

Coral Consortium Whitepaper

February 2006



THIS DOCUMENT IS PROVIDED "AS IS". THE CORAL CONSORTIUM CORPORATION ON BEHALF OF ITSELF AND ITS MEMBERS MAKES NO REPRESENTATION OR WARRANTY, EXPRESS OR IMPLIED, INCLUDING ANY WARRANTY OF MERCHANTABILITY, NONINFRINGEMENT, FITNESS FOR ANY PARTICULAR PURPOSE, OR ANY OTHER WARRANTY CONCERNING THE COMPLETENESS, ACCURACY, OR APPLICABILITY OF ANY INFORMATION CONTAINED IN THIS DOCUMENT AND DISCLAIMS ALL LIABILITY OF ANY KIND WHATSOEVER, EXPRESS OR IMPLIED, ARISING OUT OF OR RESULTING FROM THE RELIANCE OR USE BY ANY PARTY OF THIS DOCUMENT OR ANY INFORMATION CONTAINED HEREIN.

THE CORAL CONSORTIUM CORPORATION ON BEHALF OF ITSELF AND ITS MEMBERS MAKES NO REPRESENTATION OR WARRANTY, EXPRESS OR IMPLIED, CONCERNING THE APPLICABILITY OF ANY PATENT, COPYRIGHT OR OTHER PROPRIETARY RIGHT OF ANY THIRD PARTY TO THIS DOCUMENT OR ITS USE, AND THE RECEIPT OR ANY USE OF THIS DOCUMENT OR ITS CONTENTS DOES NOT IN ANY WAY CREATE BY IMPLICATION, ESTOPPEL OR OTHERWISE, ANY LICENSE OR RIGHT TO OR UNDER ANY CORAL CONSORTIUM CORPORATION MEMBER COMPANY'S PATENT, COPYRIGHT, OR OTHER PROPRIETARY RIGHTS.

Copyright © 2005, 2006 Coral Consortium Corporation. All Rights Reserved.

Coral Consortium Corporation
39355 California Street, Suite 307
Fremont, CA 94538
USA

Website: <http://www.coral-interop.org>

Email: info@coral-interop.org

Table of Contents

Table of Contents	ii
Executive Summary.....	1
A Typical Scenario.....	3
A Coral-Enabled Scenario	3
Coral Objectives	4
The Interoperability Problem.....	5
The Coral Interoperability Framework Architecture	7
Deconstructing the Coral-Enabled Scenario.....	10
Summary	12

Executive Summary

Digital distribution of movies, music, and other content has enormous potential for growth. It is far more efficient for the content owner and distributor to send a digital copy of the content, than to ship, store, and retrieve the physical media containing the content. Digital distribution should also prove to be far more appealing to consumers, providing them with the experience of relatively instant gratification with respect to acquisition and use of content. To date, however, this potential has yet to be realized, primarily because digital content is highly susceptible to unauthorized content reproduction and distribution, imposing significant potential risk to content providers and other participants in the content distribution value chain. With digital content, such unauthorized copies may be virtually indistinguishable from the original.

Digital rights management (DRM) systems provide a means for content providers and distributors to address the unauthorized copying issue. These systems are used to express and enforce content distribution and usage models that are consistent with content provider and distributor requirements. Ideally these models should also be fully consistent with consumer expectations. While there is certainly room for improvement in the models themselves, there is one area associated with DRM systems that has recently gained more attention and that is in large part responsible for general consumer confusion and reluctance to acquire DRM-governed content.

Current DRM systems work only in closed, monolithic systems that are designed not to be interoperable. Consumers have a problem with this, as their purchased content that is protected using DRM A will play only on devices that support DRM A. The problem is compounded on portable devices, where size and cost constraints restrict the number of supported DRMs. As a result, consumers are forced to purchase different versions of the same content, formatted to play on their different devices. To some extent, consumers have accepted this model for video games and audio content. However, it is not a consumer friendly experience, and frustrations resulting from a lack of interoperability among DRM systems as well as confusing usage models encourage consumers to use illegitimate distribution systems.

Having multiple DRM technologies and content formats is healthy for the market from the standpoint of encouraging competition and innovation. However, consumer reluctance to adopt DRM technology because of confusion resulting from multiple DRMs and formats that do not interoperate is not good for the market. In order for legitimate digital content distribution systems to succeed, DRM approaches and related services and applications upon which they are based must exist in an environment that supports interoperability.

The Coral Consortium (hereafter called Coral) is a collection of content providers, service providers, consumer electronics manufacturers, and other technology companies that is defining a framework to address DRM and format interoperability issues. Coral's goal is to enable interoperability between disparate DRMs used in consumer media

applications, services, and devices. Coral is designing an interoperability framework to ensure that the consumer can conveniently access protected content from any source and play it on any device without having to be concerned with the DRM technology supported by the device.

The Coral framework solves the problem of mismatches that result from using multiple DRM systems that do not communicate with one another. Coral does this by taking advantage of concepts derived from service-oriented architecture. Within this framework, trustworthy services communicate with one another via trusted interfaces, exchanging whatever information is required to mitigate differences among different DRM systems. This approach is designed to provide transparency to end-users as well as additional functionality that does not exist in content distribution services today.

To achieve these goals, Coral is developing the Coral Interoperability Framework, a set of specifications for secure, trusted interfaces and core services or roles. These specifications promote secure and trusted interoperability among applications, services, and equipment that are compliant with those specifications. . To support the initial technical Coral Interoperability Framework architecture specifications, Coral will also create compliance and robustness criteria for the framework, a certification process and trust management infrastructure, and adopter agreements.

The Coral Framework will be used further as the foundation for ecosystems in which common usage paradigms, ecosystem-specific compliance and robustness criteria, and particular technologies will be specified. Coral will specify such an ecosystem as one of its earliest tasks.

A Typical Scenario

Bart regularly buys digital content from online content service providers. As a result, he has acquired a sizeable library of music tracks and videos that he stores on his PC. Bart realizes that not all the tracks and videos play in the same application. On the PC this is annoying but manageable. Bart then buys a portable player and is excited about moving copies from his content library onto the device. He finds that while some of his content plays fine on his new device, much of it does not. Bart tries hard to make it work but finally gives up in frustration. He later discovers the culprit. Different pieces of his content are protected by different competing technologies called digital rights management (DRM). The reason only some of his content plays on his new device is that the device only supports one particular type of this technology. Upon further investigation, Bart discovers that this device also plays content in an unprotected form and he remembers that there are places on the Internet where he can get bootlegged copies of the same content that is unprotected and free. Bart's temptation to abandon the legitimate services in favor of services of questionable legitimacy that serve free content that plays across all of his devices becomes very hard to resist.

A Coral-Enabled Scenario

Bart has accumulated a vast digital content library from multiple online stores, with audio and video supporting different formats and different DRM technologies. He buys a new portable device. When he plugs it in for the first time, it detects his local network; his PC is also part of his local network. When Bart adds the portable player to his local network, he finds his content library and is able to access all of it on his new device.

In a Coral-enabled world, content providers, content distribution services, devices, and applications may all be aware of DRM and content format differences. The presence of the Coral interoperability framework will mitigate these differences. As a result, consumers will see none of the differences and experience seamless access to content across their collections of devices. The rest of this paper provides more detail on how this is accomplished. At the end of the paper, we revisit this scenario with a look behind the scenes.

Coral Objectives

The Coral Consortium is defining a framework that enables interoperability between disparate DRM approaches in the context of consumer media applications, services, and devices.

Existing content distribution systems provide many choices to consumers, but unfortunately neglect interoperability. This consumer requirement is often neglected by technology and service providers seeking to differentiate their value proposition through proprietary systems. The lack of interoperability among DRM systems together with a preponderance of confusing business and content usage models conspire to encourage consumers to use illegitimate distribution systems.

If legitimate content distribution systems are to succeed, the DRM approaches and related services and applications upon which they are based must exist in an environment that supports interoperability. Such an environment must support the ability for consumers to discover and acquire any content they desire and that will play on their devices and in their applications, with a minimal understanding of DRM and content formats. The environment must also support the intuitive use of content for all consumers. Additionally, content providers and device manufacturers must be able to support content in the formats that are most practical in the context of their respective businesses.

To meet these objectives, Coral has created the Coral Interoperability Framework – hereafter known as the Framework. The Framework uses concepts from service-oriented architectures to bridge gaps and mismatches that naturally exist between different DRM systems. This approach supports secure, policy-managed communication among trusted peers, which can be both clients and services. Service providers and content owners can use these policy-managed interfaces to govern all access to and use of their content, and create policies to govern interoperability among various DRM systems and formats. In other words, only trusted DRM systems and related devices and applications may acquire content access rights.

In Coral, industry leaders and experts are working together to develop the Coral core interoperability conceptual model to create content distribution frameworks that support the interoperable coexistence of disparate DRM and distribution technologies. Coral has defined a set of desirable interoperability scenarios, and based on these scenarios Coral has developed the necessary interoperability specifications that meet the requirements of all value chain participants in the consumer media domain.

The Interoperability Problem

Most content distribution systems deployed today are composed of the following elements:

- A set of applications used to package content into a service-specific protected format
- A service used to distribute the protected content
- A retail service that manages service participants and content rights, and creates licenses for use by client applications. These licenses govern use of the protected content in the particular service-specific format
- A set of consumer devices and content rendering and management applications that understand the content format and the governance and protection schemes associated with it

These deployments are monolithic in the sense that their elements – services and content – typically support a single protected content format and system for expressing and enforcing content usage rules. Content providers publish their content into these monolithic content distribution systems and only client applications and devices that support the specific format may render that distributed content or process associated rights. A consumer who has just purchased a device that supports a different, second format will find that it is impossible to use content from services based on the first format. This is both confusing to the consumer as well as detrimental to the service provider and ultimately to the content provider and the future of legitimate content distribution itself. We refer to this as the interoperability problem (Figure 1).

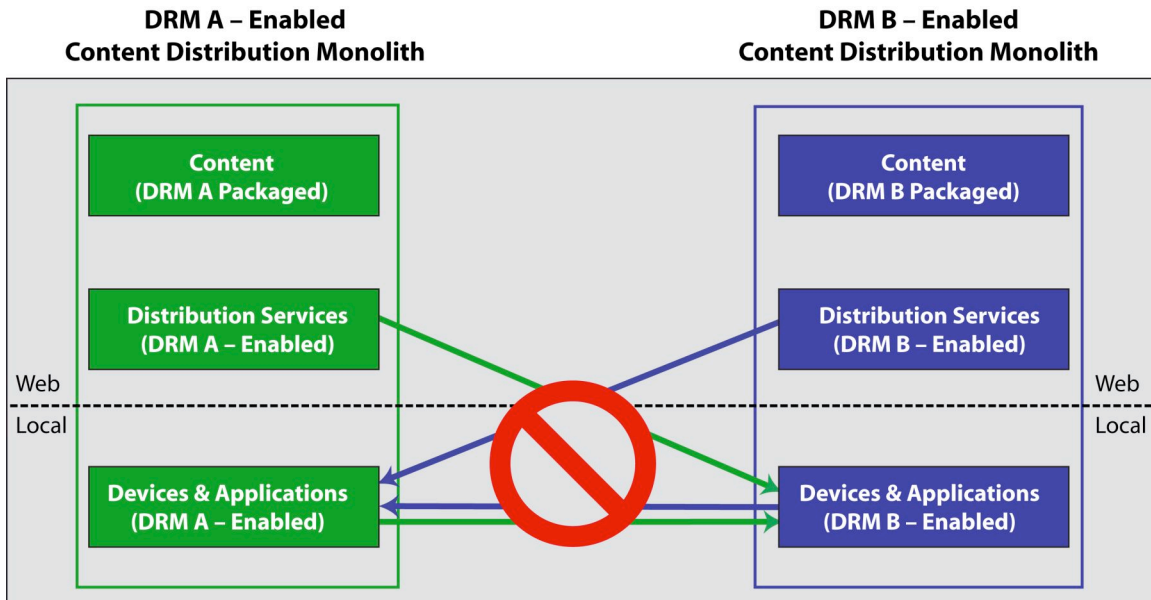


Figure 1. The Interoperability Problem

When the interoperability problem is limited to different content formats or encoding schemes, for example AAC and MP3 in the audio domain, the problem is annoying but solutions exist that can translate content from one format to another. However, the problem is further compounded when DRM and content protection schemes govern content distribution and usage. Content providers must now trust not only the protected format used to distribute their content, *but also* any other format into which that content may be translated as well as any associated services, devices, and players. This trust includes having confidence that usage and distribution rights expressed in one system maintain their equivalent semantics when expressed in another.

Typically, when institutions use different distribution solutions, a *de facto* standard emerges or the institutions and other interested parties work together to standardize an approach that meets everyone's needs. This is a time-honored approach to solving interoperability problems. In general, once the new solution is in place, we encounter the same problem as when a new format emerges which is that there will always be new alternatives. This is especially true for DRM systems. DRM technology requires rapid evolution and response to new threats and attacks. As with almost any security technology, relying on a single approach can be disastrous when that approach is compromised. Additionally, since DRM provides distribution frameworks with trust and control needed to create distribution business models, using a single DRM approach limits the flexibility required by various existing and emerging content value chain participants. It is therefore highly likely that there will always be multiple approaches to DRM.

As mentioned above, Coral has based its Interoperability Framework on service-oriented architecture and associated relevant standards to develop a framework that supports interoperability between different DRMs and content formats with the goal of providing a consumer experience that is intuitive and transparent. In the ideal scenario, consumers will be unaware of DRMs and content formats, as they are able to use their content seamlessly across the entire range of their devices and applications.

The Coral Interoperability Framework Architecture

Trust management is an essential aspect of every Digital Rights Management system — it is the means by which known, legitimate participants in a content ecosystem are distinguished from unknown and potentially untrustworthy participants. One of the primary goals of the Coral Framework architecture is to provide a common trust framework that can bridge the differences in the trust management between diverse but trusted DRM systems.

In the Coral Framework architecture, trust management has two facets:

- *Certified identities.* Every device or system that adheres to the Coral Framework architecture specifications receives a unique, certified identity that can be used as a basis for trust with other Coral-compliant systems.
- *Trusted Roles.* Each Coral-compliant device or system must be certified for one or more roles defined by the interoperability framework. For example, systems that control the movement of rights adopt a role, and DRM license servers that turn the expression of those rights into specific DRM licenses adopt another role. Coral roles act as a second layer of trust management, ensuring that only entities authorized for particular behaviors engage in them.

Taken together, these two layers of trust management ensure that devices and systems built by different manufacturers and integrated with different DRM systems can engage in trusted communications with one another in a compliant manner.

While certified identities provide a necessary ingredient for cross-vendor interoperability, the majority of technical specifications in the Coral Framework architecture are concerned with behaviors that must be adopted in order to obtain certain roles in the interoperability framework. There are potentially two types of behavior specified for each role defined by the Coral Framework architecture:

- *Interface Behavior.* Each role may require its holder to expose one or more interfaces to other Coral-compliant systems, which implement other Coral roles. These interfaces are standardized to ensure that the interacting parties will be able to analyze and process messages – that is, to communicate – regardless of their implementers. The Coral interfaces are built on a trusted messaging framework that (a) ensures that the sender and receiver hold certified, trusted

identities; (b) ensures that the sender and receiver hold the proper roles for the transaction in question; and (c) protects information on the communications channel for confidentiality and integrity.

- *Persistent Role Behavior.* Each role may be associated with behavior that persists across invocations of the interfaces it is required to expose. For example, one role acts as a storage point for rights. In this capacity, it must not only expose interfaces for storing and retrieving rights, but must also persistently cache those rights until they are explicitly removed.

The roles specified in the Coral Framework architecture define the basis for DRM interoperability transactions. Particular business decisions (such as the choice of acceptable usage models) are left to ecosystem specifications built on top of the Framework. For example, the Framework architecture specifies data structures and interfaces for handling DRM-neutral encodings of usage models, but it is agnostic as to the specific nature of those usage models or the policies that govern their movement among DRM systems.

The Coral Framework architecture defines some 30 roles that represent the various functions that are active in a typical interoperability transaction. Some of these roles simply provide information (such as the media formats a device supports), whereas others make relatively sophisticated policy decisions. The list below highlights some of the more critical roles defined in the Coral Framework architecture.

- *DRM-integrated roles.* Some of the roles defined in the Framework architecture connote integration of native DRM functionality with Coral functionality. This type of integration allows a formerly non-interoperable system to participate in a broader ecosystem of devices and technologies. The Framework architecture does not specify the nature of the integration; instead, it focuses on the interface contract between the DRM-integrated system and the rest of the Coral Framework. Examples of DRM-integrated roles include:
 - *License Issuers.* One of the key roles in the Framework architecture, License Issuers are Coral interfaces to proprietary DRM license servers. License Issuers expose an interface that allows a Coral Framework to request a generation of DRM licenses in a native DRM format without requiring detailed knowledge of those (many) formats to be integrated into Coral. A device or system that implements the License Issuer role is responsible for converting messages from the Coral Framework into specific requests to generate DRM licenses, and must be integrated with a native license server.
 - *Content Handling Roles.* These roles are integrated with DRM export functionality and DRM packaging functionality to allow the transcoding of protected content without the intervention of additional online services.

These roles are optional, but provide the convenience of a purely local content chain between DRMs that are capable of local export and import.

- *Pure Coral roles.* The Coral Framework architecture defines several roles that bridge between multiple DRM systems, or perform tasks that are not DRM *per se*.
 - *Rights Mediators.* A Rights Mediator is the key participant in any DRM interoperability transaction defined in the Framework architecture. It acts as the policy decision point for such transactions, and applies the policies agreed to by all the participants in a content ecosystem. Its primary responsibility is to collect enough information to decide whether a given interoperability transaction is allowed, and if so, to create tokens that prove the authorization.
 - *Rights Registries.* These act as DRM-neutral storage points for rights transacted in a Coral system and thus provide a crucial ingredient for building end-to-end systems that are not dependent upon individual DRM technologies.
 - *Principal Identity Managers.* These provide a DRM-neutral way of representing relationships amongst various entities in a content distribution system. For example, in interoperable home domain models, the member devices must represent their membership in a way that does not depend on the particular DRM systems they support. Principal Identity Managers can also act as the front end to existing identity management systems (e.g., such as that specified by the Liberty Alliance) that maintain equivalence relations between user names.

Fundamentally, the Framework is designed to provide monolithic content distribution systems with a means to exchange any information that can enable the consumer to experience interoperability; moreover, this is done while providing the rest of the participants in the content distribution value chain with the flexibility to use whatever DRM or format best suits their respective needs. This framework works in both online and offline modes. Currently, consumers can acquire content from a content distribution service that supports one DRM and play that content on a device that supports the same DRM. Using the Coral Framework in an online mode with roles provided via online independent services or as part of the content distribution services, consumers can reacquire the content in the form required by their other devices that support different DRMs. The framework can also function in an offline mode with local instantiations of Coral roles that allow consumers to transform the content to the form required by their other devices.

The relationship of the Coral Framework elements is depicted below (Figure 2). The Coral elements in this figure are meant to represent functionality; the Coral nodes can exist as independent services or can be part of existing services or devices. Additionally, Coral can be configured so that some of the various interoperating

elements are not aware of Coral. For example, one of the DRM B-enabled devices below may not support Coral interfaces. That device simply contacts a local content manager that is itself Coral aware. The content manager then acquires the content in the form required by the requesting device using the Coral framework to mitigate any DRM or format differences. This is further elaborated in the following Coral-enabled use case.

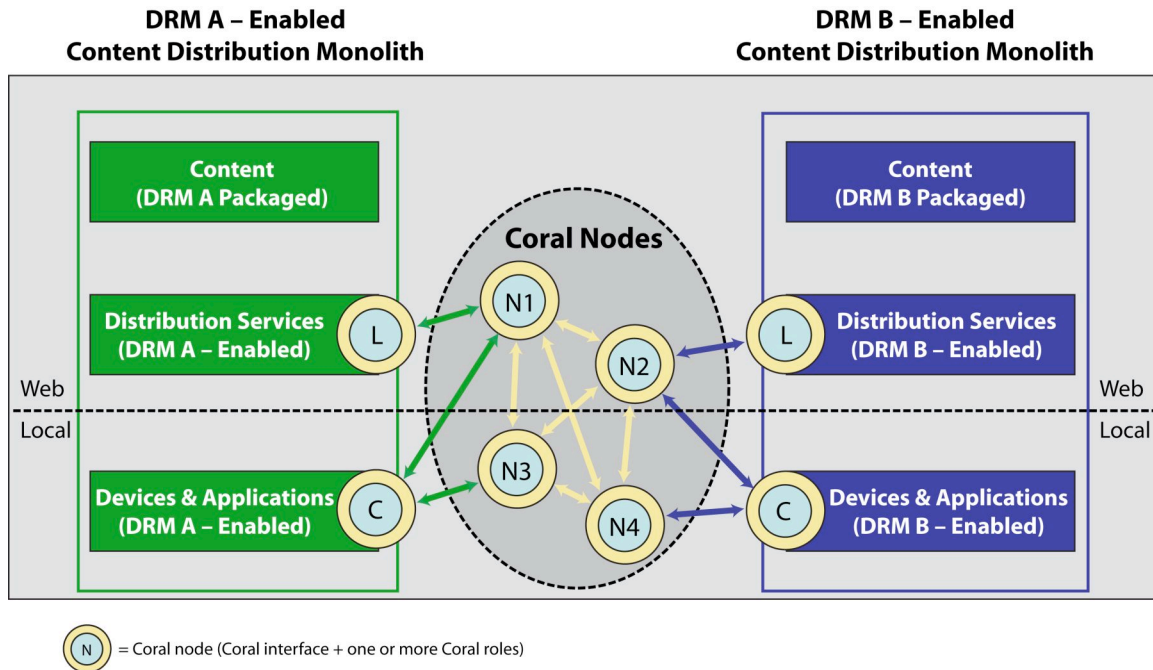


Figure 2. Relationship of Coral Elements

Deconstructing the Coral-Enabled Scenario

1. Bart purchases content from a DRM A-enabled distribution service to play on his PC Media Center
 - a. In the background, Bart has acquired and stored a DRM-independent token that is a proof of his purchase of this content.
 - b. A Coral license issuer role interfacing with the distribution service manages the token and indicates to the DRM A license service that it should create a DRM A license for Bart

- c. Bart acquires the license on his PC Media Center and can access the content using the DRM A-enabled rendering engine.
2. Bart then acquires a new device that he connects to his local area network
3. Using this new device Bart connects with his PC Media Center and sees the content that he had recently purchased
4. Bart drags that content onto his new device and it begins to play
 - a. In the background the following has happened to make this possible:
 - i. Bart's new device has contacted his Media Center and requested a copy of the content in DRM B format
 - ii. The PC Media Center's Coral Client role contacts a Coral Rights Mediator node requesting a DRM B version of the content (NOTE: The Coral Rights Mediator role is pictured as an independent web service - it could actually be a local service or actually part of a content distribution services)
 - iii. The request includes information about the content (such as the location of the token mentioned in step 1.a) and the information about the requesting entity (its DRM, ID, etc.) The request also includes information regarding the desired outcome of the rights mediation process (request the creation of license for DRM B for specific entity and under certain usage model.)
 - iv. The Rights Mediator contacts a Principal Identity Manager node to synchronize user IDs and a Content Identity Manager node to synchronize content IDs across different distribution points
 - v. The Rights Mediator contacts the token home service to ascertain that it is acceptable for a new, DRM B formatted version of the license and content to be created
 - vi. If successful, the Rights Mediator then contacts a DRM B based distribution service (perhaps pointed out by the original service or by using other discovery mechanisms)
 - vii. The DRM B-based service creates a new license for the requesting device and returns it either to the PC Media Center or directly to the requesting device (as pictured below in Figure 3)
 - viii. Bart is able to access the content on his new device.
5. The PC Media Center can set this up at the time that the new device is added to or registered with the local network so that there is no delay.

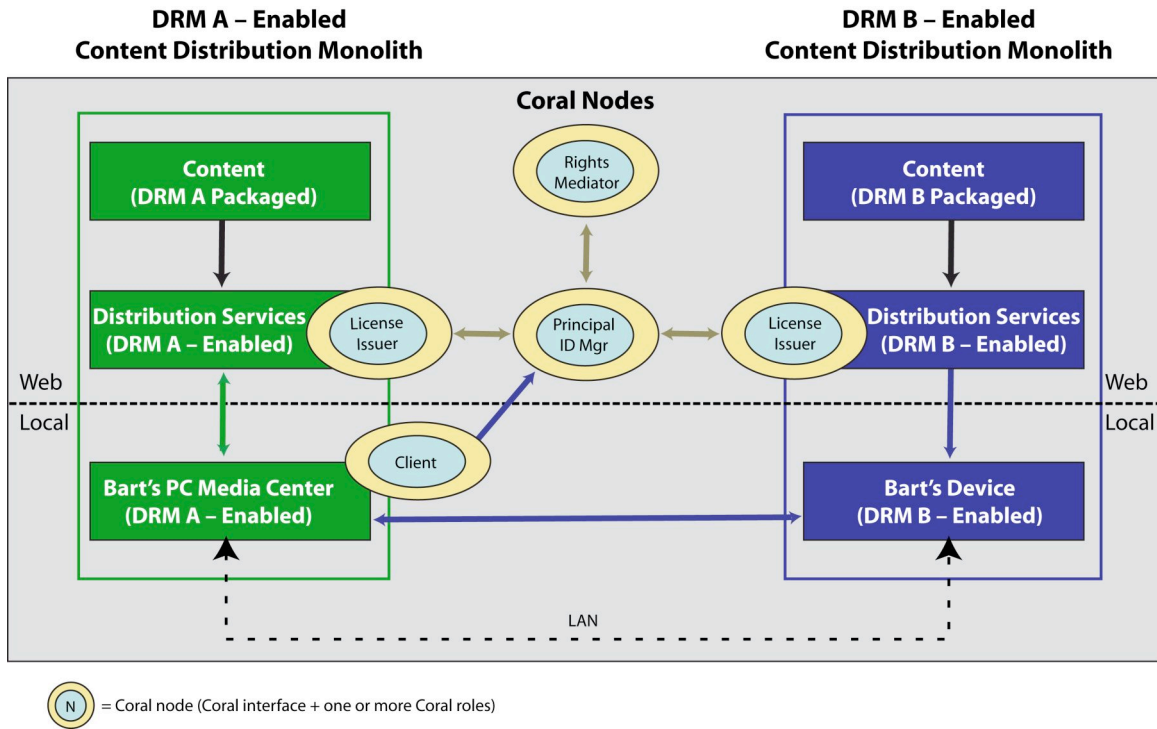


Figure 3. PC Media Center.

The above example is one of many possible scenarios. Clearly, it is possible to create a set of services that the consumer knows very little about and that support content discovery in a form that is required by all consumer rendering devices and applications. Content providers may choose to support multiple formats (as is currently the practice), or work with format translation services that are part of the consumer’s local environment or provided by web-based service providers.

Summary

The Coral framework provides benefits to participants across the entire content distribution value chain.

Coral and Content Companies

- Content companies can use the Coral framework to maintain consistent control of their content across all devices and distribution channels regardless of DRM or format support.
- Content is accessible by any trusted and compliant device.

- Response to DRM and format upgrades by existing devices and applications can be managed by policy-managed services.
- Overall improvement of the world of legitimate content distribution removes incentives for consumers to use non-legitimate channels.

Coral and Device Manufacturers

- Devices may be designed and manufactured to support the DRM approach and content format that is most suitable to the manufacturer's business and technology needs.
- The Coral framework provides a guarantee that these devices will be capable of playing content published in alternative formats using alternative DRM approaches.
- Avoiding the need to put multiple DRMs on a single device is particularly important on portable devices, which are restricted by memory capacity, computing power and cost issues.

Coral and the Consumer

- Consistent and intuitive access and usage models for content across all devices and applications.
- Legitimate high-quality content sources for all devices.
- No more confusion about formats and DRM.

Coral and the Service Provider

- Expands service provider's market reach
 - Not constrained by DRM implemented
 - Allows competition on service offering not DRM technology chosen
- Service-based domain management and rights lockers
 - Creates "stickiness" with customers
 - Provides consumer value
- Consumer portability

The goal of Coral in the domain of consumer media services and applications is to minimize barriers to consumer access to content of all types, regardless of device, location, or time. As service, application, and device providers adopt Coral interfaces and the interoperability philosophy, all value chain participants will realize the promise of content distribution service frameworks that provide consumers with a rich set of services that go well beyond experiences with unsanctioned or illegitimate services.