

Digital Rights Management (DRM) RSA Security Business Brief

Alexandre Stervinou

<astervinou@rsasecurity.com>

RSA Security Inc.

Abstract

Forrester Research predicts that content owners will be losing \$4.6 billion per year by 2005 due to piracy. This has created an impetus in the market to find solutions that will protect the rights of content owners in the digital world. Content owners want to take advantage of the lower costs, viral marketing opportunities, and consumer satisfaction that comes with digital content distribution. Piracy fears have become a harsh reality for the entertainment industry with the advent of unrestricted peer-to-peer file sharing technology, high-quality, open digital content formats like MP3 and duplication technology that creates near-perfect copies of offline media. Consumers have taken well to these new technologies as they allow them flexibility with their purchased media.

However, consumers are generally not well-versed in the complexities of copyright law and their desire for more digital content functionality has far outpaced their understanding of the consequences of their actions. The entertainment industry has attempted to respond with copy protection and other technologies that prohibit digital duplication, but these technologies have been met with collective chagrin by consumers who believe the industry is interfering with their rights. The entertainment industry desires to give consumers the digital experience they want, but, they have their own business and the rights and compensation of their artists to protect. It is a delicate balance that has yet to be achieved with currently employed technology. The fundamental issue that has led to consumer resentment of protected content arose in this physical world: consumers believe once they pay for a piece of content, they “own” it, and should have very liberal rights to do with that content as they please. The entertainment industry has been forced to resort to costly and unfortunate legal action in an attempt to protect their rights and their business. Continued frustration on all sides will not improve the digital content experience for anyone. RSA Security understands these complexities and works with the leading standards bodies in the industry to champion open, broadly-compatible solutions that tackle these challenges with proven, stable security technologies. Our solutions help give consumers the seamless, flexible digital content experience they desire while ensuring the rights and revenue of copyright owners are fully protected.

1 WHAT IS DIGITAL RIGHTS MANAGEMENT?

Digital Rights Management technologies restrict access, usage, and distribution of content in digital form after a user receives it within boundaries specified by content owners as terms of their contract with the recipient. Digital content, in essence, becomes “bound” to the recipient and only the recipient (i.e. original licensor) is granted rights to access, use, or (in rare cases) distribute that content. Essentially, DRM solutions attempt to keep consumers within the bounds of copyright law through technological means. Unfortunately, to date, many DRM solutions have been difficult to use, not sufficiently transparent, easy to circumvent, or place restrictions on consumers outside the bounds of their expectations. Successful digital content services such as Apples iTunes have proven a significant segment of consumers will pay for protected digital content if the process is as frictionless as possible. In contrast, current solutions from other leading technology companies use incompatible rights management technology that creates friction for those consumers that prefer one vendors portable music devices yet enjoy anothers music services: the two do not work together because those devices cannot assert the appropriate digital rights defined in the services music format. Granting consumers the experience they really want requires content portability.

2 ACHIEVING CONTENT PORTABILITY

Consumers believe the digital content they pay for should be usable on any device they own, from their personal computer to their portable music player to their home or car stereo. Consumers purchase

personal electronics devices based on the features provided by those devices giving little or no thought to what digital formats, rights management, or other technologies they support and they should not have to. The largest fear of the entertainment industry is a proliferation of varying digital formats and rights protection technologies will create an environment of customer confusion and frustration as consumers purchase more advanced digital devices. This problem also compounds as device capabilities continue to converge. For example, you now have mobile phones on the market with embedded digital music players. The only way to provide content portability that avoids this conundrum is by enabling rights portability.

Rights portability can be achieved through a trusted value chain that binds the identity of consumers to their devices, consumers to their licensed content from various content services, and the unique identity of those devices to the network. This creates a network of trust ensuring that consumers get the experience of portability they desire with their content while protecting the rights of content owners. This will also enable content owners to enforce appropriate usage rather than extreme restrictions for a consumers own devices because there is surety built into the system that those devices should be trusted. This model will help provide the seamless digital content experience consumers expect while still protecting the rights of copyright holders. This provides a needed parallel in the digital world to the physical world of the compact disc (CD) where you are assured that any CD should play on all CD players. In order for this trusted network to emerge, however, standards-based rights management technology must be built into an increasing number of consumer devices to support rendering and playback of protected digital content. Only this will help create the frictionless commerce experience needed to provide significant value over free, unprotected services.

3 PORTABILITY REQUIRES OPEN STANDARDS

The industry is already working on putting the infrastructure in place to build this trusted network. Standards bodies like the Open Mobile Alliance (OMA) are developing rights management standards that are widely supported by content owners, service providers, and device manufacturers. The OMA is a broad consortium of over 200 leading consumer electronics, entertainment, software technology, and service provider companies. It is committed to developing standards that work seamlessly across networks, devices, service providers, and geographies. Standards will ensure consumers can be comfortable purchasing the digital devices, services, and content they desire based on capabilities, convenience and price, not on whether they support a particular vendors proprietary technology. The collective innovation of the industry can be brought to bear in bringing consumers the legal and profitable digital content experience they desire while ensuring content owners and their artists are properly compensated.

RSA Security is a member of the OMA and coauthor of the latest version of a key standard for DRM, OMA DRM 2.0. Proven, widely deployed security technologies such as identity management, strong authentication, encryption, and certificate handling are all essential to the success of a portable rights management infrastructure. RSA Securitys strong market reputation and technical leadership in all of these areas allow us to contribute significant value and expertise to these standards efforts. For nearly 20 years we have been a champion of information security standards and we are committed to helping our customers have the most flexible, compatible, and broadly applicable standards-based DRM solutions available.

The OMA DRM 2.0 architecture is not limited to wireless devices. It is an open architecture designed to be easily supportable by a broad range of platforms and devices. RSA Security is working to expand the standard and usage of the technology to personal computers and all types of digital devices. We are committed to pursuing open standards and working with all parties independent of content formats to establish trust among all parties and ensure digital content services are a success for all involved.

4 ENABLING NEW BUSINESS MODELS

OMA DRM 2.0-compliant solutions also enable new business models for content owners previously not available with DRM technologies. The OMA DRM 2.0 model is built around a concept called “domains.” A domain is a logical grouping of authenticated, trusted devices. There can be any number of domains, any number of devices can be part of a single domain, and devices can exist in multiple domains granting flexibility. There can be a domain associated with a single consumer and all of their personal devices are registered to that domain. Or, you can create a domain that includes an entire family and all of their devices. This enables flexible rights and usage models that better mirror the reality consumers are

accustomed to in the physical world. For example, families would be able to share digital music with each other much the way they share compact discs today as long as all are part of the same domain.

The domain concept also enables broader distribution models that can be used to generate even more revenue through techniques such as promotional tie-ins and geography-based targeting. For example, a domain could be established for all attendees to a popular artists concert who own portable music players. After the concert, the attendees would receive exclusive unreleased tracks and other promotional media about the artist. In the case of limited release films, for another example, all consumers that own a particular mobile phone in the geographic area of the films release can be sent an exclusive video or audio preview of the film. All of these examples are possible because the OMA DRM 2.0 model ensures registered devices are trusted and content is only utilized in the manner desired by the content owner.

The OMA DRM 2.0 model also enables “super distribution.” Super distribution is a new form of secure peer-to-peer (P2P) technology that enables content owners to take advantage of viral marketing techniques and “word-of-mouth” promotion. Unlike other peer-to-peer technologies, the OMA model restricts distribution to defined domains and usage based upon content owner desires. For example, a consumer may purchase a new digital music single or mobile video game from a popular retailer. As part of their purchase, the consumer is able to share the song or game with any number of their friends. However, when their friends receive the content, they are only able to hear the first thirty seconds of the song or play the first few levels of the game before they are given instructions on how to purchase the full version. This allows powerful “word-of-mouth” marketing to be combined with instant gratification: a desirable combination for many markets, especially young adults. As you can see, standards-based DRM technology enables very liberal and flexible content distribution and usage models that consumers will love, but still ensures copyright holders are properly compensated.

RSA, RSA Security and Confidence Inspired are either registered trademarks or trademarks of RSA Security Inc. in the United States and/or other countries. All other products and/or services are trademarks of their respective companies. © 2004 RSA Security Inc. All rights reserved.