Creative Content Online

Coral response to the EU Commission Consultation

Background to the Coral Consortium Submission

The Coral Consortium was formed in September 2004. Its current membership includes content companies, consumer electronics companies, service providers, and technology companies[1]. Its founding charter was to create a framework that enables interoperability across existing and future DRM systems for content distribution. For Coral, a fundamental assumption has been that there will always be multiple approaches to DRM. A single DRM standard will be difficult to achieve primarily for non-technical, business and trust issues.

Coral's goal has been to create an interoperability framework such that to the consumer, DRM is as invisible as possible and content usage across all of a consumer's devices is transparent. Coral's participants believe that to be successful, the digital content distribution industry must provide consumers with a positive experience. The industry must seek solutions that provide consumers with this transparency and instill in them confidence that DRM-enabled content will remain available over time and across different devices. In addition to these consumer-oriented goals, Coral sought a solution that would require little change to participating DRMs. Coral's resulting framework specifications, released for application in October 2007, meet all of these goals.

Using the Coral framework, it is possible to deploy content distribution ecosystems that support multiple DRMs. Coral has standardized a framework that provides for secure exchange of relevant data among participants in an ecosystem of service providers and other parties that have deployed different DRMs and that have agreed to interoperate. Coral does this by associating a DRM-independent "token" with each piece of content acquired by a consumer. The token is then used to derive DRM-specific licenses for each DRM that participates in the ecosystem. From that point, the content and its associated license are managed by that DRM. Coral supports both a model that allows consumers to download multiple copies of content encoded by the different DRMs (the "reacquisition model") and a model that allows direct device-to-device transformation of content. The latter model requires the participating DRMs to trust one another explicitly as part of their technical policy. The reacquisition model (which is increasingly convenient as available bandwidth increases) does not. From the consumer's perspective, use of the appropriate model is determined by the specific application and will be nearly transparent.

In other words, the Coral technology provides for DRM interoperability via a secure platform, which allows different DRM technologies to coexist without compromising their respective security and confidentiality. The technology operates in a way that is seamless and invisible to the consumer.

Consumers have made it very clear that they want their content to be portable and persistent. That is, consumers want their content to be usable across all of their devices and they want to trust that content acquired via the Internet will survive local disk crashes as well as the whims of the

---

[1] For a complete list of current members see http://www.coral-interop.org/main/membership/index.html.

marketplace as content formats, DRMs, service providers, etc. come and go. Coral provides support for content portability across devices through a Domain model, and for content persistence during mishaps and change of service providers through a Rights Locker model.

Executive Summary

The following points provide a summary of Coral's position on DRM interoperability:

- Coral is a very broadly based consortium which has created open standards for interoperability between DRMs
- Interoperability is key to consumer value proposition. It is not true that interoperability comes only from using a single DRM or no DRM at all.
- Interoperability and security are not mutually exclusive
- Coral members assert that it is not necessary to allow circumvention of DRM technology to deliver interoperability
- Coral makes specifications available that will facilitate content interoperability among different DRMs without compromising content security and without requiring DRM providers to expose the inner workings of their DRM
- The Coral specifications are available to all interested parties.
- Coral encourages all content owners and DRM providers to look at its specifications and to consider implementing them.

Details about all aspects of the Coral approach and the Coral Specifications can be found at www.coral-interop.org.

Interoperability is as much a business issue as it is a technical one. It is important to note that interoperability among DRMs can only happen if the entities that support and use the DRMs agree to interoperate.

Questions:

Coral responses are provided for questions 1, 2, and 5.

Digital Rights Management

1) **Do you agree that fostering the adoption of interoperable DRM systems should support the development of online creative content services in the Internal Market? What are the main obstacles to fully interoperable DRM systems? Which commendable practices do you identify as regards DRM interoperability?**

   Fostering the adoption of interoperability across DRM systems will absolutely support the development of online creative content services in the Internal Market. There are two major inhibitors of the widespread adoption of content acquisition using the Internet:

   1) Lack of DRM interoperability – if a consumer acquires protected content for use on a device that supports one DRM scheme, they cannot play that content on a device that supports another. Even on a PC, there is no single software application that supports multiple DRMs seamlessly. Consumers have made it quite clear that the ability to play their content across all of their devices seamlessly is of paramount importance. Therefore arriving at a solution that provides for this interoperability and seamlessness and yet also provides the kind of protection that the content industries require is critical if digital content distribution is to meet its full potential.

   2) Lack of persistence of rights – if a consumer purchases a piece of content and their storage is broken or lost, their content is often lost as well. The consumer should absolutely have their rights stored online either by their original retailer or by a service that provides this. It is reasonable to expect consumers to be charged for restocking their content libraries if the content is lost and it is important to be sure such services do not become a means for manipulating the system for improper use. However, by supporting online content rights storage, electronically distributed content could easily be more durable than the physical forms it is trying to replace. Additionally, this kind of support will strengthen consumer trust in digital content distribution systems. (Below, we will explain how Coral supports this feature via Coral Rights Lockers).

Three aspects of DRM that make interoperability particularly challenging:

1) **Semantic Interoperability** – ***Consistent support for content usage or business rules across multiple DRMs*****:** DRM systems are not equally expressive. They vary greatly in terms of the usage models they can express. Typically each DRM supports a means for expressing content usage models using a form of rights expression or some other paradigm for capturing the semantics, meaning, or terms of that usage model. These expressions are delivered either separately from or together with the content. The client-side of the DRM processes the expressions in such a way that content providers and service providers can be sure that the content will be used consistently with their intended semantics. The various means of expressing the semantics differ in subtle

ways, which makes translating from one paradigm into another generally a difficult problem.

Coral does *not* require translation from one expression paradigm into another. Coral's approach works around this problem through the use of a Rights Token – a DRM-independent data structure that associates a user identifier, a content identifier, and a business model identifier. Note that the Rights Token does *not* express the semantics of the business model – it merely identifies that model. DRMs chosen to participate in a Coral Ecosystem are chosen in part based on their ability to faithfully execute the semantics of the business model referenced by the business model identifier. These DRM providers are responsible for creating the logic that maps the Coral Rights Token into their own specific license generation functionality. When content is required for a device or application that supports a particular DRM, the service provider that is responsible for creating content licenses, uses this DRM-specific license generation functionality to create a license based on the information included in the Rights Token.

2) **State Management** – ***Keeping track of business model-specific state information across multiple DRMs*****:** State management refers to the fact that DRMs sometimes need to remember certain values. For example, assume a domain model in which consumers are allowed to create domains of all of their devices up to some limit. Some entity is required to keep count of the number of participating devices for a particular domain. This number of devices is a state variable for that domain. Other state information often associated with content distribution systems may be the number of copies allowed, or the number of times a piece of content can be played. Typically this state information is managed by the DRM. Managing these values across multiple DRMs, as would be required when the different devices in the Domain support different DRMs, must be done by some common functional element or service. Devices must be added and removed from the consumers' device domain, or copies must be counted across different devices that may support different DRMs. If content is purchased in one DRM and moved into another, there must be common state management. Coral provides support for cross DRM state management via its Coral Ecosystem and Coral Domain Manager concepts discussed below.

3) **Trust Management** – ***Ensuring that the interoperability solution doesn't degrade the security of participating DRMs*****:** DRM systems rely on their own secure protocols. Placing new requirements on these protocols to enable interoperability would require intrusive changes that are impractical for technical and business reasons. As such, a pragmatic DRM interoperability solution needs to require minimal (if any) changes to the underlying DRM systems — it needs to work with the systems as they are designed. DRM systems typically define a trusted channel through which content may flow, defining behavior along every step of the process from delivery to consumption. The definition of this behavior includes rules for the robustness and tamper resistance of implementations as well as rules associated with approved content outputs from devices and other aspects of content consumption. Content providers trust implementations that are compliant with these rules. Typically these robustness and compliance rules are defined by the DRM vendor in conversation with content companies. There exists no single set of rules that covers all DRMs. So, if a content distribution solution is designed to include interoperable support for multiple DRMs, it must consider how to

harmonize the compliance and robustness needs of the content providers supporting this distribution solution with the specific compliance and robustness rules associated with each DRM.

Coral approaches this aspect of DRM interoperability through the definition of the Coral Ecosystem concept. Ecosystems include one or more companies working together to create a content distribution system that supports a common set of content business models / usage rules, a set of DRMs interoperating via the Coral framework, service providers, and devices. The ecosystem participants define a set of common compliance rules coupled together with those of participating DRMs. In fact, in the same way that Coral does not require technical changes of participating DRMs, Coral does not tamper with the DRM-specific compliance rules. That is, the Coral philosophy is that DRMs and their associated trust frameworks that are already trusted by content providers should remain untouched to the extent possible. The ecosystem concept ensures that this philosophy is maintained.

Approaches to achieving DRM interoperability:

1) **All devices support the same DRM.** This would seem the most obvious solution to the interoperability problem. There are several possibilities here:

   - One of the existing DRMs emerges as a de facto standard,
   - Interested parties create a standard DRM, or
   - A standards-based intermediate DRM is created into which others translate.

   Indeed many attempts to standardize DRM have been made, some of them still underway. Though these standards may achieve varying levels of commercial adoption, it is unlikely that one will emerge as the only DRM. There are several reasons for this. One has to do with a fundamental aspect of DRM – trust. In order for a single, standardized DRM system (de facto or other) to be truly interoperable, a single, monolithic trust system must be established across relevant players and geographies. Such a trust system would be responsible for ensuring the robustness of implementations, the adherence to and compliance with security and trust policies, and the management of security and trust credentials. Currently, the DRM vendors provide their own DRM-specific compliance frameworks. Content providers put their content into those DRMs that they trust. With one common mandated DRM, there would be no market forces to assure appropriate protection. Additionally, with only one DRM in place, there would be very little incentive to innovate with respect to support for new business models or new usage paradigms that evolve as a result of technological advances. That is, competition among different DRM providers is ultimately good for all participants in the content distribution value chain – particularly consumers.

   Even if agreement on the technical aspects of arriving at one DRM solution were possible (and this has proven elusive because of the various players' differing requirements), the trust issue and the need to respond to the evolving marketplace would be very hard to tackle in an open-market economy.

Another important factor is that a single solution provides a single point of failure against which attackers can focus all of their energies. It is simply bad security practice.

2) **Devices support multiple DRMs.** This is typically expensive for the device manufacturer, and makes product development longer than necessary – there could be many DRMs to support in each device, each requiring hardware real estate, software development time and effort, and license fees. Additionally, because of the security requirements, changing from one DRM to another in a device typically adds latency and metadata mismatches, which degrade the user experience. Each DRM will also require certification and trust credentials, which may or may not be available from a single source – resulting in yet more overhead. None of this additional overhead is welcomed by the consumer electronics industry, and consumers will inevitably pay a premium for their devices because of the duplication of technologies and development cost.

3) **Translate and exchange content and rights between mutually trusting DRMs.** In this case, content is transcrypted and licenses are translated from one DRM system to another. DRM providers would establish bilateral trust relationships with one another, and a set of exchange semantics would be required for each pair of mutually trusting DRMs. If there are only a few DRMs in the market, this solution might work. However, as the number of DRMs increases, this approach clearly does not scale. In order for each new DRM to enter the marketplace in an interoperable fashion, it would have to establish such a relationship with all existing DRMs, which may not have a business incentive to do so. An alternative but similar approach requires all DRMs to share "secrets" with one another to enable transparent interoperability. This approach again requires a single trust management solution. Additionally, this solution suffers from the semantics mismatch and state management problems described above and it also has the effect of providing attackers with a single focus for their attacks. It simply ignores commercial and competitive realities of DRM vendors.

4) **Translate and exchange content and rights between DRMs using a common semantic framework and a common secure authenticated channel.** In this case, the semantic interoperability problem is resolved using a common semantic framework from which rights expressions in all DRMs are derived. The difficulty with this approach is that it requires the participation of the DRM vendors who must agree to interoperate and to trust the common semantic framework and the common secure authenticated channel. Thus far the largest DRM vendors have not agreed to permit this but technically, it is something they could do with relative ease and it would very much facilitate interoperability for the consumer. In Coral, as described in the section on *Semantic Interoperability*, the common semantic framework is based on the Rights Token concept, which avoids the need for rights expression translation between DRMs. Coral provides support for this particular interoperability model via this Rights Token concept, a common secure authenticated channel, and a set of client-side functional elements for exchanging content.

5) **Reacquiring content packaged in each of the DRMs supported by consumers' devices.** In this model we assume a consumer purchases content on a device that supports DRM A and wants to play the content on another of their devices that supports DRM B. The second device can then download a new copy, including appropriate rights, from a source that has knowledge of the business model under which the original content was licensed. This does require time and bandwidth, but with the ever-increasing availability of bandwidth and with peer-to-peer mechanisms becoming ever easier to use, this is a reasonable approach. This method solves the trust issue and doesn't require translations between different rights encoding frameworks. Coral supports it natively via its Rights Token concept.

   In this reacquisition model, content acquisition (purchase, rental, etc.) by consumers would result in the association of a Rights Token with the transaction. Whenever a consumer needs content for a device that supports a particular DRM, the content distribution service provider passes this Rights Token to a DRM-specific license generator to generate a license for the requested DRM. The content and content license are then delivered to the consumer's device using exactly the same mechanisms native to the specific DRM – as if that DRM were the only DRM being supported. That is, content and rights are *reacquired* for each device supporting a different DRM. From the consumer's perspective, this can all be done transparently.

In summary, Coral supports both the reacquisition model (model 5) and the local transformation model (model 4).

Recommended practices:

Coral identifies the following commendable practices as regards DRM interoperability, within the bounds of a well-defined, unified usage model[2].

1) **Rights Lockers:** Coral proposes the adoption of voluntary Rights Lockers services to support the persistence of consumer content rights. When consumers purchase content, they should have the option of having their "rights" stored with a Rights Locker service of their choice, or provided by the retailer. This enables not only the reacquisition of content in the event of a damaged or lost device but it also facilitates access on multiple devices and from multiple locations while respecting the usage rules related to the specific content. It should also enable the persistence of rights when service providers go out of business, and the portability of rights from one service provider to another. Again, this process must be monitored for abuse and may be an optional, additional service against payment. In Coral's view provision of this service is necessary to achieve more consumer confidence in electronic distribution.

[2] Each of these recommendations must be consistently applied in the context of specific usage models. Persistence of rights can only be supported for usage models for which such persistence makes sense. For example, for electronic sell-through content, such persistence is clearly germane. However, for rental models, it is not. Similarly for domain models, access to content by a consumer on all of their devices may and may not be consistent with the terms of a specific usage model. For example, under a rental model content may only be accessible on a subset of a user's devices.

2) **Domain Managers:** Coral proposes the adoption of "Domain Managers". A Domain Manager is a service or application that allows a consumer to register their devices into a grouping called a Domain (also known as Authorized Domain, Home Media Network, Personal Area Network). The consumer should be able to add or remove devices from their domain when they acquire, dispose of, or lose devices. The size of the domain is determined for specific ecosystems and is managed by the ecosystems' domain manager services. For the consumer, this creates an ideal situation in which they are able to move their content freely among all of their devices.

   Both of the above commendable practices are supported in the Coral framework. Coral provides specifications for Domain Managers and Rights Lockers that support interoperability across DRMs.

2) Do you agree that consumer information with regard to interoperability and personal data protection features of DRM systems should be improved? What could be, in your opinion, the most appropriate means and procedures to improve consumers' information in respect of DRM systems? Which commendable practices would you identify as regards labelling of digital products and services?

These comments apply to questions 2, 3, and 4.

This subject is beyond Coral's Charter.

However, Coral's interoperability solution would go a long way to resolving consumer concerns in this area. If content will play on all or almost all devices regardless of the specific DRM used, then there will be fewer issues to deal with as regards information in EULAs and arbitration of claims by consumers disappointed by a lack of interoperability. Indeed, use of Coral to provide this interoperability, presents the consumer with common, DRM-independent usage terms implicated by the Coral rights token. We expect that the simplicity of this approach will make it easier to express to consumers the terms under which their content may be used.

3) Do you agree that reducing the complexity and enhancing the legibility of end-user licence agreements (EULAs) would support the development of online creative content services in the Internal Market? Which recommendable practices do you identify as regards EULAs? Do you identify any particular issue related to EULAs that needs to be addressed?

See answer to question 2.

4) Do you agree that alternative dispute resolution mechanisms in relation to the application and administration of DRM systems would enhance consumers' confidence in new products and services? Which commendable practices do you identify in that respect?

See answer to question 2.

5) **Do you agree that ensuring a non-discriminatory access (for instance for SMEs) to DRM solutions is needed to preserve and foster competition on the market for digital content distribution?**

Coral believes that DRM should be available to all parties that need it to enable their business, large or small. It is difficult to create a single DRM that suits all parties. Coral enables the existence of multiple DRMs catering to different markets and customers, providing an interoperability path where needed.

Using the Coral mechanism a service provider or device manufacturer can choose any DRM they want. Coral provides a mechanism whereby compliant DRMs can interoperate. Coral does not require DRMs to share their secret information to facilitate this interoperability. A fundamental premise of the Coral solution is that the DRM systems themselves remain robust and secure per each DRM system's specific terms.

Please submit your comments by 29/02/2008 in electronic format. All submissions will be published on the Commission's website if not requested otherwise. Contribution to be treated confidentially should indicate this at the top of the first page. Should you want to add a cover letter please do so in a separate document. In case your comments exceed four pages, please provide an executive summary. All submissions should be mailed to the functional mailbox of the Audiovisual and Media Policies Unit of the Directorate-General for Information Society and Media: avpolicy@ec.europa.eu.