A Web Service-based Digital Rights Management Framework for Mobile Media Distribution

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

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

Minder Chen
School of Management
George Mason University
MSN-5F4
4400 University Drive
Fairfax, VA 22030, USA
mchen@gmu.edu

Abstract

Performing digital rights management (DRM) on mobile media distribution (MMD) services encounters many technical problems. Major problems include privacy and trust, coordination and interoperability, security, license management, DRM operations, as well payment. This paper proposes a generic DRM framework using Web services (WS) to tackle these problems. The proposed framework consists of (1) an operational mobile infrastructure; (2) Web services; and (3) a mobile DRM model. This paper emphasizes on the use of WS for DRM because Web services are the most appropriate middleware technology for integrating media for mobile devices. The framework enables basic rights insertion and enforcement, as well as media sharing. It is independent of specific mobile technologies. The framework has been compared with other similar DRM solutions and the results show that it outperforms them in terms of practicability and capabilities.

1. Introduction

Media distribution services, including video conferencing, video-on-demand, online music distribution are emerging mobile services. Digital Rights Management (DRM) is required in media distribution services to protect the intellectual property of the distributed digital media. DRM technology includes rights insertion, rights enforcement, license management, license (or media) sharing and so on. Rights insertion and rights enforcement [14] are the basic DRM operations. License management is to manage the usage and access rights of the purchased media [7, 10, 11]. License (or media) sharing [1, 19] that involves processes of transferring rights and issuing authorization is a important new feature in media distribution services demanded by users. Payment systems [6, 8] are also related to DRM operations because media usage and access rights often require payments.

Mobile media distribution (MMD) services involve multiple independent business entities such as mobile operators, service providers, enabling technology providers, and mobile users. The success of MMD is dependent upon the mutual trust among these entities because media distributed are a form of intellectual property. Due to the limitations of mobile device namely slow CPU speed and small memory capacity [20], there are problems to overcome in order to perform DRM on MMD as discussed in the following:

- **Coordination and Interoperability** [15]: 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 MMD involving these parties needs to resolve the problems of coordination and interoperability among heterogeneous systems.
- **Security** [13, 17]: 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 clearing 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** [5]: Personal information including personal identities (IDs), keys and so on are held by different parties and required to be exchanged for DRM to work properly. Privacy becomes a great concern when trust does not exist in these involved parties.
- **Payment** [12]: A secured payment system is needed for MMD. 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** [12]: 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 third party. Besides, DRM technology provider is required in order to perform these DRM operations.

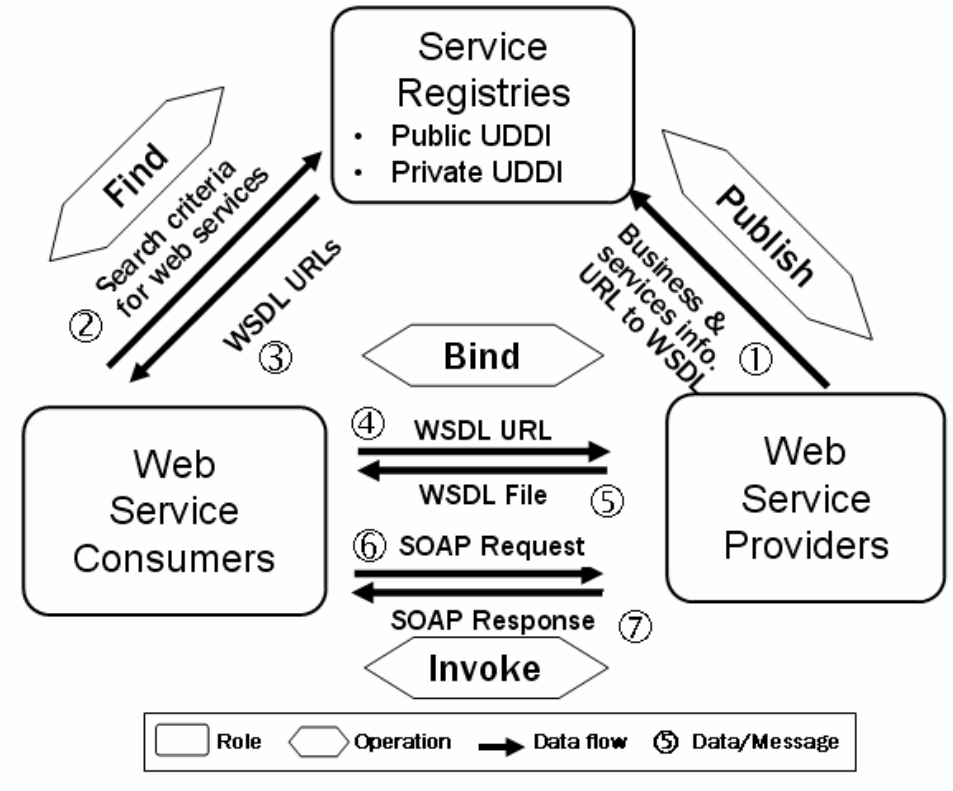

Figure 1: Service-oriented Web service architecture

- **License Management** [12]: License management models, such as tethered, un-tethered, and enhanced models [14] require 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 older generations of mobile devices are used because 2.5G and older mobile technologies are not capable of managing licenses.

Web Services (WS) is a strong candidate to tackle the problems of coordination and interoperability among multiple entities. The WS paradigm is a promising technology for developing component-based 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 WS over wireless networks [20]. Mohan [18] defines that WS are self-contained, self-describing, modular applications that can be published, located, and invoked across the Web. WS perform functions ranging from simple requests to complicated business processes. WS are agnostic regarding the choice of operating system, object model, and programming language; therefore, they become important enabling technology for building flexible and loosely coupled business systems, including mobile applications [22].

This paper proposes a generic DRM framework for MMD using WS to tackle all these problems. The paper is organized as follows. Section 2 covers the background of WS and relating technologies. In Section 3, we present the proposed DRM framework which provides rights insertion and rights verification functions. Section 4 compares various DRM solutions in terms of the practicability, capabilities, and limitations. Finally, we conclude the paper in Section 5.

2. Background

Web services provide a standard-based approach to implementing distributed software components. Via Web services, data and business logic services can be offered over standard Internet protocols to applications programs inside a firm or across enterprises.

2.1 Web Services model and related technologies

Web services are a set of standards to form a service-oriented architecture (SOA) [2], as depicted in Figure 1 [4]. This architecture models the interactions between three roles: the service provider, service consumer, and service registries [3]. The interactions involve service publishing, finding, and binding operations. Interfaces to a Web service implementation can be described by Web Services Description Language (WSDL). A Web service provider can publish a Web service defined by WSDL to a service registry such as UDDI (Universal Description, Discovery, and Integration). WSDL is an interface definition language specified in XML format for "describing network services as a set of endpoints operating on messages containing either document-oriented or procedure-

oriented information [23]." WSDL is similar to the Interface Definition Language (IDL) in CORBA. WSDL usually are generated automatically by Web services development tools.

A Web service requester (consumer) can search and find WSDL access points of appropriate Web services from a UDDI directory. It will then retrieve the WSDL file from the Web service publisher. The service consumer uses the service description to bind with the Web service by generating a client-side Web service proxy. Then, a programmer can use the Web service as if it is an imported class and invoke specific Web methods/operations of the Web service. Behind the scene, at run time, SOAP messages [24] will be sent via the Web service client proxy to the service provider to invoke these Web operations and optionally receives SOAP responses. By conforming to Web service standards, software components can be accessed by applications from customers and business partners independent of hardware, operating system, and programming language.

The Universal Description, Discovery and Integration (UDDI) depicted in the SOA architecture is a standard that enables companies and applications to easily and dynamically find and use Web services over the Internet or intranets [21]. There are public UDDI registries where Web services and other business services can be registered. There are few companies that are actually using UDDI dynamic services discovery and integration in real business applications. A browser-based interface to UDDI registry can be used to publish and search a Web service while programming interfaces, implemented as Web services, are available to automate these activities. Private UDDI registries are often created to support EAI efforts. We can also build industry specific UDDI registries to support vertical markets for Web services.

Using the ubiquitous and low-cost internet, web services can easily provide software functions over the internal networks and the public internet for mobile computing applications [16]. Mobile computing devices that are capable of consuming web services can use distributed components implemented as web services to get access to legacy data and applications [25]. This approach will enrich the functionality of mobile applications as well as increase the reusability of distributed software components. As a result, maintenance of business logic that is shared by both mobile and non-mobile applications

3. A Generic DRM Framework using Web Services

The proposed generic DRM framework is derived from NTT DoCoMo i-mode infrastructure [9], the mobile DRM model [12], and the DRM infrastructure with Web services [15]. The proposed framework also indirectly references to the mobile device-driven architecture [20], as the WS-based DRM infrastructure is inherited from the mobile device-driven architecture. 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 screens and limited storage memory. The mobile DRM model offers the DRM functionalities over mobile networks. The DRM infrastructure with Web services provides a mechanism to the use of Web services for DRM operations. The proposed framework uses the enhanced license management model [14] and the unique DRM model employs in the framework is a commonly trusted party that serves as a clearing house to handle DRM operations and interactions 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. Besides, the framework enables other DRM-related activities; such as media sharing between mobile users using a license management mechanism. The center of the framework is a clearing house (i.e., 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 clearing center. The trust requirement is very important, specifically for DRM applications in the context of electronic commerce [5]. This requirement is implemented in the i-mode network infrastructure through the i-mode service center that bridges the mobile users and information providers [9]. This is why the i-mode infrastructure is adapted in the proposed framework. Another underlying DRM model contributing to our proposed framework is due to Kwok [12], which also manages DRM operations through a service center 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.

The proposed generic DRM framework with the support of WS for MMD services is presented in Figure 3. The clearing house in the proposed framework can be regarded as a value-added service center. The IPs are any service providers that offer media distribution services [9, 12]. To simplify the framework, only key DRM-related entities are shown in Figure 3.

To support DRM with WS, the clearing house plays the role of service requestor on behalf of the buyer. An additional entity, service directory is required to participate in Web services applications. Based on the DRM infrastructure with Web services [15], 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.

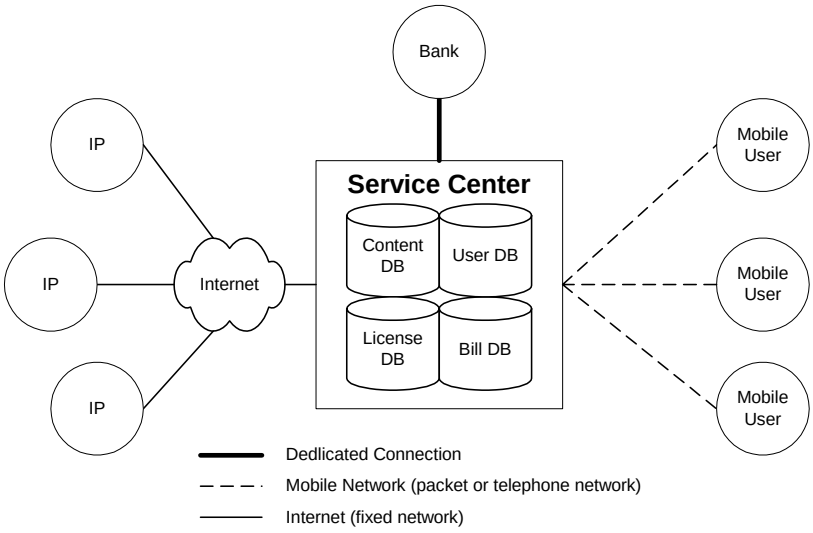

Figure 2: The DRM model in mobile environment.

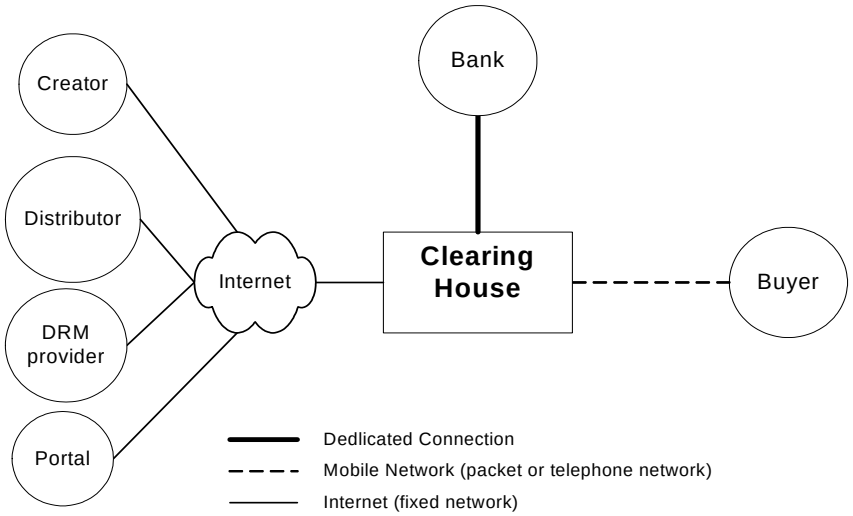

Figure 3: The proposed generic DRM framework.

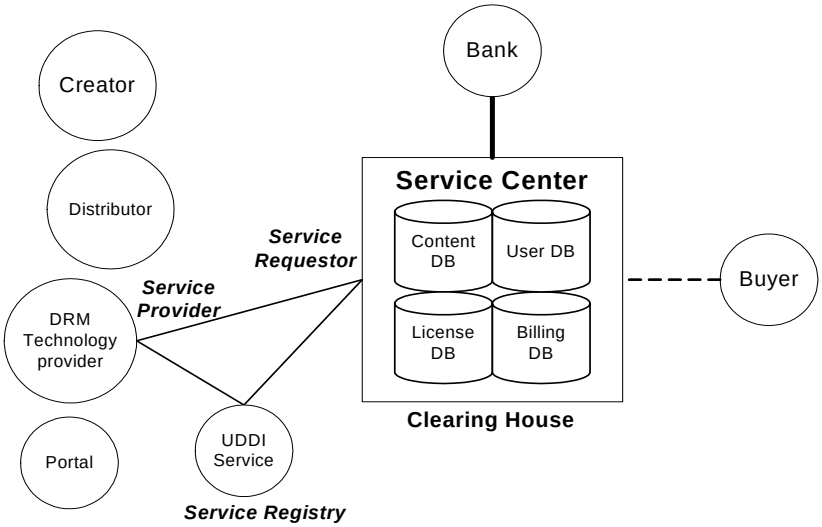

Figure 4: The proposed DRM framework with the support of Web Services.

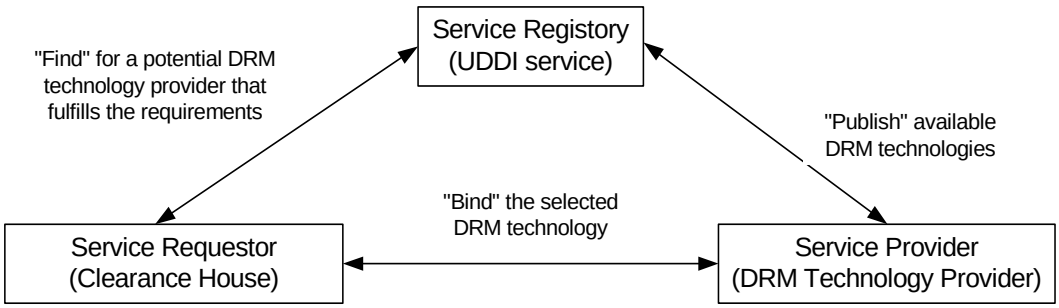

Figure 5: Interactions between the clearing house and the DRM technology provider in the process of embedding/extracting an ID into/from the media.

Based on the DRM infrastructure with Web services [15], it contains a *creator*, a *buyer*, a *distributor*, a *portal*, a *DRM technology provider*, and a *clearing 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 clearing house are different from each other depending on the required security level. For example, a dedicated network may be used between the bank and the clearing house, since highly confidential information is transferred through this channel, while the clearing house relies on the packet-switching 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. These components are discussed in detail in this subsection.

3.1.1 Mobile Network Infrastructure

The mobile network infrastructure is based on the NTT DoCoMo's i-mode [9]. It provides a network architecture that connects all involved parties to the service center which is the mobile operator (e.g., NTT in the case of i-mode). 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 System

Payment system is an critical component of MMD. The payment part of the generic DRM framework employs the DoCoMo i-mode [9] and eCyberPay [8] 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 at the backend.

3.1.3 Databases

Within the service center, there are a number of databases – content database, license database, billing database, and user database [12]. 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 stored in the content database. 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 contains data of all registered mobile users including their personal profiles and payment data. A mobile user must register with the mobile operator before accessing the mobile network's services.

3.2 DRM System

In this section, we first explain how a digital ID implemented as a digital certificate or a watermark can be embedded into a digital medium 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. [15] for mobile applications. However, the rationales behind the process are different from [15], 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-based approach to facilitating ID insertion/extraction. The clearing house initiates the process. The clearing 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) and any specific DRM technologies. The clearing house may also impose other requirements, such as the type of the ID(s), the payment arrangement and so on.

3.2.2 Rights insertion

The rights insertion phase 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.

Since the buyer is always attached to the clearing house (also known as service center or mobile operator in other cases), messages from the buyer must go through the clearing house before reaching other external parties. This facilitates the clearing 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 clearing house to act on their behalf explicitly. This increases the user-friendliness of the framework (in contrast with [12]). The rights insertion operation is implemented via with Web service. It embeds buyer's ID, creator's ID, and distributors' ID in the rights-protected media Mwb+wc+wd.

3.2.3 Rights enforcement

When a buyer wants to listen to his previously purchased media, the buyer can make a request to the clearing house directly through her mobile device. Built-in software in the mobile device can facilitate this. The clearing house will first verify the buyer's ID and the license terms. In verifying an ID, the clearing house does not need to rely on any DRM technology provider as the clearing 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 clearing 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 clearing 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 clearing house. However, the clearing house assists the process by providing buyer information, license information, and information of the DRM technology provider. The ID extraction process 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 clearing house.

3.2.4 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 clearing house about her decision to loan her purchased digital media content to another registered buyer – Buyer B.

Step S2: The clearing 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 clearing 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 clearing 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 clearing house to transfer the ownership of her purchased digital media to Buyer B. It

Table 1: The practicability of various DRM solutions for MMD

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	✓	×	×

is up to the agreement between Buyer A and B how the payment is made. It could also be done with the clearing house if a prior arrangement is made with the clearing house between Buyer A, Buyer B, and the clearing house.

4. Evaluation by Comparisons

In this section, we compare the proposed generic DRM framework (denoted as M1) with the DRM with WS [15] (denoted as M2), and the general DRM framework [12] (denoted as M3) in terms of their practicability, capabilities, and limitations for mobile applications.

Table 1 compares the practicability of various DRM solutions for MMD 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 the benefits of M2 and M3 because the proposed framework to a certain extent is 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, various DRM technology providers can participate in the bidding process. The SOA offers a fair competition for all DRM providers to offer services to any clearing house (also known as mobile operator). Cross-network services among clearing houses are also supported. In this case, the rights-protected media contents may be transferred from one clearing house to another clearing house (the process is similar to the above sharing example from Buyer A to Buyer B). However, before the transfer begins, the hosting clearing house must have an approval from the corresponding creator. If the creator does not trust the second clearing 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 clearing 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 clearing 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 representations, including both digital certificate and watermark. The DRM framework is independent of the ID representation.

Overloading: There is only one commonly trusted party – clearing house in the proposed framework. This can ensure privacy and trust. However, the burden of the clearing house could be very high. A very high computation power is required at the clearing 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.

Risk: The clearing house constitutes a single point of failure, which exposes the whole network to attacks. A successful break-in by attackers to the clearing house could lead to a disaster to all involved parties. Even a short power interruption at the clearing house may cause inconvenience and losses. The framework could cause serious problems when the clearing house is controlled by an untrustworthy, insecure or abusive monopoly.

5. Conclusions

This paper presented a generic DRM framework using WS for mobile media distribution services. The proposed 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 clearing 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 response to the problems of DRM operations and license management.

The proposed framework was proved 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 mobile 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 clearing 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 clearing 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. However, clustering or grid computing solutions may increase the availability and reliability of the clearing house.

References

[1] Brown, J., The Gnutella Paradox, 2005,http://dir.salon.com/tech/feature/2000/09/29/gnutella_paradox/index.html

[2] Burbeck, S., The Tao of E-Business Services, 2005,http://www-106.ibm.com/developerworks/library/ws-tao/

[3] Champion, M., et al., Web Services Architecture, W3C November 14, 2002,http://www.w3.org/TR/2002/WD-ws-arch-20021114/

[4] Chen, M., "Factors Affecting the Adoption and Diffusion of Xml and Web Services Standards for E-Business Systems," *International Journal of Human-Computer Studies* 58 (3) 2003, 259-279.

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

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

[7] DRM, Digital Rights Management, 2005,http://www.microsoft.com/windows/windowsmedia/drm.aspx

[8] eCyberPay, Ecyberpay.Com, 2002,http://www.ecyberpay.com

[9] I-mode, I-Mode Global, 2005,http://i-mode.nttdocomo.com

[10] InterTrust, Intertrust, the Metatrust Utility, Announces Openrights Initiative, Intertrust Press Release 2000.

[11] 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.

[12] 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, 97-111.

[13] Kwok, S. H., "Watermark-Based Copyright Protection System Security," *Communications of the ACM (CACM)* 46 (10) 2003, 98-101.

[14] Kwok, S. H. and Lui, S. M., "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)* 3 (3) 2002.

[15] Kwok, S. H., et al., "Digital Rights Management with Web Services," *Electronic Markets* 13 2003.

[16] Mello, A., Can Web Services Drive Mobile Apps?, May 1, 2002,http://www.zdnet.com/filters/printerfriendly/0,6061,2863482-92,00.html

[17] Memon, N. and Wong, P. W., "A Buyer-Seller Watermarking Protocol," *IEEE Transactions of Image Processing* 10 (4) 2001, 643-649.

[18] Mohan, C., "Dynamic E-Business: Trends in Web Services," *Third VLDB workshop on Technologies for E-Services*, Hong Kong 2002.

[19] Napster, Napster, 2005,http://www.napster.com

[20] Piloura, T., Tsalgatidou, A., and Hadjiefthymiades, S., "Scenarios of Using Web Services in M-Commerce," *ACM SIGecom Exchanges* 3 (4) 2003, 28-36.

[21] UDDI, Uddi.Org, 2005,http://www.uddi.org

[22] Vinoski, S., Putting the "Web" into Web Services. Web Services Interaction Models, Part 2, in *IEEE Internet Computing*, vol. 6 (2002), 90 -92.
[23] W3C, Web Services Description Language (Wsdl) 1.1, March 15, 2001,http://www.w3.org/TR/wsdl
[24] W3C, Simple Object Access Protocol (Soap) 1.1, W3c Note, May 8, 2000,http://www.w3.org/TR/SOAP/
[25] Wigley, A. and Roxburgh, P., *Building .Net Applications for Mobile Devices*, Microsoft Press, 2002.