DIGITAL RIGHTS MANAGEMENT FOR MOBILE COMMERCE USING WEB SERVICES

Sai Ho Kwok
Department of Information Systems
College of Business Administration
California State University, Long Beach
1250 Bellflower Boulevard
Long Beach, CA 90840-8506, USA
jkwok@csulb.edu

Robert Chi
Department of Information Systems
College of Business Administration
California State University, Long Beach
1250 Bellflower Boulevard
Long Beach, CA 90840-8506, USA
rchi@csulb.edu

ABSTRACT

Performing digital rights management (DRM) on mobile distribution services encounters many technical problems. Major problems include privacy and trust, coordination and interoperability, security, license management, DRM operations, and payment. This paper proposes a generic DRM framework to tackle these problems. The proposed framework consists of (1) an operational mobile infrastructure; (2) Web Services (WS); and (3) a mobile DRM model. This paper emphasizes on the use of WS for DRM because research applying WS to mobile media distribution services is scarce. The framework enables basic rights insertion and enforcement (both online and offline), and media sharing. It is generic in the sense that it is independent of the generation of mobile technology. The framework has been compared with other similar DRM solutions and the results show that it outperforms them in terms of practicability and capabilities. However, there could be possible overloading and risk problems with it. This paper contributes by (1) proposing a generic DRM framework to support mobile media distribution services; and (2) exploring the use of WS for mobile commerce.

Keywords: digital rights management, mobile commerce, web services, multimedia.

1 Introduction

Nowadays, mobile commerce (abbreviated M-Commerce) is getting more and more important as the number of mobile user grows in a rapid manner worldwide, and the mobile networks and services expand to cross-country and even worldwide coverage. M-commerce is simply a way to conduct electronic commerce using mobile devices. M-commerce usually involves multiple independent business entities, for instant mobile operators, service providers, enabling technology providers, and mobile users. Coordination and interoperability become a great concern in such a business setting. Moreover, the success of M-commerce is also dependent upon the mutual trust among these entities. For example, when intellectual property is a concern of a business, privacy and trust become requirements of the business. Furthermore, other business components, such as payment and security also play important roles in M-commerce.

Media distribution services, including video conferencing, video-on-demand, online music distribution are major mobile businesses. Digital Rights Management (DRM) is required in media distribution services to protect the intellectual property of the distributed digital media [Kwok, et al. 2004]. DRM technology includes rights insertion, rights enforcement, license management, license (or media) sharing and so on. Rights insertion and rights enforcement are responsible for basic DRM operations. License management is to manage the usage and access rights of the purchased media [DRM 2005, InterTrust 2000, Kwok 2000]. License (or media) sharing [Brown 2005, Napster 2005] that involves processes of transferring rights and issuing authorization is a demanding feature in

media distribution services. Payment [CSRA 2005, eCyberPay 2002] is highly related to DRM operations, as usage and access rights are mainly due to the purchasing agreements and terms.

Due to the limitations of mobile device namely low CPU and memory capacities [Piloura, et al. 2003], there are problems to overcome in order to perform DRM on M-commerce. The following are major problems.

- **Coordination and Interoperability** [Kwok, et al. 2003]: Electronic commerce protocols and Web technologies are usually different from sites to sites – from one mobile service provider to another mobile service provider. Integrating DRM into a mobile business with these parties needs to resolve the problems of coordination and interoperability.
- **Security** [Kwok 2003, Memon and Wong 2001]: ID insertion and verification processes are required in DRM. These processes should be treated as black-box processes and sensitive information involved should be kept and handled by a trusted party only, e.g., a clearance house. Crackers and hackers will find it difficult to break into these processes even they are able to gather confidential information, such as buyer's and seller's IDs from the mobile networks.
- **Privacy and Trust** [Cheung, et al. 2002]: Personal information including personal identities (IDs), keys and so on are held by different parties and required to exchange for DRM. Privacy becomes a great concern; in particular trust does not exist in these involved parties. For example, a trust between enabling technology providers and mobile users cannot be guaranteed in all cases.
- **Payment** [Kwok 2002]: A secured payment channel is needed for M-commerce. It is believed that the most secured payment method would be the one using a private channel, such as a value-added network (VAN), and the payment method should involve minimal exposure of personal and credit card information over the mobile network.
- **DRM operation** [Kwok 2002]: The buyer's ID cannot be stored on the buyer's mobile device due to the limitation of storage and processing power. Therefore, trusted third party is required to provide the required ID on behalf of the buyer for rights insertion. With the same reason, rights enforcement is also executed by a trusted party. Besides, DRM technology provider is required in order to perform these DRM operations. However, this is not required in traditional electronic businesses.
- **License Management** [Kwok 2002]: License management models, such as tethered, un-tethered, and enhanced models [Kwok and Lui 2002a, Kwok and Lui 2002b] requires additional storage and processing power to handle and process license documents and rights-protected contents. License management operates at the service provider side when 2.5G or below mobile devices are used because 2.5G mobile technology is not capable of managing licenses.

Web Services (WS) is a strong candidate to tackle the problems of coordination and interoperability among multiple entities [Beneventano, et al. 2004, Rotchanakitumnuai and Speece 2004, Zhou, et al. 2004]. Moreover, it is a solution to the DRM problem of security of M-commerce. The WS paradigm is a promising technology for developing applications in open, distributed and heterogeneous environment. The benefits of the WS include interoperability, dynamic service discovery and reusability. There is a strong interest in making mobile devices capable of providing and consuming web services over wireless networks [Piloura, et al. 2003]. Mohan [Mohan 2002] defines that Web services are self-contained, self-describing, modular applications that can be published, located, and invoked across the web, and Web services perform functions, which can be anything from simple requests to complicated business processes. WS are language- and environment-neutral programming models, which yield flexible and loosely coupled business systems [Vinoski 2002].

To address and tackle the problems of privacy and trust, and payment, an operational mobile infrastructure is needed. We consider the NTT DoCoMo i-mode service [I-mode 2005] that provides a centralized framework to M-commerce as a desirable reference model. Its advantages consist of centralized payment scheme, format conversion, service management and so on.

Regarding the problems of DRM operations and license management, a DRM model that supports DRM operations in mobile environment is preferable. The mobile DRM model proposed by Kwok [Kwok 2002] can offer basic DRM operations for M-commerce. The WS-based DRM infrastructure proposed by [Kwok, et al. 2003] is the ideal solution to us.

This paper proposes a generic DRM framework for M-commerce to tackle all these problems. The framework is designed based on the NTT DoCoMo i-mode infrastructure [I-mode 2005], the mobile DRM model [Kwok 2002], and the WS-based DRM infrastructure [Kwok, et al. 2003]. The proposed framework also indirectly references to the mobile device-driven architecture [Piloura, et al. 2003], as the WS-based DRM infrastructure is inherited from the mobile device-driven architecture. The proposed framework is generic in the sense that it is independent of the

generation of mobile technology. In other words, it can work with 2.5G mobile technology and can also work with 3G or 4G mobile technology.

The paper is organized as follows. Section 2 covers the background of the present study. This includes DRM, Web services and related technologies. In Section 3, we present the proposed DRM framework. Illustrations on rights insertion and rights verification are given. Section 4 compares various DRM solutions in terms of the practicability, capabilities, and limitations. Finally, we conclude the paper in Section 5.

2 Background

2.1 Digital Rights Management

Stewart [Stewart 1998] defined that rights management in general refers to the problems associated with intellectual property rights, including copy protection, and in particular to the problem of assuring that, in a commerce setting, payment is made for a particular use of content, and that the use made does not exceed the use authorized. Further Anderson and Lotspiech [Anderson and Lotspiech 1995] defined DRM referred to the process of honoring those copyright provisions, license terms and usage agreements established by the owners of the intellectual property in online business. In short, DRM protects digital media sold online. For example, in the context of online media business, DRM involves specifying and associating rights with a digital media, placing controls on the media to enforce rights, enabling access checks, and tracking permissions usage and payment. Ramanujapuram and Ram [Ramanujapuram and Ram 1998] stated that the required capabilities contain (1) rights specification and rights label management; (2) content protection, rights enforcement, and trusted rendering; (3) rights authorization; (4) rights tracking; and (5) security and commerce infrastructure. In summary, these DRM requirements are implemented in rights insertion and rights enforcement processes [Kwok and Lui 2002a, Kwok and Lui 2002b]. Moreover, license management process is also needed in managing license terms and documents [DRM 2005, InterTrust 2000, Kwok and Lui 2002a, Kwok and Lui 2002b].

In the DRM model for Web applications [Kwok, et al. 2003], it involves six parties; namely a creator (the owner of the digital product), a buyer (the one who purchases the digital product), a content distributor (the one who promotes and sells the product), clearance house (a trusted third parties for creator, distributor, and buyer), a DRM technology provider (a third party who masters the DRM technology for rights insertion and verification), and a portal (the one who provides and manages a marketplace for online business). These six parties are also referred in our DRM framework.

2.1.1 Rights Insertion

Rights insertion is a process to assign business rules and conditions, together with IDs of concerned parties to the media file. The concerned parties in online media business include media creators, owners, distributors, and consumers. Technologies for embedding ID information consist of digital certification (usually for any individual's ID) and digital watermarking (for company's ID). The rights insertion usually takes place at the media company and the distribution site.

Owner/creator's ID is inserted to the media file using both digital certification and digital watermarking at the media company. Business rules and conditions are laid down on a license document at the media company, or the distribution site or both. To meet new circumstances, opportunities and challenges, additional rules for the use of the media file may be needed for value chain partner, so that the distributor may insert other rights to the media. For example, consumer information including user's certificate or user's keys may be added to the license document to certify that he/she is the legitimate buyer of the media. A digital media file with an associated license document is known as a *rights-protected media*.

2.1.2 Rights Enforcement

There are two types of rights enforcement, namely active enforcement and passive enforcement [Kwok 2002]. In normal situation, DRM systems perform active rights enforcement whenever the media file is being played. This enforcement can be a built-in function in the media player; for example Windows Media Rights Manager by Microsoft [DRM 2005] conducts active enforcement within Media Player. After the media file or the license document is corrupted by intentional or un-intentional attacks, active enforcement may fail to verify and follow business rules and conditions associated with the media file. The DRM system will not notice this until passive enforcement is performed. Passive enforcement is an offline ownership verification process. The passive enforcement process takes place when a suspicious media file is found and it usually checks the hidden owner IDs. These hidden IDs cannot be easily detected and modified by attackers, and therefore they are needed when passive enforcement is included in the DRM solution.

2.1.3 License Management and Payment

After a license document has been created, a license management is required for managing license and payment effectively. The license management refers to issuing, hosting, and verifying license. There are basically two license

management models – tethered [CSRA 2005, DRM 2005, ISIS 2001] and un-tethered [InterTrust 2000] models used in commercial DRM systems. In the tethered model, consumers must be online to purchase digital music. License distribution and management are achieved by a license services center where centralized license storage and centralized security are used. In the untethered model, consumers store licenses on their own computers and are able to make purchases offline with a local DRM services center; payment is made at a later date. The untethered model is designed to promote music super-distribution models [Cox 1996]. Different payment model uses different license management models; for instance online payment uses the tethered model, while offline payment employs the un-tethered model. Existing commercial DRM systems support either the tethered model or the un-tethered model, but not both [Anonymous 2000].

An application of license management is media sharing; when a user shares a purchased media with another user, license creation, modification, and transfers are required in providing this sharing feature.

2.2 DRM Standards

There are several DRM standards available for electronic commerce. They include Secure Digital Music Initiative (SDMI), Microsoft Windows Media Rights Manager, open mobile alliance (OMA), and MPEG-4 DRM. However, many of these standards are still under development.

SDMI [SDMI 2005a, SDMI 2005b] is a multi-industry forum to develop a voluntary open framework for playing, storing and distributing digital music to enable a new market to emerge. It is composed of more than 200 companies and organizations representing information technology, consumer electronics, telecommunication, security technology, the worldwide recording industry, and Internet service providers. SDMI is primarily designed for music distribution over the Internet.

The Microsoft Windows Media Rights Manager [Pruneda 2005] in Windows Media Technology [Windows 2005] is an end-to-end digital rights management (DRM) system that offers content providers and retailers a flexible platform for the secure distribution of digital media files. Music creators or distributors can deliver music via the Internet in a protected format. Window media uses the strongest DRM encryption schemes, which would take days of supercomputer time to decode. In addition, the PC-by-PC licensing scheme acts as a strong deterrent to piracy. Windows Media Rights Manager packages the digital music. The packaged music file has been encrypted and locked with a ”key”. This key is stored in an encrypted license, which is distributed separately. Other information is added to the media file, such as information from the music distributor. The protected digital music and video are saved in Windows Media Audio format (.wma extension) and Windows Media Video format (.wmv extension).

OMA [OMA 2005] provides the currently and potentially most popular DRM standard in the mobile platform. Its sponsoring companies include IBM, Microsoft, and Vodafone, and its member companies include AOL, AT&T, LG etc. The DRM standard of OMA (OMA-SRM-v1.0) is partially supported by a few handsets such as Nokia 3100 (supports forward lock), and is supported more fully by newer handsets, for example, the serias60 from most company.

MPEG-4 [MPEG 2005] is a new audio and video standard, developed by the Moving Pictures Expert Group. ISMA (Internet Streaming Media Alliance) [Naraine 2005] is planning to standardize MPEG-4 DRM specifications as soon as possible. MPEG views that lack of standardized DRM in MPEG-4 is the final obstacle in wide-spread use of MPEG-4 in commercial applications such as video-on-demand over TCP/IP networks. Hollywood studios have shown great interests in adopting the MPEG-4 DRM specifications.

2.3 Web Services model and related technologies

The term “Web Services”, describes specific functionality, value delivered via Internet protocols, for the purpose of providing a mechanism for another service or application to use [Bosworth 2001]. The concept of WS model can be based on a new service-oriented architecture (SOA) in building better software applications [Burbeck 2005]. Services must be based on shared organizing principles that constitute a SOA. The term, service-oriented architecture focuses on how services are described and organized to support their dynamic, automated discovery and use. Service provider, service requester, and service registry are the three roles in SOA. These roles are related by means of the key requirements of “service description”, “service publication” and “service binding and invocation”. To facilitate information exchange between roles, these requirements support publish, find, and bind. The roles and interactions in SOA are shown in Figure 1.

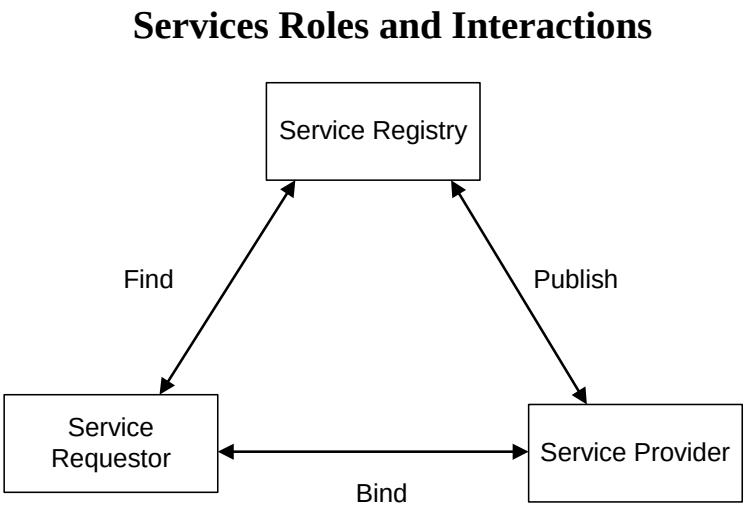

Figure 1: The roles and interactions in SOA.

The most widely used standards for "service description", "service publication" and "service binding and invocation" in a distributed service-oriented environment are WSDL (Web service Description Language) [Christensen, et al. 2005], UDDI (Universal Description, Discovery, Integration) [UDDI 2005], and SOAP (Simple Object Access Protocol) [Box, et al. 2005]. Readers may refer to [Tsalgatidou and Pilioura 2002] for various approaches and standards.

3 A Generic DRM Framework using Web Services

The proposed generic DRM framework is partially referenced to the NTT DoCoMo i-mode infrastructure [I-mode 2005], the mobile DRM model [Kwok 2002], and the DRM infrastructure with Web services [Kwok, et al. 2003]. Incorporating with the i-mode infrastructure can ensure the proposed framework can support ordinary 2.5G WAP or i-mode mobile devices with limited physical resolution in their display and limited storage memory. The mobile DRM model offers the DRM functionalities over mobile networks. The DRM infrastructure with Web services provides insights to the use of Web services for DRM operations. The proposed framework uses the enhanced license management model [Kwok and Lui 2002a, Kwok and Lui 2002b]. It is novel in the sense that its DRM model employs a commonly trusted party, i.e., a clearance house to handle DRM operations and interact with WS.

The objectives of the framework are to support DRM, including rights operations and payment in the mobile environment for mobile media distribution applications and services, while the constraints of mobile technologies are overcome by using WS – SOA. Besides, the framework enables other DRM-related activities; such as media sharing between mobile users using license management.

The center of the framework is a clearance house (or a service center) that controls and manages all DRM issues and DRM-related operations. From the DRM perspective, all key parties, namely the creator, buyer, distributor, and DRM technology provider trust the clearance center. The trust requirement is very important, specifically for DRM applications in electronic commerce [Cheung, et al. 2002]. This requirement practically holds in the i-mode network infrastructure [I-mode 2005] that bridges the mobile users and information providers through the i-mode service center. This is why the i-mode infrastructure is adopted in the proposed framework. Another underlying DRM model contributing to our proposed framework is due to Kwok [Kwok 2002], which also manages DRM operations through a center service but the trust between service center and other information providers (IP), such as creator, distributor etc. does not necessarily exist in that model. Moreover, Kwok's DRM model does not work with SOA as shown in Figure 2.

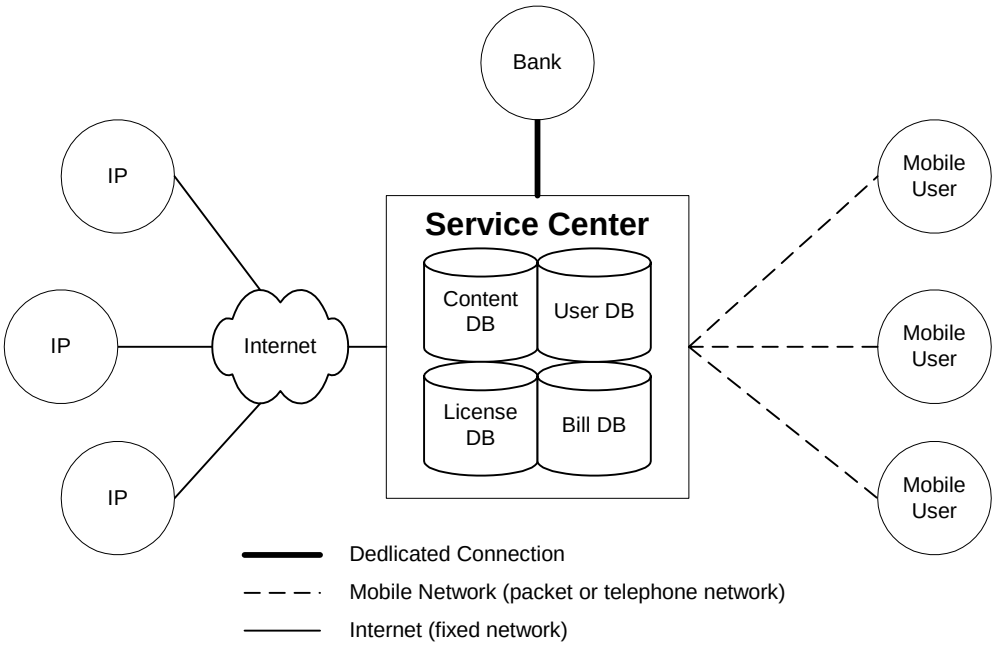

Figure 2: The DRM model in mobile environment.

The proposed generic DRM framework with the support of WS for M-commerce is presented in Figure 3. In the proposed framework, the clearance house can be regarded as a value-added service center. The IPs could be of any service providers that offer media distribution services [I-mode 2005, Kwok 2002]. To simplify the framework, only key DRM-related entities are shown in Figure 3.

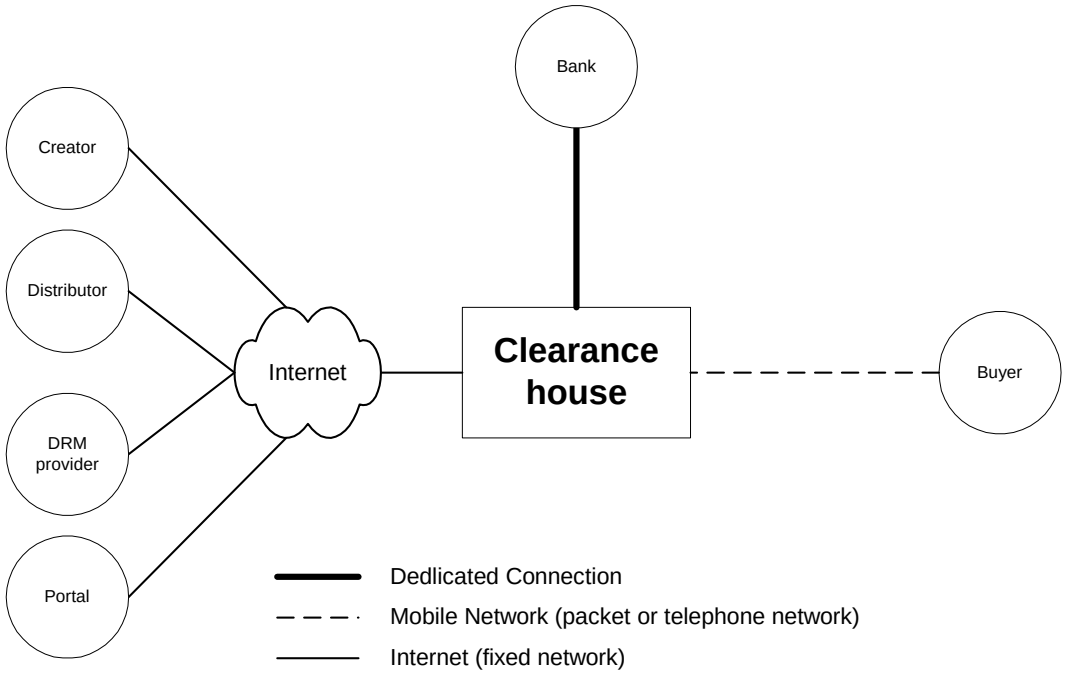

Figure 3: The proposed generic DRM framework.

To support DRM with WS, the clearance house plays the role of service requestor on behalf of the buyer in the context of SOA. An additional entity, service directory is required to participate in Web services applications. Based on the DRM infrastructure with Web services [Kwok, et al. 2003], the DRM technology provider is the party to provide the state-of-the-art DRM technology for rights insertion and verification, and therefore SOA takes place in connection with these three parties as shown in Figure 4.

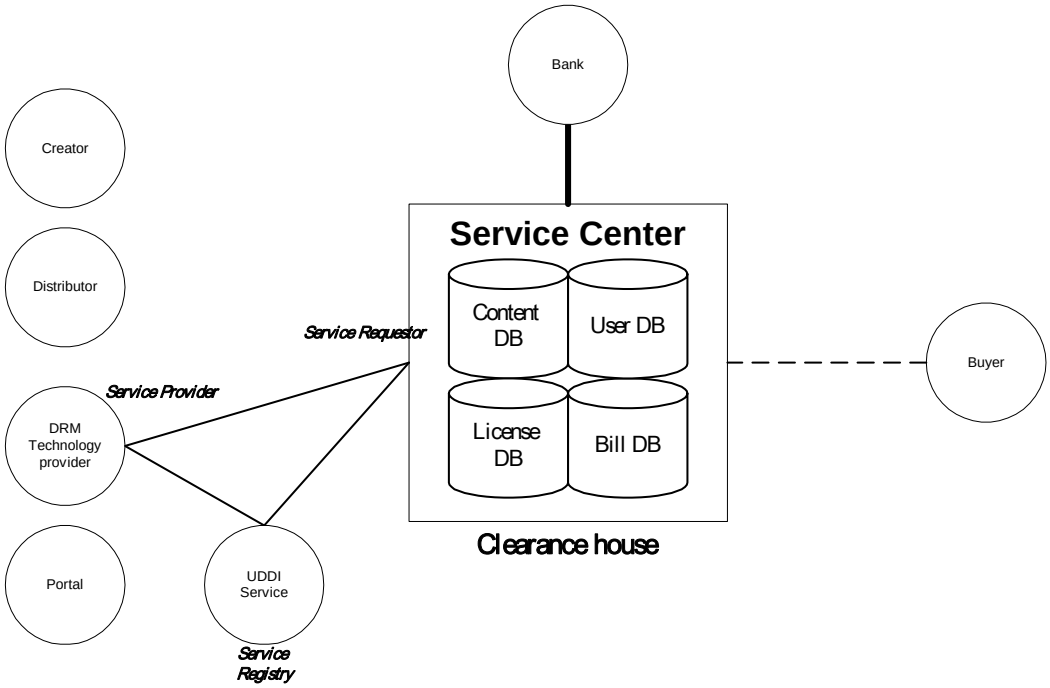

Figure 4: The proposed DRM framework with the support of Web Services.

Based on the DRM infrastructure with Web services [Kwok, et al. 2003], it contains a *creator*, a *buyer*, a *distributor*, a *portal*, a *DRM technology provider*, and a *clearance house*. In addition to these, the proposed framework includes two more parties, namely *bank* and *service registry*. The communication channels between different parties and the clearance house are different from each other depending on the required security level. For example, a dedicated network is used between the bank and the clearance house, since highly confidential information is transferred through this channel, whilst the clearance house relies on the packet network for content delivery.

3.1 Principal Components

In the proposed framework, the principal components include (1) a mobile network infrastructure, (2) a payment system, and (3) databases.

3.1.1 Mobile Network Infrastructure

The mobile network infrastructure is based on the NTT DoCoMo i-mode [I-mode 2005]. It provides a network architecture that connects all involved parties to the service center (or clearance house), which is the mobile operator – NTT in this case. The service center, being the only gateway for information delivery to mobile users, can provide value-added applications and services on top of the regular services offered by IPs. Value-added applications and services include billing service, a payment scheme, DRM service and so on. Network capacity, bandwidth, throughputs, and error tolerance differ with different telecommunication companies and communication networks. The proposed generic DRM framework could also take advantages of these services and enhance the applications and services. A 3G networking system could greatly improve many different aspects of the performance of the mobile network. Mobile multimedia, virtual reality and other high-bandwidth services could become possible.

3.1.2 Payment

Payment is an un-detachable component of M-Commerce. The payment part of the generic DRM framework employs the DoCoMo i-mode [I-mode 2005] and eCyberPay [eCyberPay 2002, eCyberPay 2003] approaches. The concept of these approaches is to centralize the payment process within the service center and IPs, and to require no confidential information from the consumer during transaction and payment. The concerned IPs receive payments

from the service center, and the service center will bill the mobile consumers together with their monthly service charges at the end of the month. The major benefit of this payment method is that consumers do not need to provide any confidential personal information to the merchant through the mobile network. Instead, a highly secure payment channel – a dedicated network - is used in the payment process.

3.1.3 Databases

Within the service center, there are a number of databases – content database, license database, bill database, and user database. The bill database and user database come with the i-mode model, while Kwok [Kwok 2002] proposed to include a content database and a license database to support mobile multimedia applications. These databases hold necessary information for various processing and operations such as transaction, payment, and DRM. The content database contains all the downloadable content provided by the distributors. The downloadable files are transferred to and held in the content database before purchasing and transactions. When a buyer or mobile user requests for a digital file, the requested media will be retrieved from the content database and delivered to the user. The license database holds license documents for all mobile users. Each license document states the owners of the content – creator, buyer, borrower, together with terms and conditions for use. The billing database keeps records of all transactions, including information about the seller and buyer, together with the transaction date, and charges. The user database is a database about all registered mobile users – their personal and payment information. A mobile user must register with the mobile operator before accessing the mobile network and experiencing mobile services. Hence, each mobile user has a record in the user database.

3.2 DRM System

In this section, we first explain how a digital ID (either digital certificate or watermark) can be embedded into a digital media with WS, then describe basic DRM operations, and finally illustrate how media sharing is realized in the proposed generic DRM framework. Throughout this section, a media distribution application will be used as example.

3.2.1 ID Insertion/Extraction Process with Web Services

Inserting/extracting ID(s) into/from a media requires technologies from external technology providers. As the proposed framework incorporates with Web services, we advocate to adopt the approach proposed by Kwok et al. [Kwok, et al. 2003] for mobile applications. However, the rationales behind the process are different from [Kwok, et al. 2003], including, (1) our approach has the flexibility to insert/extract one ID, or all IDs into/from the media at a time, (2) user requirements are taken into account in choosing DRM technology providers, and (3) our approach supports both watermark and certificate. Figure 5 shows a SOA to facilitate ID insertion/extraction. The clearance house initiates the process. The clearance begins with a search of potential DRM technology providers who can meet the user requirements. Specific user requirements include (1) whether the buyer and/or other parties prefer any specific technology provider(s), any specific DRM technologies. The clearance house may also impose other requirements, such as the type of the ID(s), the payment arrangement and so on.

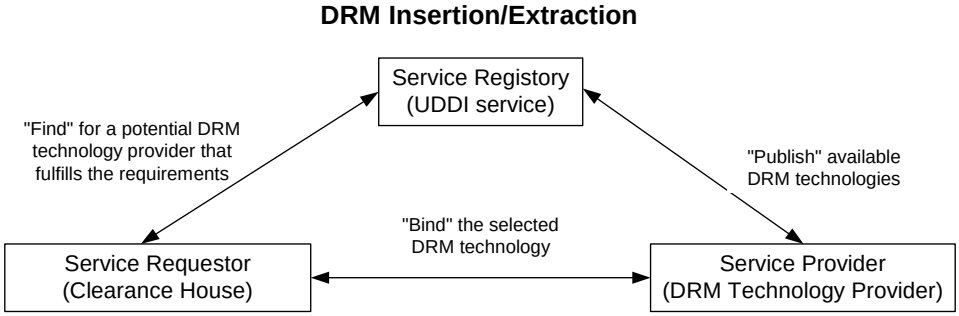

Figure 5: Interactions between the clearance house and the DRM technology provider in the process of embedding/extracting an ID into/from the media.

3.2.2 Rights insertion

The rights insertion phase outlined in Figure 6 includes three stages; (1) preparation; (2) searching and ordering; and (3) rendering. The goal of this phase is to generate a rights-protected media, $M_{wb+wc+wd}$ that contains all concerned parties' IDs, where *wb* refers to the buyer's ID, *wc* refers to the creator's ID, and *wd* refers to the distributor's ID.

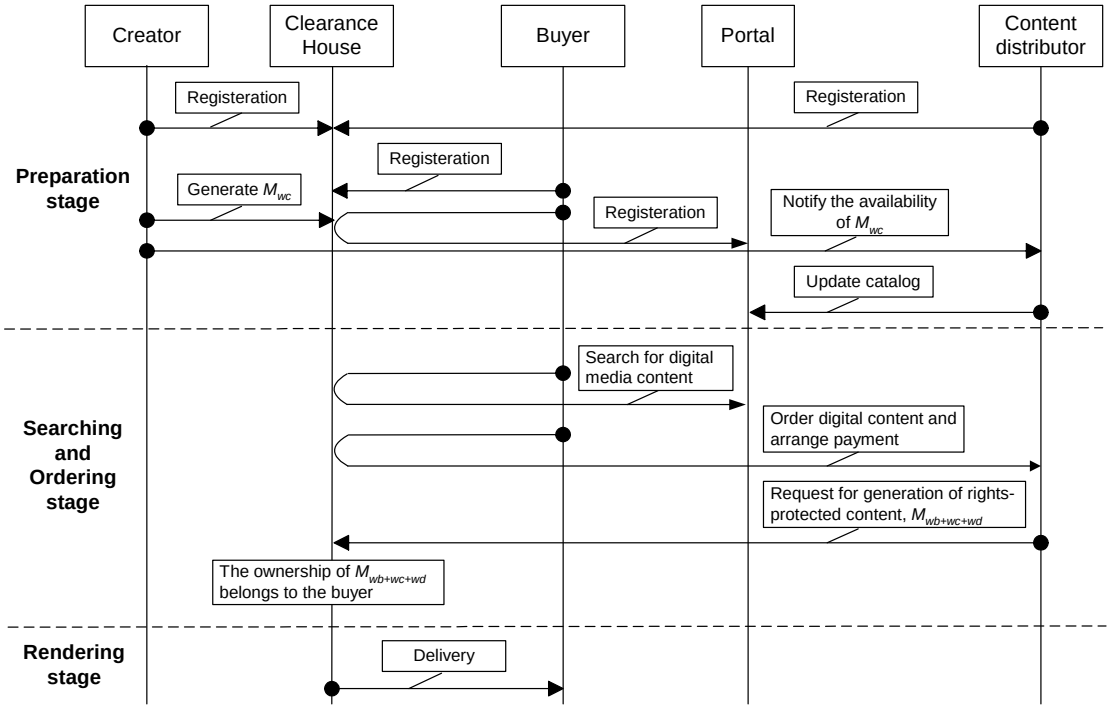

Figure 6: Basic operations of the generic DRM framework.

The preparation stage consists of the following steps.

Step P1: All creator, distributor, and buyer first register with the clearance house by passing their IDs to the clearance house. And the clearance house will either (a) collect ID from the parties in the format of digital certificate or digital watermark, or (b) generate certificates or watermarks as IDs for them. The IDs together with other profile information are kept in the user DB. In addition, the clearance house will issue a *record number* to the distributor, and open an account for the buyer with a unique account number.

Step P2: After the creator has created a digital media, the original media, M is transferred to the clearance house for ID insertion. The clearance house ensures all media contents carry their creator's ID, denoted as *wc*. This is achieved by invoking the *ID insertion process with Web services* to embed the corresponding creator's ID into the content using watermarking technique before storing it in the content DB. The media with the creator's ID is denoted as M_{wc}. On successfully generating M_{wc}, the creator can notify potential distributor the availability of the digital media.

Step P3: The distributor registers with the portal and then uploads a catalog to the portal, so that the buyer can access the product information from the portal.

The searching and ordering stage will take action when the preparation stage is complete. The following outlines the interactions between various involved parties in purchasing a rights-protected media in the proposed framework.

Step O1: A buyer browses the catalog at the portal with her mobile device – a mobile phone.

Step O2: When the buyer decides to subscribe or purchase a particular media content, the buyer will inform the portal. And the portal will forward the order to the designated distributor.

Step O3: The distributor formally notifies the clearance house about the order by providing the distributor's record number and the buyer's phone number. The clearance house will then verify the information. A way to verify the information is to crosscheck the connection ID between these two parties.

Step O4: The clearance house then updates the buyer's monthly bill with the charge of the purchased media. A money-transfer process is activated to transfer money from the clearance house's bank account to the distributor's bank account based on the payment method set by i-mode [I-mode 2005].

Step O5: The clearance house retrieves the selected digital media from the content database and inserts the buyer's ID, denoted as *wb* and the distributor's ID, denoted as *wd* into the digital media. The *ID insertion process* with Web services takes place. The media becomes a rights-protected media,

$M_{wb+wc+wd}$ and the rights-protected media is kept in the content DB. This is also considered to be a major rights insertion operation. A specific license is generated and kept in the license database. The license contains the media usage agreement and other terms.

The rendering stage is composed of the following step.

Step R1: The rights-protected media is delivered to the buyer via the packet network or the conventional mobile channel. This step can be executed immediately after the purchase and whenever the buyer requests it.

Since the buyer is always attached to the clearance house (also known as service center or mobile operator in other cases), messages from the buyer must go through the clearance house before reaching other external parties. This facilitates the clearance house to keep track of the ordering process, and know when to take part in the process. Therefore buyers do not need to notify the clearance house to act on their behalf explicitly. This increases the user-friendliness of the framework (in contrast with [Kwok 2002]).

In the above steps, the rights insertion operation takes place at steps P2 and O5 using the ID insertion process with Web service. It embeds buyer's ID, creator's ID, and distributors' ID in the rights-protected media $M_{wb+wc+wd}$. The framework provides the flexibility to insert IDs at various steps. For example, creator's ID can also be embedded into step O5.

3.2.3 Rights enforcement

When a buyer wants to listen to his previously purchased media, the buyer can make a request to the clearance house directly through her mobile device. Built-in software in the mobile device can facilitate this. The clearance house will first verify the buyer's ID and the license terms. In verifying an ID, the clearance house does not need to rely on any DRM technology provider as the clearance house can identify any buyer based on her account number (usually telephone number). If the buyer has the rights to play to the media, the clearance house will execute it at step R1 and alter the license terms when a pay-per-view payment scheme is in use. This is regarded as an active rights enforcement operation. The active rights enforcement operation is transparent to the buyer, as the operation takes place at the clearance house.

The passive enforcement process takes place when a suspicious media file is found and it is to verify the hidden owner IDs. The process is conducted by external parties and organizations, other than the clearance house. However, the clearance house assists the process by providing buyer information, license information, and information of the DRM technology provider. The ID extraction process as shown in Figure 7 is executed offline by the same DRM technology provider who inserted ID(s) into the media. In Hong Kong, Customs and Excise officers administer the intellectual property law and are responsible for performing passive rights enforcement operations against any suspected copyright violation. The passive rights enforcement basically compares the embedded digital IDs in the rights-protected media and the rights information kept in the digital license stored in the license database at the clearance house.

Media Sharing

Consider the case where Buyer A wants to share her purchased digital media with her friend Buyer B, with or without charge. The procedure to share rights-protected digital media from one buyer to another is given below.

Step S1: User A informs the clearance house about her decision to loan her purchased digital media content to another registered buyer – Buyer B.

Step S2: The clearance house extracts the corresponding license from the license database and verifies its terms and agreements. The license terms must state that the purchased media is sharable or transferable before proceeding to the next step.

Step S3: If Buyer A wants to charge Buyer B for the usage, the clearance house may bill Buyer B according to the instructions from Buyer A and the agreement from Buyer B. Otherwise, this will be skipped.

Step S4: The clearance house generates a "borrow" license for Buyer B to enable Buyer B to render the media content. The "borrow" license enables Buyer B to render the media, but it may or may not be shareable with the third party, subject to the agreement specified by User A. The license for User A could be frozen if the original license prohibits concurrent use while Buyer B has the rights to render the media. The rights-protected media will remain unchanged in a "borrow" case, while the rights-protected media will be altered with Buyer B's ID in a "transfer" case.

Step S5: Buyer B can access and render the digital media, just like Buyer A before.

It is noted that Buyer B will not participate in the media sharing process if payment is not required. However, if Buyer B purchases the media from Buyer A, Buyer A must instruct the clearance house to transfer the ownership of her purchased digital media to Buyer B. It is up to the agreement between Buyer A and B how the payment is made. It could also be done with the clearance house if a prior arrangement is made with the clearance house between Buyer A, Buyer B, and the clearance house.

4 Evaluation by Comparisons

In this section, we compare the proposed generic DRM framework (denoted as M1) with the DRM with WS [Kwok, et al. 2003] (denoted as M2), and the general DRM framework [Kwok 2002] (denoted as M3) in terms of their practicability, capabilities, and limitations for mobile applications.

Table 1: The practicability of various DRM solutions for M-commerce.

Constraints	M1	M2	M3
Privacy and Trust	✓ (good)	✓ (good)	×
Coordination and interoperability	✓ (good)	✓ (good)	×
Security (payment)	✓ (good)	✓	✓ (good)
License management	✓ (good)	✓ (good)	✓ (good)
DRM operations	✓ (best)	✓ (good)	✓
Payment	✓ (best)	✓	✓ (good)
Mobile limitations			
Restricted BW	✓	×	×
Temporary unavailability	✓	×	×
Low CPU and memory capacities	✓	×	×

Table 1 compares the practicability of various DRM solutions for M-commerce services. It is noted that the proposed DRM framework can overcome all constraints caused by the mobile infrastructure, network, and device.

4.1 Benefits and Problems

In terms of capability, the proposed framework has all benefits of M2 and M3 because the proposed framework is to a certain extent derived from them. Moreover, with the adoption of WS in mobile domain, the property of *coordination and interoperability* further enhances the framework in terms of *extensibility* and *flexibility*. In terms of limitations, all three have similar problems. But the proposed framework introduces the problems of overloading and risk.

Coordination and Interoperability: Coordination and interoperability play an important role in mobile services that support DRM operations. The DRM model involves many parties, and they are required to interact with others to perform ID insertion and verification, and other tasks. The communications between parties are through message exchange. WS offers a standard protocol and message format for communication. This could attract service providers and other parties to be involved in the media distribution business.

Extensibility: With the support of WS, un-official and/or unregistered DRM technology providers can participate in the bidding process. The SOA offers a fair competition for all DRM providers to offer services to any clearance house (also known as mobile operator). Cross-network services among clearance houses are also supported. In this case, the rights-protected media contents may be transferred from one clearance house to another clearance house (the process is similar to the above sharing example from Buyer A to Buyer B). However, before the transfer begins, the hosting clearance house must have an approval from the corresponding creator. If the creator does not trust the second clearance house, the transfer cannot and should not proceed. This is to protect the interests of the owner of the media – the creator.

Flexibility in DRM operation: The clearance house is in charge of all DRM operations. It has the flexibility to choose a DRM technology provider based on certain requirements, such as buyer's, distributor's and clearance house's requirements and preferences. It can even download the DRM objects from the chosen DRM technology provider and execute ID insertion/extraction within the site, which is different from M2 and M3 that trust external DRM providers to prepare the rights-protected media.

Flexibility in ID representation: The framework supports various ID representation, including both digital certificate and watermark. The DRM framework is independent of the ID representation.

Overloading: There is only one commonly trusted party – clearance house in the proposed framework. This can ensure privacy and trust. However, the burden of the clearance house could be very high. A very high computation power is required at the clearance house to handle all kinds of processes – DRM, registration, account management, etc. A large amount of memory requirement is also needed to hold data and information, in particular media contents. Each media may require three copies of it, namely M, M_{wc}, and $M_{wb+wc+wd}$.

Risk: The clearance house constitutes a single point of failure, which exposes the whole network to attacks. A successful break-in by attackers to the clearance house could lead to a disaster to all involved parties. Even a short

power interruption at the clearance house may cause inconvenience and losses. The framework could cause serious problems when the clearance house is controlled by an untrustworthy, insecure or abusive monopoly.

5 Conclusions

This paper presented a generic DRM framework for mobile media distribution services. The proposed framework overcomes constraints due to the mobile infrastructure, network, and device. The framework tackles several specific constraints including (1) coordination and interoperability; (2) security; (3) privacy and trust; (4) payment; (5) DRM operations; and (6) license management. The proposed framework was derived from several known DRM and WS solutions. The core of the framework is a centralized mobile infrastructure that is derived from the NTT DoCoMo i-mode service to manage daily operations and deal with the problems of privacy and trust, and payment. The center of the centralized infrastructure is a commonly trusted third party - a clearance house that bridges all involved parties, such as buyers, service providers, DRM technology providers and so on. The design of the framework takes advantages of WS to tackle the problems coordination and interoperability among multiple independent entities. The use of WS also indirectly improves the extensibility and flexibility of the framework. A mobile DRM model is integrated into the framework in order to respond to the problems of DRM operations and license management.

The proposed framework was found to be useful and practical. It was compared with other similar DRM solutions and the proposed framework outperforms others and is proven to be capable for media distribution in mobile environment. However, this paper also highlighted potential problems of the proposed framework. The problems are mainly due to the centralized approach. The central clearance house could easily be overloaded by users and therefore the requirements of both memory and processing power could be very high. Moreover, it could be costly when the clearance house is in any problems, such as system breakdown, attacks, and so on. All users and businesses will be affected and it can lead to great financial losses.

REFERENCES

Anderson, L. C. and J. B. Lotspiech, "Rights management and security in the electronic library," *Bulletin of the American Society for Information Science*, Vol. 22, pp. 21-23, 1995.

Anonymous, "The Major Players, Partners in Digital Rights Management," *Billboard*, Vol. 112, pp. 103, 2000.

Beneventano, D., F. Guerra, S. Magnani, and M. Vincini, "A Web Service Based Framework for the Semantic Mapping Amongst Product Classification Schemas," *Journal of Electronic Commerce Research*, Vol. 5, pp. 114-127, 2004.

Bosworth, A., "Developing Web Services," Proceedings of the International Conference on Data Engineering, 2001.

Box, D., D. Ehnebuske, G. Kakivaya, A. Layman, N. Mendelsohn, H. F. Nielsen, S. Thatte, and D. Winer, Simple Object Access Protocol (SOAP) 1.1, http://www.w3.org/TR/SOAP/, accessed on 11 April 2005.

Brown, J., The Gnutella paradox, http://dir.salon.com/tech/feature/2000/09/29/gnutella_paradox/index.html, accessed on 11 April 2005.

Burbeck, S., The Tao of e-business services, http://www-106.ibm.com/developerworks/library/ws-tao/, accessed on 11 April 2005.

Cheung, S. C., H. Curreem, and D. K. W. Chiu, "A Watermarking Infrastructure for Digital Rights Protection," Proceedings of the 4th International Conference on Electronic Commerce (ICEC 2002), Hong Kong, 2002.

Christensen, E., F. Curbera, G. Meredith, and S. Weerawarana, Web Services Description Language (WSDL), http://www.w3.org/TR/wsdl, accessed on 11 April 2005.

Cox, B., *Superdistribution: Objects as Property on the Electronic Frontier*: Addison Wesley Publishing Company, 1996.

CSRA, Computer Science Research at Almaden - Madison - Music on the Web, http://www.almaden.ibm.com/cs/madison.html, accessed on 11 April 2005.

DRM, Digital Rights Management, http://www.microsoft.com/windows/windowsmedia/drm.aspx, accessed on 11 April 2005.

eCyberPay, eCyberPay.com, http://www.ecyberpay.com, accessed on 1 January 2002.

eCyberPay, eCyberPay, http://www.c-music.com.hk/ecyberpay.htm, accessed on 26 January 2003.

I-mode, i-mode Global, http://i-mode.nttdocomo.com, accessed on 11 April 2005.

InterTrust, "InterTrust, The MetaTrust Utility, Announces OpenRights Initiative," Intertrust Press Release 2000.

ISIS, Intel Software Integrity System, http://developer.intel.com/software/security/backgrounder.htm#ISIS, accessed on 1 January 2001.

Kwok, S. H., "An Enhanced License Management Model in Digital Rights Management for Online Music Business," International Conference on Information Society in the 21 Century: Emerging Technologies and New Challenges (IS 2000), 2000.

Kwok, S. H., "Chapter 5: Digital Rights Management for Mobile Multimedia," in *Mobile Commerce: Current States and Future Trends*, E. P. Lim, Z. Shen, and K. Siau, Eds.: Idea Group Publishing, 2002, pp. 97-111.

Kwok, S. H., "Watermark-Based Copyright Protection System Security," *Communications of the ACM (CACM)*, Vol. 46, pp. 98-101, 2003.

Kwok, S. H. and S. M. Lui, "A License Management Model for Peer-to-Peer Music Sharing," *Special Issue on Virtual Organizations and E-Commerce Applications in the International Journal of Information Technology and Decision Making (IJITDM)*, Vol. 1, pp. 541-558, 2002a.

Kwok, S. H. and S. M. Lui, "A License Management Model for Peer-to-Peer Music Sharing," *Special Issue on Virtual Organizations and E-Commerce Applications in the Journal of Applied Systems Studies (JASS)*, Vol. 3, 2002b.

Kwok, S. H., S. M. Lui, S. C. Cheung, and K. Y. Tam, "Digital Rights Management with Web Services," *Electronic Markets*, Vol. 13, 2003.

Kwok, S. H., C. C. Yang, and K. Y. Tam, "Intellectual Property Protection for Electronic Commerce Applications," *Journal of Electronic Commerce Research*, Vol. 5, pp. 1-13, 2004.

Memon, N. and P. W. Wong, "A buyer-seller watermarking protocol," *IEEE Transactions of Image Processing*, Vol. 10, pp. 643-649, 2001.

Mohan, C., "Dynamic E-business: Trends in Web Services," Third VLDB workshop on Technologies for E-Services, Hong Kong, 2002.

MPEG, MPEG Pointers and Resources, http://www.mpeg.org, accessed on 11 April 2005.

Napster, Napster, http://www.napster.com, accessed on 11 April 2005.

Naraine, R., ISMA Pushes DRM for MPEG-4, http://www.internetnews.com/dev-news/article.php/2173041, accessed on 11 April 2005.

OMA, Open Mobile Alliance, http://www.openmobilealliance.org, accessed on 11 April 2005.

Piloura, T., A. Tsalgatidou, and S. Hadjiefthymiades, "Scenarios of using Web Services in M-Commerce," *ACM SIGecom Exchanges*, Vol. 3, pp. 28-36, 2003.

Pruneda, A., Introduction to MS Windows Media Rights Manager, http://www.microsoft.com/technet/treeview/default.asp?url=/technet/prodtechnol/netshow/maintain/wmrtsmgr.asp, accessed on 11 April 2005.

Ramanujapuram, A. and P. Ram, "Digital Content & Intellectual Property Rights," *Dr. Dobb's Journal*, Vol. 23, pp. 20-27, 1998.

Rotchanakitumnuai, S. and M. Speece, "Corporate Customer Perspectives on business Value of Thai Internet Banking," *Journal of Electronic Commerce Research*, Vol. 5, pp. 270-286, 2004.

SDMI, SDMI Home, http://www.sdmi.org, accessed on 11 April 2005.

SDMI, SDMI Portable Device Specification Part 1, Version 1.0, http://www.sdmi.org/download/port_device_spec_part1.pdf, accessed on 11 April 2005.

Stewart, T., *Designing Systems for Internet Commerce*: Addison Wesley, 1998.

Tsalgatidou, A. and T. Pilioura, "An Overview of Standards and Related Technology in Web Services," *Distributed & Parallel Databases*, Vol. 12, pp. 135-162, 2002.

UDDI, UDDI.org, http://www.uddi.org, accessed on 11 April 2005.

Vinoski, S., "Putting the "Web" into Web services. Web services interaction models, Part 2," in *IEEE Internet Computing*, vol. 6, 2002, pp. 90 -92.

Windows, Windows Media, http://www.microsoft.com/windows/windowsmedia/default.aspx, accessed on 11 April 2005.

Zhou, L., W.-y. K. Chiang, and D. Zhang, "Discovering Rules for Predicting Customers' Attitude Toward Internet Retailers," *Journal of Electronic Commerce Research*, Vol. 5, pp. 228-238, 2004.