Article in T-110.501 Seminar on Network Security 2001 ISBN 951-22-5807-2
Publications in Telecommunications Software and Multimedia TML-C7 ISSN 1455-9749
Helsinki University of Technology, Telecommunications Software and Multimedia Laboratory

http://www.tml.hut.fi/Studies/T-110.501/2001/papers/index.html

Mobile Digital Rights Management

Zheng Yan
Nokia Research Center
zheng.z.yan@nokia.com

Abstract

This paper presents a technical overview of current state in Mobile Digital Rights Management (MDRM). Main aspects, such as a DRM system's requirements and architectures are studied. MDRM technologies, such as rights definition languages, cryptography and digital watermarking are discussed. The paper also analyzes the limitations and extra requirements for developing Mobile DRM systems, classifies MDRM based on content types, and proposes MDRM use case models and a MDRM terminal structure. Further more, important issues are discussed regarding the success of MDRM challenge.

1 Introduction

With the rapid growth of the Internet communications, the Internet has become one of the most efficient distribution channels of digital contents for commerce. At present this channel is being extended to mobile area. Certainly, It is ideal to distribute all divers of digital information via networks to consumers' desk-top devices or portable devices. But digital contents, if not protected and managed, can be easily copied, altered, defaced, and distributed to a large number of recipients. Digital Rights Management (DRM), which permits the smooth, secure, trusted movement of digital works from creators and publishers to sellers and consumers, as well as among consumers, is needed for addressing this problem.

In the future, encrypted credit cards, micro-payments, and digital cash will be established in mobile devices. Commerce with digital contents will become a suitable area for both electronic and mobile domains. Mobile DRM (MDRM), the base-bone of future mobile media commerce is the first issue should be addressed. The Mobile DRM is a set of actions, procedures, policies, product properties, and tools that an entity uses to manage its rights in digital contents according to requirements over mobile networks. This paper aims to give an overview of the current state of the MDRM, to analyzes requirements and to discusses technologies, use case models and challenges for developing the MDRM.

2 State of the art

2.1 Basic requirements

The Digital Rights Management concerns techniques, processes, procedures and algorithms related to establishing a trusted computing environment, and trusted infrastructure for the secure preparation, transmission, and prevention of misuse and/or consumption of protected digital contents.

General requirements are proposed in an IETF draft on a Digital Rights Trading System [1]. In this draft, a digital-right is defined as "a digital representation of the right to claim the services or goods". This definition limits digital-rights for claiming services or goods, does not contain usage rights for controlling content's consuming. Therefore, this proposal cannot be applied to a DRM system that ensures content integrity, secures copyright, controls content usage and manages rights acquisition, specification, as well as granting. But it is a good reference for proposing basic requirements of a DRM system.

1. From scalability point of view, "it MUST handle diverse types of rights issued by different issuers".
2. From system security point of view, "it MUST prevent illegal acts" on both rights and contents. For the rights, it MUST prevent them from alternation, forgery, duplicate-redemption, reproduction, and repudiation, and SHOULD ensure privacy. For the contents, it MUST protect their integrity, prevent illegal copy, and make sure the contents are used correctly according to the consumer's rights, as well as provide trust manageability. Because different customer has different preference, privacy may not be a mandatory requirement.
3. From business point of view, "it MUST be practical in terms of scalability, simplicity, implementation / operation cost and efficiency".

2.2 System architecture

Fig. 1 illustrates a lifecycle of digital rights. Typically, there are four stages:

1. Package stage: The operators of this stage are authors or content providers who conduct the following
   - Create rights protection requirements
   - Specify digital rights management policies
   - Specify conditions fee, time, access
   - Specify tracking requirements
2. Sell/protect stage: The handlers of this stage are service providers who do the following works
   - Define pricing

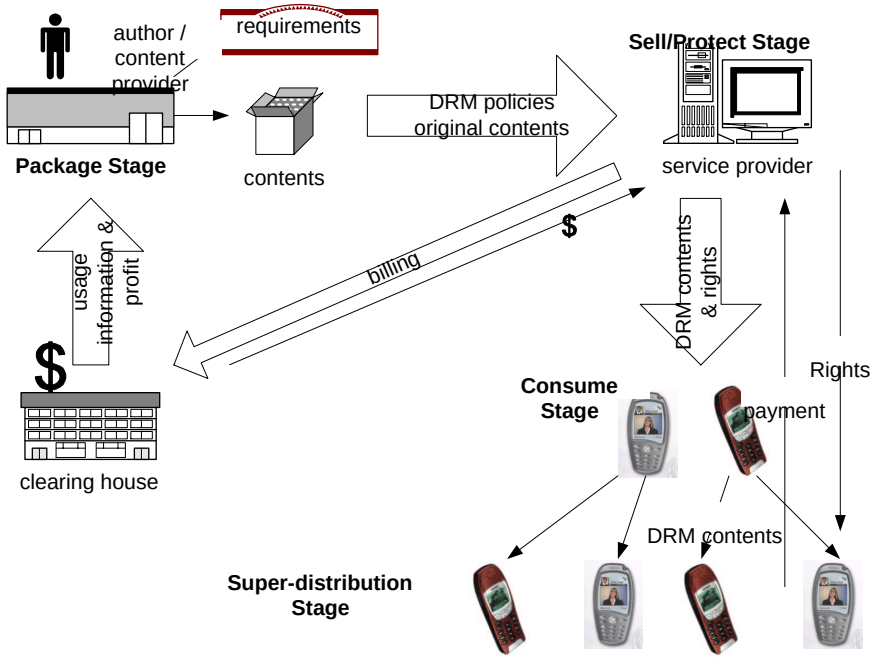

Figure 1: A lifecycle of digital rights

- Define business model
- Specify watermarks
- Package contents with DRM protection
- Distribute contents
- Communicate financial clearinghouse for billing
- Track the usage of contents

3. Consume stage: In this stage, the contents are consumed by a user who determines allowed rights to be purchased. Besides,
   - Contents are customized for that particular user
   - DRM client (e.g. a MDRM device) verifies purchased rights and contents, controls content consuming, rejects illegal activities, and tracks content usage
4. Super-distribution stage: The user can also super-distribute DRM controlled contents to another user who gets additional digital rights from the service provider for consuming protected contents. This activity may continue many times. But no matter how content is distributed, it should be DRM protected.

There are three kinds of system architecture to realize digital rights management: centralized rights management, distributed rights management and semi-distributed rights management.

Centralized rights management:

The rights are managed by a trusted party (a secure server) based on accounts. Any processing of the rights is handled by sending a request to an account manager through a network. Generally, on-line verification is needed in order to prevent duplicated rights redemption. However, this type of system is expensive because accounts have to be maintained for each service provider and for each user. Therefore, it is hard to support system scalability. Additionally, account-based systems have been designed to protect accounts from malicious users but provide less protection from malicious managers. Therefore, the trust policy of these systems is imbalanced. Some Internet coupon systems, such as CoolSavings and ClipACoupon, use this architecture. And this technology is generally used for developing server-based mobile advertisement systems.

Distributed rights management:

There are two approaches to realize it. One is using a tamper-resistant device, like a smart card or a Personal Trusted Device (PTD). In the tamper-resistant device based system, digital rights are stored in a trusted device and circulated among devices. The tamper-resistant device can protect digital-right from both malicious users and malicious service providers. Thus, this kind of system seems to have a bright future especially in the application area of tickets and coupons since one smart card or PTD can store and manage diverse tickets without the cost of maintaining rights centrally. However, these systems create several issues that are hard to overcome, i.e. who should be responsible for issuing a smart card or a PTD if it is shared by multiple applications, how to achieve high performance given the memory and CPU constraints of the small devices. Moreover, the business issue with smart cards or PTDs is that the devices for smart card or PTD verification are not very common especially as user terminals such as PC.

In general, PTD-based solution is suitable for such applications as eTicket, eCoupon, eLicense, etc.

The other approach is using a self-protecting container, which is the key element in InterTrust's commerce platform [11]. The secured container DigiBox enables the association of rules and controls via cryptographic means with information content, to specify the types of content usage permitted and the consequences of usage. Containers are manipulated by using a trusted rights protection application in order to make the protected content available according to its associated access control rules. Payment is generally conducted when a consumer wants to open the container (pay when use, or download first pay later). Similar functionality is provided by IBM's "cryptolope" container [12, 14]. The secure container allows rights management components to be integrated with content in highly flexible and configurable control structures. This approach enables true super-distribution and can support virtually any network topology and any number of participants, including distributors, re-distributors, information retailers, corporate content users, and consumers. But it requires pervasive deployment of tamper-resistant hardware devices to perform secure processing of protected contents. Container technology is playing an increasingly important role as a building block for sophisticated digital rights management system.

Container-based architecture is achieving leadership in the digital content distribution, e.g., eBook, eMusic, eImage, and software, etc.

Semi-distributed rights management:

This architecture tries to combine the advantages of the above two ways and overcome their disadvantages. In [13], a proposed scheme uses a ticket-account server to manage user's rights. The personal rights are not managed by the service provider, but the user himself or someone delegated to manage the account. A smart card is used only for authentication. This approach aims to reduce the account management cost and avoid bottlenecks caused by smart cards. Payment consideration during the rights circulation is ignored in this scheme. Therefore, it is difficult to practice payment for rights transference between users if using this scheme.

3 Technologies

This part introduces technologies for achieving mobile digital rights management.

3.1 DRM languages

A good digital-right representation is necessary in the MDRM system. The representations could be different. There are several candidates available, which are from different sources.

Digital rights expressed by relational database [2]

Jams Barker and his colleagues at Case Wstern Reserve University (CWRU) worked out a database representation, defined as a set of relational database tables and their interpretation. More than 10 basic tables are used to describe the right-properties, together with a large number of administrative, logging and support tables. The advantage of this method is the values in columns of the tables are not restricted by software, but rather by administrators' entries in the support tables. This permits tailoring to any installation's needs together with validity checking of permission table entries. It is convenient to achieve semantics, syntax and security requirements by making use of database technologies. But it is inefficient if table relationships become complicated. And it is only suitable for centralized rights management architecture. Some digital libraries support this digital rights expression.

Xerox's DPRL (Digital Property Rights Language) [3]

Xerox's DPRL (Digital Property Rights Language) is a language that can be used to specify rights for digital contents. It provides a mechanism in which different terms and conditions related to access, fee and time can be specified and enforced for the different operations on digital documents, such as view, print, and copy. Rights specifications are represented as statements in DPRL. Different rights can be specified for different parts of a digital work using a work specification. Within a work specification, different sets of rights applicable to this work are specified. Rights can be grouped into named-groups called "rights groups". Each right within a rights group is associated with a set of conditions. Conditions can be of different types: fee to be paid, time to use, type of access, type of watermark, type of device on which the operation can be performed, and so on. It also allows different categories of rights, such as transfer rights, render rights, derivative-work rights, file-management rights and configuration rights.

XrML (eXtensible rights Markup Language) [4]

Originating from DPRL, XrML addresses some DPRL unsolved issues, such as integrity, authentication of entities, and extends it by adding a set of structural and semantic tags suitable for specifying metadata of XrML documents, validating integrity of XrML documents as well as of digital contents, and authoring relatively simple XrML documents (such as licenses). In addition, XrML adds support for specifying conditions for usage locations and tracking, and simplifies some DPRL document elements and their attributes. XrML is driving the standard for digital rights management. This XML-based language is deployed for expressing the agreement between the content/service provider and information consumer. Therefore, it is more suitable for centralized digital rights management that requires complicated digital rights expression. It has advantage if the centralized DRM server deploys a database that supports XML format. But due to its complication, this DRM language is not suitable for supporting rights management at the terminal, such as a mobile device.

ContentGuard has developed and contributed XrML as an open specification licensed on a royalty-free basis to unify the Digital Rights Management industry and encourage interoperability at an early stage. XrML is supported by such companies as Adobe Systems, Xerox, Hewlett-Packard, Microsoft, Preview Systems and Time Warner.

ODRL (Open Digital Rights Language) [5]

ODRL is another XML-based digital rights expression language. It is a vocabulary for representing terms and conditions over digital contents, which include constraints, permissions, obligations and agreements. The ODRL has no license requirements and it is available in the spirit of "open source" software. This policy will attract many new DRM vendors' support.

Compared with XrML, ODRL is very simple. It is focused on concrete rights expression. ODRL can be used within trusted or untrusted systems. However, it does not determine the capabilities nor requirements of any trusted services. For example, it does not contain any information related to content protection key and rights issuer's digital signature, which are needed in the real system. It is extensible for supporting rights management at the mobile terminal. And obviously, it is not a suitable candidate for centralized DRM system.

XMCL (Extensible Media Commerce Language) [6]

XMCL is an open XML-based language for media commerce and rights management. XMCL is an interchange format that describes usage rules applied to multi-media contents. It is designed to communicate these rules in an implementation independent manner for interchange between business systems and DRM implementations responsible for enforcing the rules described in the language. This language tries to satisfy the requirements of media commerce and provides definitions of client information, digital rights expression and authentication information. But the rights description is simpler compared with ODRL and XrML. It is very suitable for the distributed DRM system, in which digital rights is parsed at the terminal to control the content's consuming.

The above three XML based DRM languages are designed from different points of view and considerations. Which one is selected for a MDRM system should be based on the system's requirements and architecture.

3.2 Cryptographic solution

Cryptographic theory is mature today. Many DRM or MDRM systems are built upon cryptographic blocks. We summarize them in the following.

Digital signatures

In MDRM systems, digital signature is often used for non-repudiation rights issuing. The digital rights should be digitally signed by the issuer. Therefore, the content user could verify the right correctness. And the signature is also a proof of rights purchase.

One-way hash functions

Hash functions are used for integrity checking. Cooperating with digital signature, the hash code of the issued rights and encrypted content is signed by the issuer's private key. The rights user verifies the integrity by decrypting the signature and comparing the hash code with the re-computing hash code. XrML and XMCL support message digest and digital signature.

Symmetric and asymmetric encryption

In some MDRM systems, contents are protected by symmetric-key encryption. While the content encryption key is encrypted using asymmetric-key encryption, therefore, only the user with the correct private key can decrypt the content key, and then consume the content. XCML supports this container based access control.

Traitor tracing (broadcast encryption)

This is an interesting branch emerged into cryptography. The scheme addresses the case when an authority broadcasts some valuable information and it is required that only legitimated clients should be able to decrypt the information. While the schemes make serious assumption about the real life models they work in, they also propose quite efficient ways to trace down the traitor who have constructed new decryption. Broadcast encryption can be used to establish trust between users and service provider, as well as between peer devices. It has some beneficial effects, including key revocation, and circumvent device denial, besides the main effect of device authentication.

3.3 Digital watermarking

In the MDRM system, usage rights (such as "copy once", "copy never", and "copy no more", etc.) are required to tightly bind with the contents using either logical binding or physical binding. Traditional cryptographic approaches separate contents from rights by using a safe container and expressing container's key and digital rights with a DRM language. But they suffer from one important drawback: they do not permanently associate cryptographic information with the contents. Thus, cryptography alone cannot make guarantees about the redistribution or alteration of content after it has initially passed through the cryptosystem. Digital watermarking is a good solution to provide these extended guarantees about digital content usage. The technique modifies the information itself so that it is feasible later to detect pirate copies. In the MDRM system, the digital watermark's function is extended for enabling copy protection, rights management and forensic tracking. It

not only contains copyright information such as creator, content provider, content ID, etc., but also carries usage rights attached to the content. At the user's PTD, the watermark is detected and the content will be processed according to the detected usage rights.

Digital watermarking technologies have been researched and developed not only for static images, but also for audio, video, text, as well as software. Fingerprinting is a branch of watermarking for the traitor catching.

But the current digital watermarking technology is not mature enough for commercial usage. Based on our study and research, there is no standardized watermark solution that can be deployed in real applications. The big issues are:

- Watermark's robustness is not satisfied. Unlike cryptographic algorithm, current watermark cannot sustain most normal attacks.
- Current academic research work has not considered the industrial requirements.

Pure watermarking DRM solution may not secure enough for satisfying the commercial requirements.

3.4 Combination

As can be seen from the above, both cryptographic and watermarking technologies should be combined and deployed in the MDRM systems.

3.5 Vendors

We compare some of the existing DRM systems as Table 1.

It seems that the best way to do the DRM is to control both the software and the hardware. Machine-readable "tags" in the software are then used to represent particular rights that the hardware can interpret. When a piece of content is loaded into a trusted device, it checks the associated digital rules and acts accordingly. From this point of view, general-purpose, but highly untrustworthy device - personal computer may not a good hardware candidate, but personal trusted mobile device will be a suitable one.

In what follows, we will discuss limitations and extra requirements for developing Mobile DRM based on portable small devices, such as mobile phones and communicators. Further more, we will present and analyze Mobile DRM use cases, propose MDRM terminal structure and summarize basic issues that should be considered.

4 Mobile DRM

The demand for various mobile media services is increasing rapidly. Ideally, people hope to do everything they can do via the Internet. Portability and mobility provide users great convenience, and at the same time attract venders to introduce m-Commerce features into

System	Architecture	DRDL	Circulation Model	Copy Prevention/Dection	DRM Technologies
InterTrust	Distributed	–	Pay-when-use, support superdistributed	Container-based	DES, RSA, etc.
EncrypTix	Centralized	–	Pay-before-use	Use authenticated terminal	–
RightsMarket	Centralized	DB based	Pay-when-use	PKL, plug-in trusted tool	–
PublishOne	Centralized	–	Pay-when-use	Container-based	–
DigitalOwl	Centralized	–	Pay-when-use	–	–
ContentGuard	Centralized	XrML	Pay-when-use, not support superdistributed	Integrity, authority	Digital signature, Hash, Watermarking
Wave Systems	Distributed	–	–	Trusted device, support privacy	–
FlexTicket	Semi-distributed	XML, RDF	Pay-before-use, support rights transfer	Secure token in the tamper-proof devices	Digital signature, hash, etc

Table 1: Comparison of different DRM systems

the mobile world. Mobile Digital Rights Management, the base-bone of digital contents related mobile services, is the first issue to address.

4.1 Limitations

Some technologies, such as WAP Identity Module (WIM), ECC (Elliptic Curve Cryptography) chip-embedding, and mobile payment solution, etc., have been and will be introduced for DRM based m-Commerce. However, we also confront difficulties. The mobile devices are small, use low-bandwidth communication technologies, have limited processing power and memory, and use batteries with limited life spans. Thus they cannot accommodate most strong encryption technologies, which are computationally intensive. What is more, the connection speed is very slow and the transaction performance is too bad for many people to accept.

Limited device hardware restricts the embedded software. It cannot support large code library to fulfill various functions as personal computers can. And in most cases, the essential code for security cannot be implemented in the small mobile devices. Hardware security protection is expected with low cost.

4.2 Extra requirements

Apart from the requirements listed in 2.1, special requirements are raised due to the above limitations:

- User interface design should be satisfied with the small display.
- System usability should be accepted by potential users, and the basic clue is simplifying the applications, but providing attractive services.
- Balance the client and server computation for achieving better performance.

Other extra important requirements are:

- Terminals shall have an environment or features for decrypting secure containers and forcing the terminal work following the digital rights.
- The MDRM architecture shall offer profit for both the service provider and the content owner. This is the main power of MDRM development and evolution.

4.3 Classifications

Mobile Digital Rights Management is a big concept that covers various digital data rights management. Based on the type of contents, it can be classified into three groups.

- Rich MDRM: The content managed by the MDRM system is rich media, such as video, e-books, which can only be consumed by high-end mobile devices, like Nokia communicators. Both cryptographic and watermarking technologies are needed for protecting the contents and controlling the usage.
- Light MDRM: The content managed by the MDRM system is light media, such as ring tones, images, music, which can be consumed by medium-end or low-end mobile devices, such as mobile phones, whose platform is close. Cryptographic protection may not be necessary. Watermarking can be used. The device handles enforced usage.
- Minimal MDRM: No digital contents attached. The digital-right itself claims the holder's rights to be served. The typical examples are e-Tickets and e-Coupon. PTD-based system is more suitable for the minimal MDRM. The mobile digital rights are saved in the secure mobile wallet.

4.4 Use Cases

Use cases are very important for analyzing and developing a new service. In this part, we provide three types of Mobile DRM use scenarios, which, we think, are main MDRM services in the future.

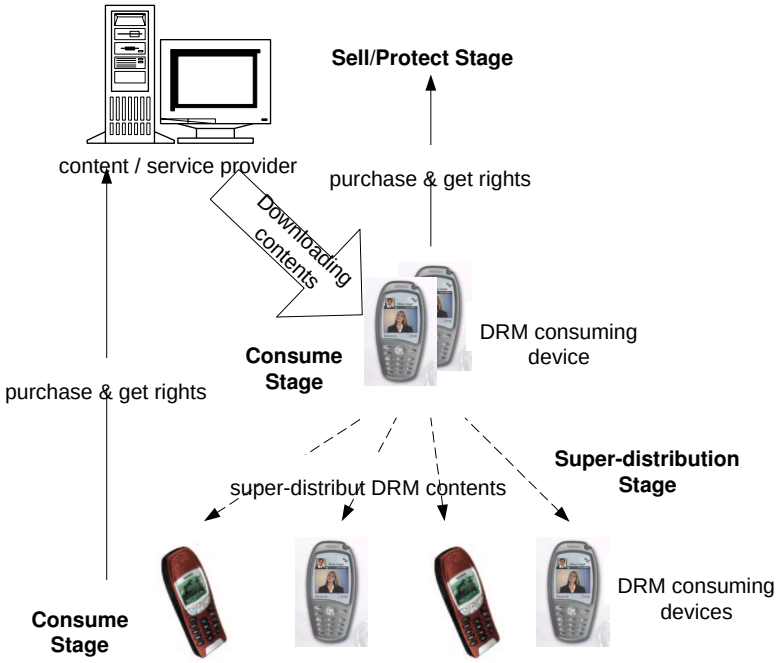

Figure 2: MDRM contents downloading

Digital contents downloading

One of most main DRM services today is downloading digital contents from a content server. This service will definitely expand to mobile commerce. DRM packaged contents, like music, ring tones, e-books, games, etc., are downloaded from a service provider / content provider to the mobile devices, such as Nokia communicator 9210, for consuming. In order to open the packaged (DRM protected) contents, the device should order digital rights from the service provider / content provider via mobile payment. With special digital rights, the user can open DRM protected contents and consume the contents only with the above said device. In addition, the user can also super-distribute the packaged contents to another user's device. But similarly, that user has to order digital rights for consuming the contents. Fig. 2 illustrates the model of above scenarios.

In the downloading service, revenue is shared among content/service providers, network operators, billing processors and DRM device vendors. In this scenario, content is DRM protected using either cryptographic methods or digital watermarking no matter how to distribute it. The digital rights used for consuming the contents need to be purchased from the content/service provider and they are customized for special device's purpose. Mobile terminal should have capability for downloading contents, purchasing digital rights, verifying its correctness and integrity, decrypting and rendering contents securely, and/or detecting watermark.

Broadcasting

Broadcasting is another important service in that DRM contents are broadcast and only users who subscribed the service can receive the plain contents. An interesting example is digital video broadcasting, which is an important channel for distributing rich contents.

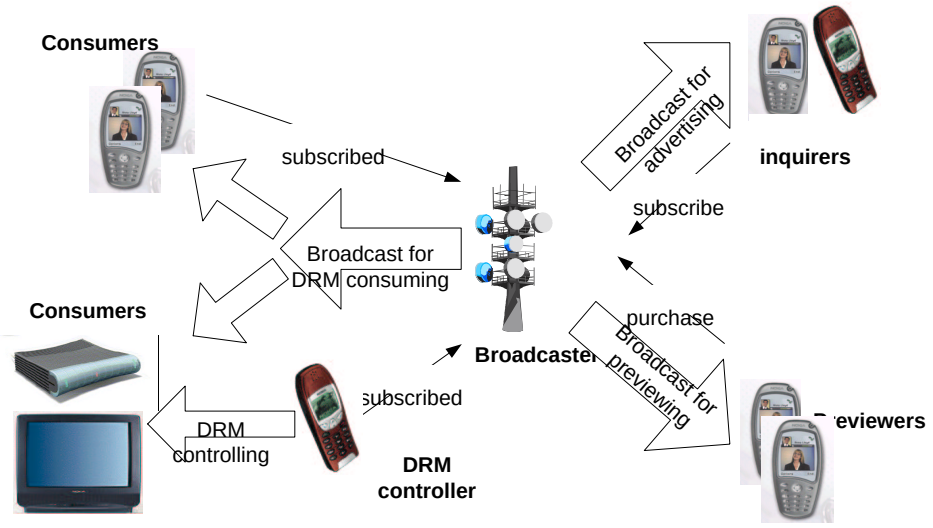

Figure 3: MDRM broadcasting

The mobile device is used to purchase subscription, and get consuming rights to control future digital TV or digital video recorder to render or record video contents. Another example is broadcasting is used for advertisement purpose and works as a digital content previewing channel. In this case, both visible watermark and invisible watermark are embedded into the contents but won't effect the reviewing. If the user is willing to buy the contents, he need purchase the watermark key to remove the visible watermark and get contents with good quality. Fig. 3 illustrates the scenarios described above.

In the broadcasting services, revenue is shared among content/service providers, broadcaster, network operators, billing processors and DRM device vendors. In these scenarios, content is DRM protected using either cryptographic methods or digital watermarking. The consuming is based on subscription or pay-after-preview or pay-when-view. Mobile terminal should have capability for receiving broadcast contents, purchasing or subscribing, decrypting and rendering contents securely, and/or detecting/removing watermark.

Personal content management

From content creators' points of view, it is very important to manage and protect the copyright of their own works. In the future, the wide-range of mobile users will mostly be potential digital content creators. They can create such digital contents as photos, ring tones, mobile phone logos, emotional short messages, animated cartoons, and so on. The requirement for managing and protecting those contents will greatly increase.

Except for managing and protecting digital rights, the future mobile DRM service will also help end users to set up their personal business and build "my digital market" for conducting content related transactions, such as sharing, exchanging, selling, renting, giving, and so on. Fig. 4 proposes a model for personal MDRM solution. A trusted MDRM server ("my content agent") is introduced for handing public personal contents, exchanging "demand" and "offer" information or contents, and providing MDRM protection. High-end mobile devices can execute person-to-person transactions directly. Devices without DRM transaction ability can also conduct business through the content agent.

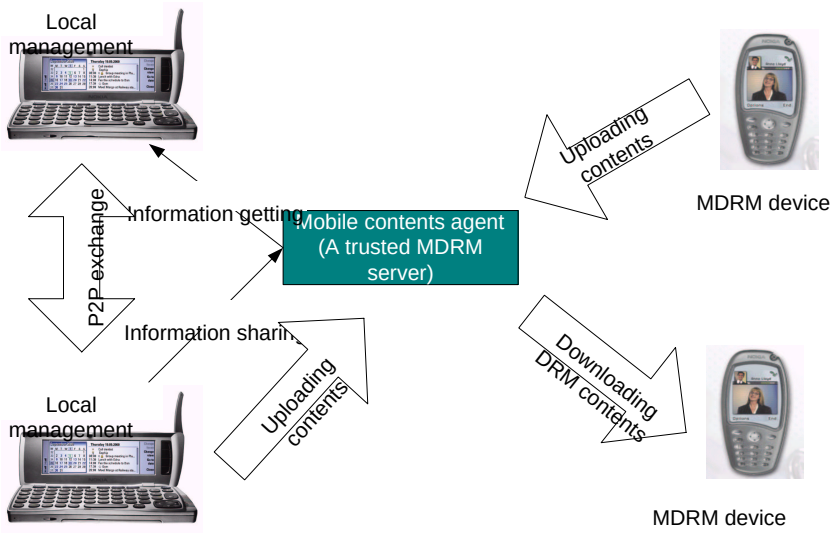

Figure 4: Personal MDRM

In the personal content management services, revenue is shared among content creators (mobile users), service providers, network operators, billing processors and DRM device vendors. The contents created by users are DRM protected using either cryptographic methods or digital watermarking. From creator's point of view, business opportunity is based on content information sharing. Mobile terminal should have capability for decrypting and rendering contents securely, content storing and managing, content DRM protecting (encryption) and controlling, and/or detecting/embedding watermark.

4.5 MDRM Terminal

Based on the above analysis, we propose a DMRM terminal structure that can support the above use cases. As shown in Fig. 5, a tamper-resistant memory is needed for storing secret data like device private key. Above the tamper-resistant memory, a secure DRM shell is running on the operating system of the device. This shell is responsible for handling secure DRM processing, such as content key decryption using the device private key, content rendering and controlling based on decrypted content key, watermark removing using secure watermark key, and mobile payment signing using the device private key, and so on. There are several models plugged into the DRM shell. Watermarking model is responsible for digital watermark embedding, detecting and removing. Mobile payment model takes charge of all kinds of payment required by the DRM applications. Cryptography model handles MDRM cryptographic processing. A secure database is used for storing logical rights and usage records. DRM applications are high level media software, which render contents based on the digital rights. DRM clients connect to networks and request contents and rights.

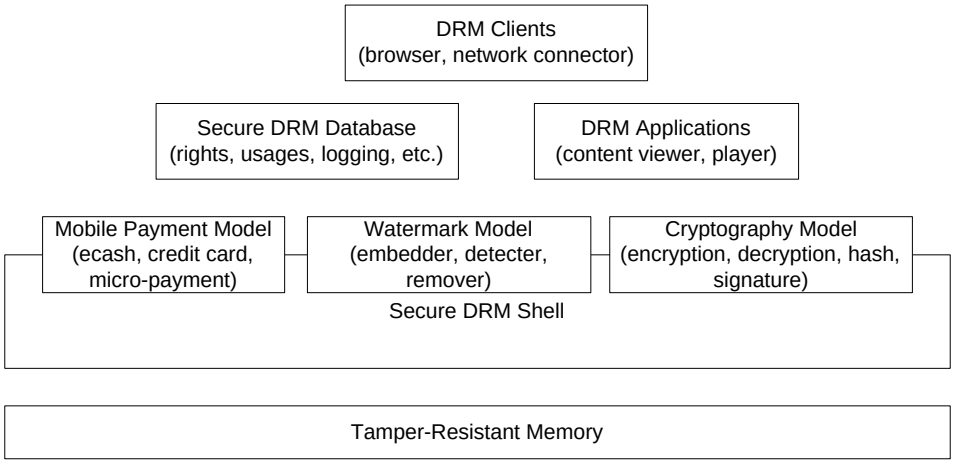

Figure 5: MDRM terminal structure

4.6 Issues

Mobile Digital Rights Management is still a new business. There are some issues that require careful considerations.

From technical point of view, cryptographic theory is mature although more efficient algorithm is always required for small, processing limited devices. Digital watermarking is very important in MDRM. But there is a long way to go for a standardized solution that can be accepted by commercial applications. The current technical situation will greatly affect today's MDRM system design and technology's selection.

From content provider's point of view, it is essential to manage digital rights for preventing piracy and retrieving large sum of lost revenues. But at the same time to set up digital rights protection, content providers also confront the risk to lose their customers. Technology is not the key issue here. How to provide an attractive MDRM service for the content users and how to achieve profit for the business's survival are the biggest challenge for service providers and vendors.

From the content creator to the content consumer, there is a value chain for digital content distribution, as shown in Fig. 6. At every phase of the chain, different companies play their own roles for achieving benefits. The whole business depends on the chain and its cooperation and competition.

5 Conclusion remarks

The paper overviews the state of the arts in the Mobile Digital Rights Management. Based on the existing technologies, we further analyze the limitations and additional requirements for developing the MDRM systems. Depending on the abilities of terminal device, different kinds of content services can be provided. In particular, we propose a number of MDRM service scenarios and analyze their business models and terminal requirements.

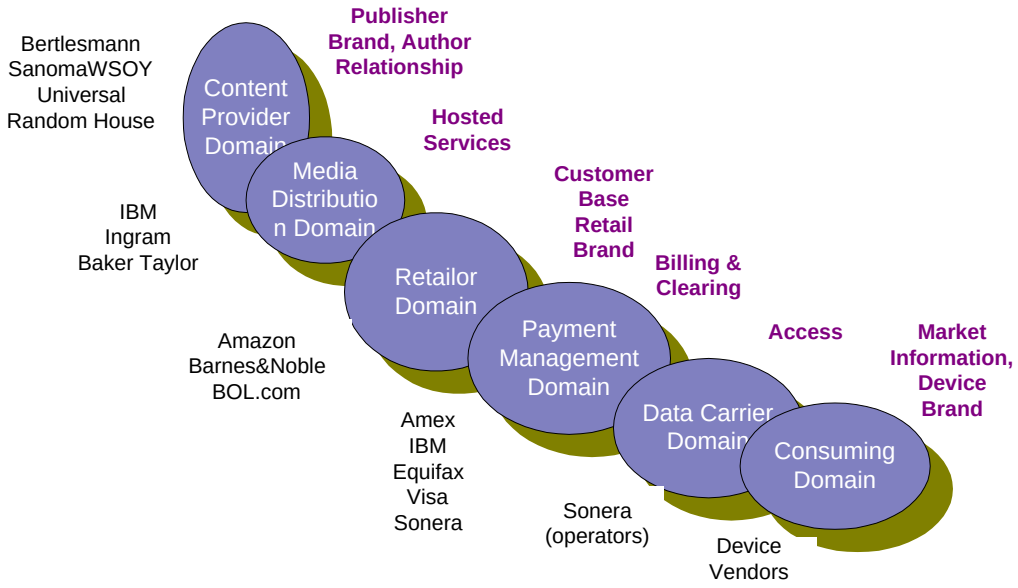

Figure 6: MDRM value chain

Furthermore, a MDRM terminal structure is proposed for adapting presented use cases. Finally, from both technical and business points of view, we summarize issues that should be considered for achieving the success in Mobile DRM.

Mobile DRM is a novel business, an attractive challenge. It is important for future mobile media commerce because it works as the basic platform for supporting almost all media services. On the other hand, it is also a challenge because its success depends on not only technologies, but also business models that can be accepted by both content/service providers and content consumers.

References

[1] Fujimura K. Requirements for Digital-Right Trading. IETF Trade Working Group. draft-ietf-trade-drt-requirements-00.txt, Feb. 2000

[2] Tareq M. A., et. al. Safeguarding Copyrighted Contents: Digital Libraries and Intellectual Property Management. *D-Lib Magazine*, Apr. 1998.

[3] Ciccione B., et. al. The Digital Property Rights Language. *Private Communication*, 1996

[4] XrML Specifications. <http://www.xrml.org/>

[5] Open Digital Rights Language. <http://odrl.net/>

[6] Extensible Media Commerce Language. <http://www.xmcl.org/>

[7] Digital Property Rights Language. <http://www.oasis-open.org/cover/dprl.html>

[8] MPEG Rights Expression Language. <http://xml.coverpages.org/mpegRights.html>

[9] Fujimura K. and Nakajima Y. General-purpose Digital Ticket Framework. *3rd USENIX Workshop on Electronic Commerce*, pp. 177-186, August 1998

[10] Fujimura K., et. al. ML Ticket: Generalized Digital Ticket Definition Language. *The W3C Signed XML Workshop*, Apr. 1999

[11] Sibert O. DigiBox: A Self-Protecting Container for Information Commerce. *1st USENIX Workshop on electronic Commerce*, July 1995

[12] Gladney H.M. and Lotspiech J.B. Safeguarding Digital Library Contents and Users: Assuring Convenient Security and Data Quality. *D-Lib Magazine*, May 1997

[13] Matsuyama K. and Fujimura K. Distributed Digital-Ticket Management for Rights Trading System. *1st ACM Conferences on Electronic Commerce*, Nov. 1999

[14] Auerbach J. S, Creation and Distribution of Cryptographic Envelope. Patent number: 5673316. Sept. 1997