8 “Security Through Obscurity”

Historically, proprietary end-to-end architectures have relied upon obscurity to avoid being cracked. Such systems are based upon a false foundation of security promises. Such systems have been cracked and will continue to be breached. Additionally, the opaque nature of these systems has led to monolithic system architectures (by nature) that presume delivery by a single vendor, which inherently increases costs through the lack of interoperability and adds difficulty when attempting to substitute one supplier for another.

DReaM promotes the view that open system architectures will present greater opportunities for review and discussion of technology choices so that shortcomings can be better evaluated and corrected (“review & repair” versus “hope & pray”) to provide the greatest protection possible.

2 Background: Basic Rights Management Components

A discussion of DRM involves many specialized concepts that are beyond the scope of this paper. We recognize that the needs for DRM services in different industries are not all alike. For the sake of this section of the paper, we will focus on the common view of DRM for Digital Asset Management.

2.1 Digital Asset Work Flow

Traditionally, digital content follows a well-defined logical work flow from creation through consumption, managed by using some form of Digital Asset Management (DAM) system. In the simplest case, newly acquired content (video, music, documents, data) is ingested into the DAM in original formats. The content might then be converted into other formats that might be used within the DAM (thumbnails, alternate archive) or the distribution service (compressed distribution formats). Data about the ingested content (metadata) is then generated (rights offer terms, content description, etc.) and stored for later search and retrieval. The ingested content might then be protected (encrypted) and usage offers prepared in anticipation of requests for consumption. The Asset Management System (AMS) coordinates all of the ingoing and outgoing data requests and interfaces with the Business Support System (BSS) that handles commerce and billing activity. The distribution formats of the content are then provisioned into the distribution infrastructure (video-on-demand, download, navigation and application servers) that service client requests to receive content along with consumption rights.

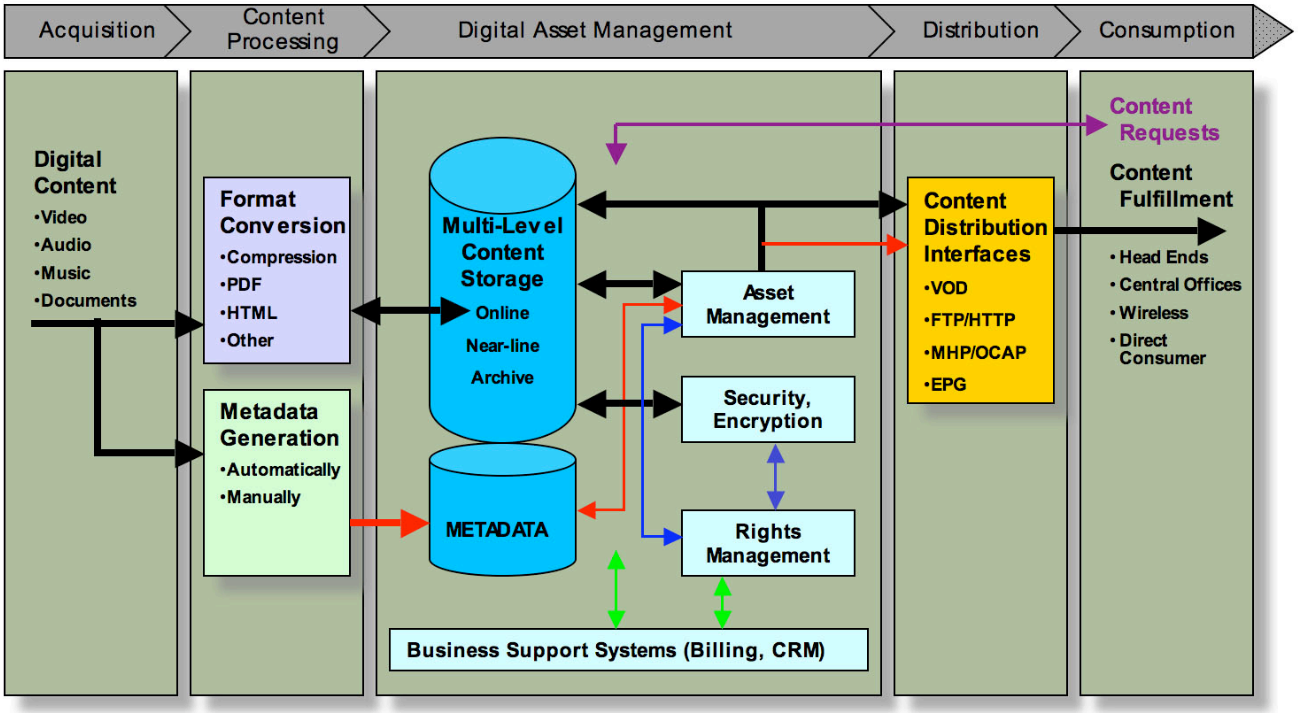

Figure 2 Digital Asset Work Flow

2.2 Business Rules Definition

Business rules are defined to be the terms and conditions under which content can be sold, rented, copied, printed or stored by a user. These terms may be presented to users in many different ways including as a license expressed in a machine-readable XML-based rights expression language. The key issue is that the business rules originate as legal or business terms which then must be translated into functional rules, which would be interpreted or enforced by a DRM system. One set of input business rules could be translated/interpreted into multiple different DRM specific functional rule sets that would be essentially equivalent from a legal or business point of view.

2.3 Protection Mechanisms

Among the many different technical protection measures, encryption is the critical process by which content is made unreadable (scrambled) without the proper decryption key(s). With the use of suitably strong encryption algorithms and appropriate protocols, protected content can be made safe from “brute force” hacking for many years or decades into the future. Encryption schemes typically have multiple levels of protection where the bulk of the content would be protected with one set of keys and those keys would themselves be protected with yet another cipher. The number of ciphers and how often keys change (per-minute, per-megabyte, per-page) is up to the content owner to determine based upon their risk assessment and willingness to pay for additional protection.

Other technical protection measures include the use of watermarking, finger printing and hashing technologies. These are used for embedding information in content to facilitate tracking or to verify the integrity of the content itself.

2.4 Packaging

The packaging process involves combining content data/files with associated metadata and creating logical packages that include the defined business rules. DRM packaging applications may have user interfaces for the human processing of content or the rights may be machine processed from business rules that are made available at the time of content ingestion. These business rules may be stored in a content management system (CMS), and the DRM packager would then read them through database queries.

2.5 License Generation

The process of license generation involves combining the business rules associated with a content title with usage rights associated with a given user and generating a license (which typically includes keys). This license specifies the conditions under which the content title may be used by the user. The usage terms may be explicitly expressed in the license in a machine-readable language such as XML, or a variant of it that would be delivered to the client. A usage license may also be acquired by a client as part of a dynamic negotiation with licensing authority. The given content license would only be usable if the conditions of utilization were satisfied.

2.6 Distribution

Protected content and the associated keys/licenses must be distributed to clients. This process requires the DAM to provision content into the distribution service environment, along with the associated keys into a licensing service. This distribution process can be carried out in either an open, well specified or a closed, proprietary environment.

Distribution may be carried out using various different processes including broadcast (one-to-many) or unicast (one-to-one), and real-time/streaming or download (non-real-time) and physical media delivery (DVD). The licenses may be delivered with the content (in-band) or separately (out-of-band) depending upon the method of delivery. This may require specific technologies to be incorporated into the distribution server. This would be particularly true for real-time content delivery (i.e., streaming).

2.7 Consumption

The DRM player will consume the content based on the conditions specified by the license. The DRM player must be secure such that unauthorized use of content is prevented. Typically, the player environment will have secure storage and execution environments, where keys and decrypted content cannot be accessed by unauthorized clients.

3 Sun’s DReaM Architecture

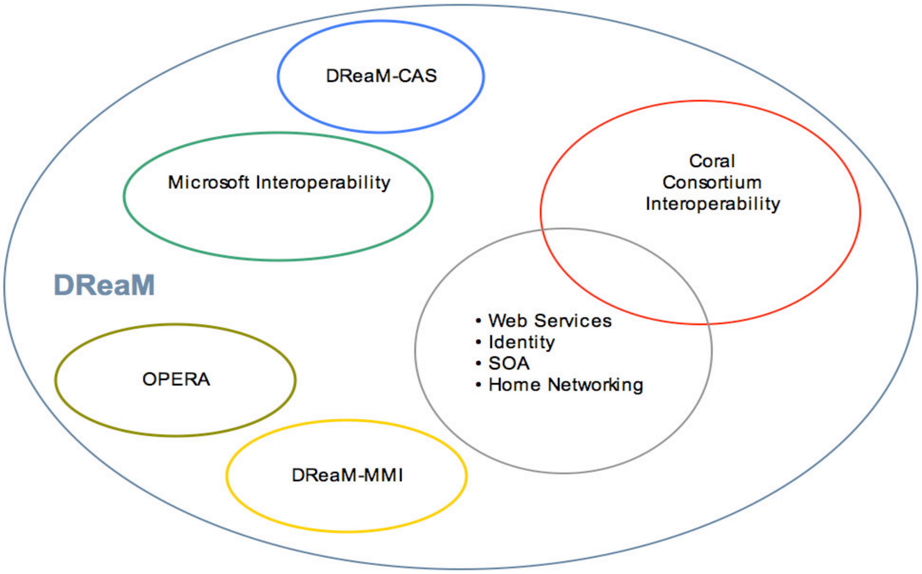

Figure 3 Sun's DReaM Architecture Diagram

DReaM is a comprehensive, horizontal solution envisioned to support multiple usage models (business, content and life vertical markets). DReaM supports open standards-based solutions for DRM and has the flexibility to deliver a mix of Sun-sourced technology interoperable with products from other vendors. DReaM is based upon a Service Oriented Architecture system design that leverages open standards. It leverages identity work pioneered in Project Liberty by promoting identity and role-based licensing models. DReaM is capable of inter-operating directly with other content protection technologies. DReaM supports services that enable both Conditional Access System (CAS) and Digital Rights Management (DRM) models.

3.1 Disintermediation

One of the key features of the DReaM architecture is the ability to accommodate the inclusion of some DRM/CAS components from other suppliers while avoiding the need to incorporate all their back-end components.

The disintermediation system enables multiple instances of these components to exist in a DRM/CAS system.

- The content protection specific components of DReaM include: player, licensor and packager.
- Components that are not content protection specific include: a disintermediating agent, conductor, catcher, licensing conductor, contracts manager, authentication service, shop and transaction system, and content delivery service.[1]

[1] In some cases of proprietary delivery services, there may be a dependency on the content protection specific components.

The process of disintermediation happens as follows:

1) Client requests a license
2) Front-end service redirects client to a client disintermediation agent
3) Disintermediating agent contacts Conductor (back-end service)
4) Conductor contacts back-end services for authentication and rights verification
5) Conductor signals front-end service with instructions to deliver license to client
6) Front-end service delivers license

The DReaM component diagram is graphically illustrated in Figure 4.

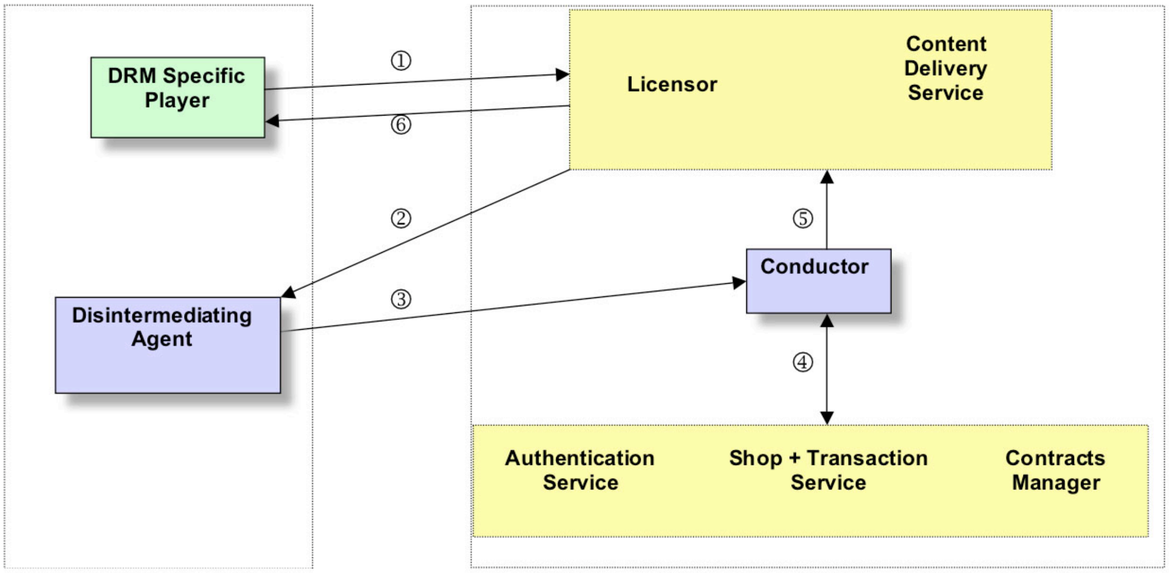

Figure 4 DReaM Component Diagram

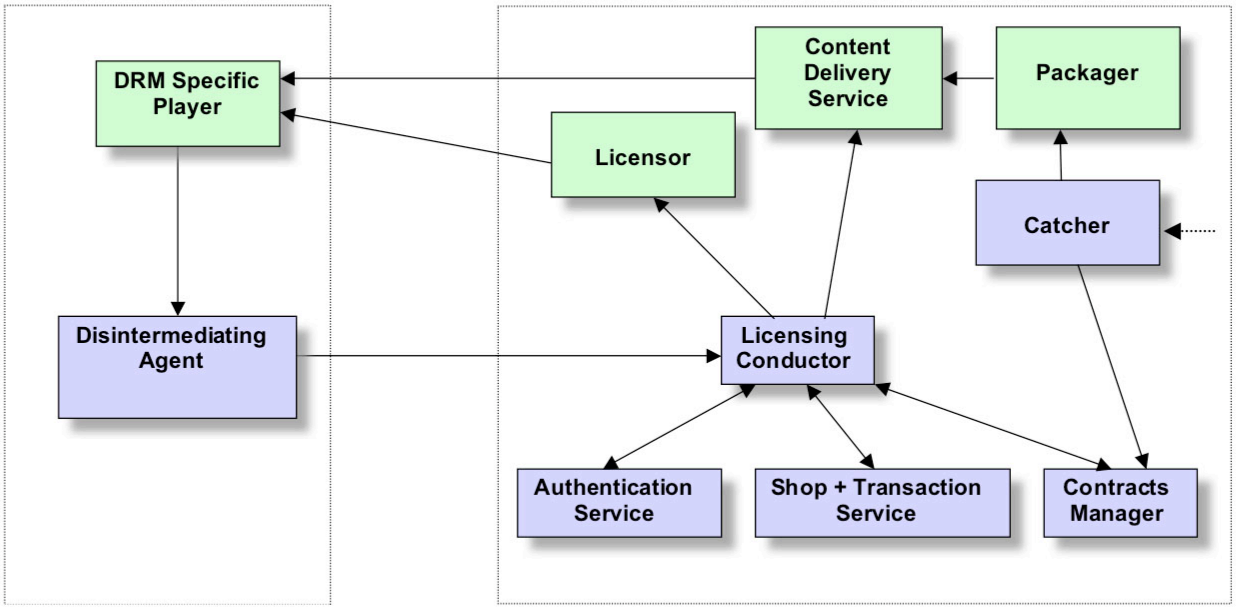

Figure 5 DReaM as a Disintermediation System

3.1.1 Client - DRM Specific Player

The DRM Specific player is a client-side player application that has DRM specific support for handling protected content and licenses.

3.1.2 Client - Disintermediating Agent

A common disintermediating agent needs to be present in the client for the disintermediation process to function. This is a Java application that would perform the re-direction required for disintermediation.

3.1.3 Licensor

The licensor is tightly bound to the DRM specific content protection technology.

3.1.4 Licensing Conductor

The Licensing Conductor plays the role of managing the licensing processes involved in the DReaM solution. It has interfaces to the DReaM Client, Shopping and Transaction Service, Authentication Service, Contracts Manager and the Licensor. It performs the necessary e-commerce transactions and authentication of the user. It instructs the Licensor to generate the license for a given user for specific content.

3.1.5 Contracts Manager

The Contracts Manager stores business rules associated with content, as well as user rights. This component has interfaces to the Licensing Conductor and the Licensor. The Licensor will generate a license for a given piece of content based on the business rules and user rights that are available in the Contracts Manager.

3.1.6 Authentication Service

The authentication service is where subscribers, users and devices are cleared for access to services and content. The methods of authentication vary from weak methods such as username + password challenge to stronger authentications such as smart cards or biometrics.

3.1.7 Shop and Transaction Service (Business Support Services)

The work flow functions of shopping and transacting purchases includes everything from collecting payments from buyers to paying sellers and making sure that everyone is appropriately compensated in a secure manner.

3.1.8 Content Delivery Server

The content distribution server will receive protected content from the packager. Stream keys used for content protection in the packager may be optionally stored with the content in the content delivery server. More details are provided in section 2.6

3.1.9 Packager

The packager performs the functions as described earlier in section 2.4.

3.1.10 Catcher

The Catcher performs content ingestion. It receives content and associated business rules from the content supplier. The content, which is unprotected at this stage, is passed to the Packager. The business rules associated with the content are passed to the Contracts Manager. Additional information about business rules are described in section 2.2.

3.2 Standards-Based Interoperability

The DReaM solutions will focus on open standards-based solutions where the market demands such open standards solutions. The DReaM Conditional Access System (DReaM-CAS) and DReaM Mother May I system (DReaM-MMI) being developed by Sun are totally open solutions, where content formats, key management and delivery will be fully specified. Third party companies and media organizations are expected to support and implement to the DReaM-CAS specification.

The DRM standards from the Open Mobility Alliance (OMA) and Internet Streaming Media Alliance (ISMA) can be supported by the DReaM solution. The OMA 1.0 DRM and 2.0 DRM standards are finding support by wireless carriers. Where the market requirement is for proprietary solutions then the DReaM solution interoperates with these solutions, thereby providing a level of "openness" and interoperability that is demanded by customers. The Microsoft Windows Media DRM and Rights Management solutions are examples of such proprietary solutions for which the DReaM solution will provide interoperability.

3.2.1 Coral Consortium

In figure 3 (above), we show that DReaM encompasses multiple simultaneous services (CAS, DRM, multi-vendor interoperability). The Coral Consortium is a new organization in which Sun is an active member. Coral aims to define and promote a web services approach to DRM interoperability by creating specifications, defining/testing conformance and promoting the adoption and usage of the specifications. Service operators are the target end-users who will benefit from the interoperability that open standards yield. Service operators will need to specify architecture and technology requirements for their vendors to provide compliant solutions so that service operators will be able to maintain full control of their business and network architectures while fully benefiting from the opportunities that open systems enable.

The Coral Consortium aims to create a common technology framework for content, device, and service providers, regardless of the DRM technologies they use. The Coral specification only requires minimal adaptation of a DRM delivery chain in order to operate in a compliant manner. It allows different interoperable ecosystems to be built on top of it, where an ecosystem is defined as a set of DRM systems that are mutually trusting, and between which content can be exchanged using interfaces defined in the Coral Consortium specifications.

The Coral architecture relies on Web Services specifications to facilitate interoperability. Discovery and orchestration of DRM component services are facilitated through Web Services. There is no need for content interoperability, device interoperability, or interoperability of key management. Instead, Coral makes it possible for independent content protection systems to coexist in parallel while sharing some back-end services.

3.2.2 DVB's Simulcrypt

Simulcrypt was specified by the Digital Video Broadcasting (DVB) project (http://www.dvb.org) in order to allow a single common transport stream (DVB/MPEG-2 TS) to be used to deliver content protected by several different conditional access systems. Proprietary cryptographic technologies and key distribution systems are supported. This ensures that the same multiplex (satellite, cable, terrestrial) may be used for different “bouquets” of programs delivered by different service providers. CAS vendors have the opportunity of providing unique (i.e., proprietary) value. However, this is at the expense of a totally open specification and having any common CAS components.

3.2.3 ISMA’s ISMAcryp

The Internet Streaming Media Alliance (http://www.isma.tv) has developed the ISMACryp specification. This specification ensures that interoperability of protected ISMA content is supported. Default algorithms for encryption, authentication and integrity are specified in the ISMACryp specification. However, a framework is provided for these to be replaced in the event that these algorithms are compromised or superior algorithms become available.

4 Content Protection Technologies

The specific technical measures for content protection forms the core of securing and safeguarding content in any DRM solution. While DReaM disintermediates monolithic content protection solutions, it also allows for the use of its own secure technical protection measures.

4.1 Sun’s Content Protection Technologies

Sun is developing its own technical protection measures to support both conditional access and rights management needs. Sun’s specific content protection technologies are described below.

4.1.1 DReaM-MMI – An Alternate Method of Expressing and Controlling Rights for Content

Sun is developing a novel mechanism for DRM that is termed DReaM-MMI (*Mother-May-I)*. The objective of DReaM-MMI is to provide a different approach to managing rights for a variety of client types that are directly or indirectly connected to content networks. The design philosophy underlying DReaM-MMI is that clients should be able to negotiate for rights through standardized protocols rather than downloading a license with an embedded expression of rights.

The process for licensing rights for content using DReaM-MMI employs the same key components as described in Section 3. Content that has been previously protected is stored in the content delivery server. Content keys are stored in a key and license server (DReaM Licensor). The rights associated with the protected content are stored in a rights repository (DReaM Contracts Manager). A DReaM-MMI compliant client will request the use of given protected content under a specific set of usage terms. For example, those terms can be a specific time window, a set of different device types, number of viewings, etc. The DReaM-Licensor responds to the client's DReaM-MMI request after communicating with the DReaM Contracts Manager to determine whether the client should be allowed access to the content on those DReaM-MMI expressed terms. If the Licensor response is positive, the content keys are delivered to the client where it will be consumed according to the terms expressed in the DReaM-MMI request. The DReaM-MMI compliant client has the responsibility for enforcing that the content is only used under those specified terms.

Presently, when content is delivered to a client, rights are also provided, using a rights expression language (REL). The client receives this REL and determines whether such use is permitted at each time the content is accessed. If such use is permitted, the usage is authorized. If the usage is not permitted, access to the content is denied. With the DReaM-MMI method described above, access is requested under certain conditions, and the client software manages the use, according to the guidelines under which the content is requested. If a client wishes to access content under different usage terms, the client could renegotiate with the DReaM-Licensor. No more access is allowed than the specific rights the client had requested. In the case of DReaM-MMI, no REL is delivered to the client.

Components required for DReaM-MMI based solution:

- The DReaM Licensor must be able to support the DReaM-MMI protocols and interfaces. These DReaM-MMI requests may be based on Web Services requests.
- The DReaM-MMI client will support the DReaM-MMI protocols and interfaces in the interaction with the DReaM Licensor.

4.1.2 DReaM-CAS – A Complete Specification of an OPEN CAS Solution

Sun Labs is developing the specification and the associated implementation of a complete open CAS solution. By utilizing open standard technologies for security (PKI, SSL, TLS, etc.), we anticipate that DReaM-CAS solutions will be royalty-free. Additionally, the DReaM-CAS solution will be fully and openly defined. This is a departure from the current state where various proprietary vendors utilize the standardized MPEG Transport without specifying all the necessary CAS components such as the Entitlement Control Messages (ECM) and Entitlement Management Messages (EMM). By under-specifying in this way they ensure that proprietary control of the CAS solution is maintained.

The DReaM-CAS specification will utilize existing content protection technologies (AES, 3DES). Key protection and management will also be fully defined. The ECM in MPEG-2 TS will be fully specified to carry protected content keys. Asymmetric key technology (public key/private key) will be used to deliver individually protected keys to unlock the content keys. The EMM format from MPEG-2 TS will be optionally used to deliver these individually protected keys.

Key components required for a DReaM-CAS solution:

- The DReaM Licensor must be able to support the protocols and interfaces of the DReaM-CAS specification including key management.
- The DReaM-CAS Client will support the protocols and interfaces defined by the DReaM-CAS specification.

5 Usage and Application Models

5.1 CAS Model

All pay-media operators require a means for ensuring that payment is received in return for the program content they provide. The technical system that achieves this objective is called a conditional-access (CA) system.

Two key functions of CA systems are to exercise control over the access to a service that is transmitted electronically, and to control the conditions under which access is granted. There are various reasons for implementing a CA system, such as the need to enforce payment by the subscriber for consumed services, to restrict access to programming in a particular geographical area because of program rights considerations or to facilitate parental control.

Typical applications of CAS are in immediate-use television broadcast, VOD and Pay-Per-View (PPV) where content is immediately accessed and not stored for future use.

5.2 DRM Model

DRM refers to the administration of rights in a digital environment. DRM solutions may use technologies to protect files from unauthorized use, as well as manage the financial transaction processing, while ensuring that rights holders have their rights respected and are possibly compensated for the use of their intellectual property.

5.2.1 Download Versus Packaged Media

Whether content is digitally retrieved over a network (Internet, Service Provider, Peer-to-Peer) or received on packaged media (DVD, CD-ROM, Memory Card, Floppy, Hard-disc), the content can be protected and managed using the same DRM mechanisms since keys/licenses are typically independent of the protected content itself.

5.2.2 Connected Versus Disconnected Usage Issues

The issue of “connectedness” is quite important even in this day and age of seemingly ubiquitous connectivity. There will still be times when you will be disconnected (airplanes, underground trains/tunnels, elevators, remote locations, etc) but would still like to consume content. In some cases, the rights and license can be cached for later use, though these rights would be limited and would likely need to be “refreshed” over time. Rights could also be transferred to disconnected devices that indirectly connect through proxies. In all of these cases, disconnected devices inherently represent weaker protection models than always connected devices; however, connectivity is but one of the checks and balances which should be employed to deter piracy and unauthorized consumption of protected content.

5.2.3 Licenses, Rights and Keys

5.2.3.1 DReaM-MMI Versus RELs

DReaM-MMI is a fundamentally new approach to managing rights and licensing by having DRM clients actively negotiate a license for protected content without employing RELs that are sent to clients to interpret and enforce. DReaM-MMI instead recommends that a secure, trusted client negotiate with the license service for terms of use and then translate that interpretation of a license into functional license service locally.

5.3 Content and Format Issues

The DReaM Architecture is independent of the content type, file and transport formats - whether the content is a time-based media (video, audio, music, games), or a document/data type. Some protection technologies (e.g., protection for conditional access) are dependent upon the transport format and sometimes on the specific content type. In those cases, there would be specific profiles defined for the content and transport dependent technologies that would be used with the DReaM architecture.

6 Conclusions

DReaM is an ambitious project that will likely attract critics and nay-sayers who either have interests to protect or insufficient perspective. Sun is confident that DReaM can realize its promise based on our view that DRM, like many other in-vogue technologies, is based upon the same technical foundations that have been tested and deployed for over 25 years.

Sun's vision behind DReaM has been shared by many, but thus-far that hope has been unrealized in the commercial industry in any substantial way. In order to help move the industry toward that goal, Sun launched the Open Media Commons (OMC – http://www.OpenMediaCommons.org). OMC will host a community forum where the technical, legal and source code issues related to DReaM will be discussed in an open manner. Sun has committed that DReaM (along with a number of other media related projects) will be open sourced without royalty. In the months ahead, Sun will be publishing more details (architectural, source code and legal opinions on royalty-free technology choices) about DReaM. Sun welcomes the participation of others in the Open Media Commons as a forum for achieving the vision of DReaM.

Sun Microsystems, Inc. Network Circle, Santa Clara, CA 95054 USA Phone 1-650-960-1300 or 1-800-555-9SUN Web sun.com