A Wrapper-based Digital Publication Issuing Mechanism

Wei-Chen Wu[1]*, Horng-Twu Liaw[2], Jiann-Fu Lin[3], Li-Lin Hsiao[4]
[1]*Computer Center, Hsin Sheng College of Medical Care and Management,
Taoyuan County, Taiwan, R.O.C.*
wwu@hsc.edu.tw
[2]*Department of Information Management, Shih Hsin University,
Taipei, Taiwan, R.O.C.*
htliaw@cc.shu.edu.tw
[3]*Department of Management Information System,
Takming University of Science and Technology, Taipei, Taiwan, R.O.C.*
alfu@takming.edu.tw
[4]*Department of Information Management, Shih Hsin University,
Taipei, Taiwan, R.O.C.*
hsiao@cc.shu.edu.tw

Abstract

With the advance in the electronic devices, digital publications become more and more popular in our life. However, the properties of digital contents make themselves be easily copied and transferred if there is not any proper protection for them. Hence, it is a critical issue for publication provider to effectively control and distribute their digital publications. Digital Rights Management is a mechanism, which might congregate various techniques to protect the rights of digital publication from copyrights violations. Moreover, Wrapper-based Digital Rights Management technique applies encapsulating digital contents by packaging content and monitoring by API-Hook to control and protect them, which provide a way to authenticate users by users' machine serial number or smart card via network. Hence, users may use the digital contents without changing their digital content player. According to the definition of Digital Rights Management, this paper provides a digital publication issuing mechanism, which supports superdistribution for advertising digital publications effectively and improving development of digital contents.

Keywords : *Digital rights management; API-hook; Wrapper; Superdistributation; Business model*

1 Introduction

With the rapid development of the Internet and computers, more and more digital documents and digital products weed through the old to bring forth the new unceasingly. It is essential to protect digital contents, which will improve the intention of digital contents providers to create new products and protect the rights of legal customers.

Digital Rights Management (DRM) is a mechanism, which congregates hardware and software to ensure the rights of digital publication providers against illegal usage [1]. The

DRM could track and manages the usage of digital contents, such as the legality of copy or distribution. However, some prevailing systems, such as Windows Media Rights Manager, iTunes, and Adobe Systems, only support their own digital content types. These systems do not provide interoperability, which limits the usage of digital contents with many restrictions.

The concept and architecture of Superdistribution is proposed by Mori [2, 3] for building up a software service system in a P2P structure. Superdistribution could also be a business model, which distributes digital publications safely and effectively by combining some free methods [4, 1].

There are some advantages would be obtained if DRM supports superdistribution, such as progressing distribution channels, reducing distribution costs, and forming strong partner networks. In this paper, we will adopt Windows32 API hooking for it is more inexpensive than designing DRM system with expensive hardware. Under the assumption of payment flow has been well implemented, we implement the DMR system on Windows 32-bit platform. The rest of this paper is organized as follows. We review the DRM model in Section 2. In Section 3, we propose a novel wrapper-based digital publication issuing mechanism. In Section 4, the comparison with other related works are presented. Finally, a conclusion is presented in Section 5.

2 Related Works

DRM [4, 5, 6, 7, 8] is a mechanism, which congregates various techniques for protecting the rights of digital publication providers. It provides the functions of content protection, process monitor, and tracing user records. To maintain interest and friendly relationships between digital contents providers and products customers, DRM needs to support digital publication transaction, rights transferring, and digital publication delivery. It also needs to describe and identify the digital publication in a digital publication transaction. Hence, the roles involved in a transaction of the traditional DRM model are content owner, distributor, license broker, and user [1, 4, 7]. However, some recent researches of DRM [7, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23] focused on ontology researches for rights description [17, 23], integration and interoperation research [7, 9], constraints prototype [18], privacy protection [20, 21], implementation [12, 14, 15], and business model, such as superdistribution [3, 10] and offline distribution [19, 22].

In 2005, Yang proposed a design of multimedia digital rights management mechanism based on XrML [14]. Yang's mechanism focused on the business model using grant of rights to form various business models, which adopted Windows Media Rights Manager and only supported some kinds of media. Moreover, it does not support offline authorization and rights transferring.

In 2007, A digital publication right issuing management practice mechanism was proposed by Liaw et al. [15]. Their mechanism provided a complete digital rights management process design. However, it does not support offline tracking, rights transferring, rights revoking and superdistribution. In the same year, Sun et al. proposed an improved digital rights management system based on smart cards [13]. They improved some disadvantages of privacy in an identity-based DRM system proposed by Conrado [20]. Their system retains users' privacy by removing relationship between users and digital publications and protects digital production by using secure memory. However, their system is not a DRM system because it does not monitor the rights of using digital publications. In 2009, a ticket based digital rights management model was proposed by Sun et al. [11]. Their mode built up a new role named service provider and used a ticket issuing mechanism to protect users' privacy. However, the system uses huge computing power with partial blind signature mechanism that leads to a huge amount of computation cost and that causes this model unavailable.

3 Our Mechanism

We propose a secure, fair and effectively distributing digital publications issuing mechanism for the systems lacking of business models and charging mechanisms to solve the problems of digital publications being transacted on the Internet.
In our mechanism, we adopts Elliptic Curve Cryptography (ECC) [24], KryptoKnight authentication and key distribution system [25] to protect customers' personal information, and add a trusted third party call certificate authority to issue licenses and to support fair judgment in transactions if necessary. The original business mode of DRM is still kept in our mechanism for easily adapting the rights of new customers. The major five roles of this mechanism are described as follows: Customer(C),Certificate Authority (CA),Digital Publication Provider(PP),Digital Publication Rights Issuing Management Platform(MP) and Bank(BK).

- Customer (C): A customer may buy digital publications from digital publication rights issuing management platform. Then, the customer can download the digital publications and get the rights of usage if the payment process has been finished.
- Certificate Authority (CA): CA is the trusted third party of this mechanism. It services for registration of applicants, licenses issuing, licenses revoking, and licenses management. It also stores the information of transactions for judgment if there are arguments about the transactions.
- Digital Publication Provider (PP): The major work of a digital publication provider is to digitalize authors' works and then provides these digital publications to customer.
- Digital Publication Rights Issuing Management Platform (MP): It provides a website to advertise and publish providers' digital publications. It also needs to provide the functions of licenses issuing, transaction tracing, and cash flow managing.
- Bank (BK): It supports the cash flow of transactions.

3.1 Architecture of Our Mechanism

Our mechanism contains twelve phases, which are Certificate Requesting and Registration Phase, Superdistirbution Phase, Publication Selecting and Authentication Phase, Flexible Payment Phase, License Issuing Phase, Tracking Phase, License Reissuing Phase, Customer's License Transferring Phase, Customer's License Redeeming Phase, Payment for Offline Use Phase, Provider's Right Redeeming Phase, and Provider's Right Transferring Phase. Table 1 shows the notations used in the twelve phases.

1. Certificate Requesting and Registration Phase
   This phase is an initial phase, all roles of this mechanism must register to CA and

Table 1. Notation used in the remainder of the paper

Notation	Description
ID_X	identity of X
PW	password
TID_X	a temporary identity generating by KryptoKnight
$PayMode$	the selected paying mode
DID_X	the serial number of X's device
MID	MP's Server ID
PID	PP's Server ID
$DPSN$	the serial number of a digital publication
$License$	the license of the digital publication
$token$	the verification code of the license
Sig_X	a signature signed with the key of X
E_X	a function encrypted with the key of X
$UseRule$	the grants of the digital publication
$UseData$	the use data of the customer
$OtherData$	other data
$GetMoney_X$	rates of X
$PayMoney_X$	account payable of X
$timestamp$	the timestamp of license issuing time
r	a random number
$GuarMoney$	guarantee money
$TradeOK_X$	success message of X's transaction
$publication$	a protected digital publication
$Cert_X$	certificate of X
DID_{DB}	the device IDs stored in database

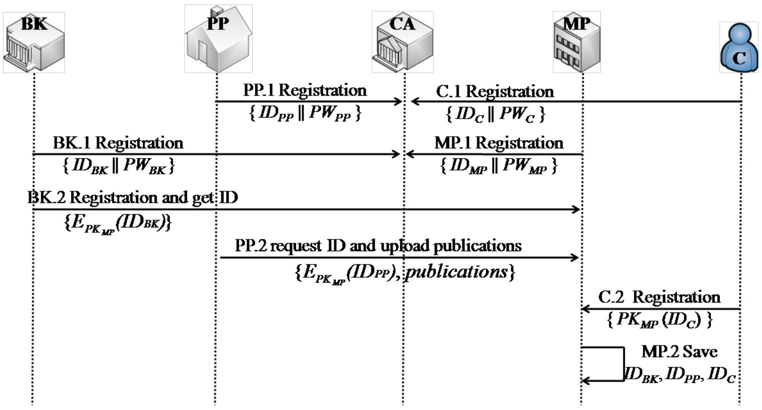
BK
PP
CA
MP
C
PP.1 Registration
$\{ ID_{PP} \| PW_{PP} \}$
C.1 Registration
$\{ ID_C \| PW_C \}$
BK.1 Registration
$\{ ID_{BK} \| PW_{BK} \}$
MP.1 Registration
$\{ ID_{MP} \| PW_{MP} \}$
BK.2 Registration and get ID
$\{E_{PK_{MP}}(ID_{BK})\}$
PP.2 request ID and upload publications
$\{E_{PK_{MP}}(ID_{PP}), publications\}$
C.2 Registration
$\{ PK_{MP} (ID_C) \}$
MP.2 Save
ID_{BK}, ID_{PP}, ID_C

Figure 1. The processes of Certificate Requesting and Registration Phase

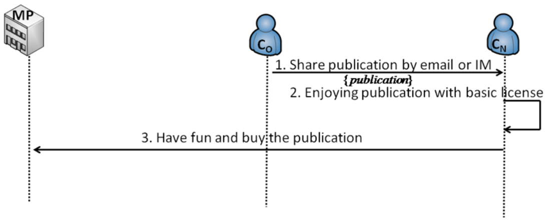
MP
C_O
C_N
1. Share publication by email or IM
{publication}
2. Enjoying publication with basic license
3. Have fun and buy the publication

Figure 2. The processes of Superdistribution Phase

request certificates. After registration, PP assigns the basic grants for superdistribution and transfers the grants of digital publications to XrML format. Then, PP sends digital publications and XrML to MP through a secure channel. If customers are interested in the digital publications, they register to MP by sending their certificate, which could be the serial number of a device or a smart card. The certificate might be the serial number of a device or smart card. Fig. 1 shows the detailed processes.

2. Superdistribution Phase
   The potential customer C_N could receive a protected digital publication shared by original customer C_O through email, instant message, or P2P. C_N can use the publication with basic grants. If C_N are interests in it, C_N could buy it from DRM controller. Fig. 2 shows the detailed processes.
3. Publication Selecting and Authentication Phase
   After the customer finishes registration and gets the certificate, the customer could get publications from the website of MP or by superdistribution. The Customer C sends request containing wanted publication identity and wanted grants to MP. Then, MP decides a temporary private key d_{MP} and generates a public key U_{MP} with Elliptic Curve Diffie-Hellman (ECDH). Next, MP sends the encrypted message PKC to C. C receives the messages and checks the content. If the message is correct, C decides a temporary private key d_C and generates the private key U_C with ECDH. Next, C generates temporary identity TID_C with KryptoKnight. Then, C sends the message to MP, including TIDC, serial number of the publication, and the payment mode. The payment modes may be credit transfer, micro-payment, or credit card payment. Finally, MP decrypts message with private key d_{MP}. Then, we could identify C by

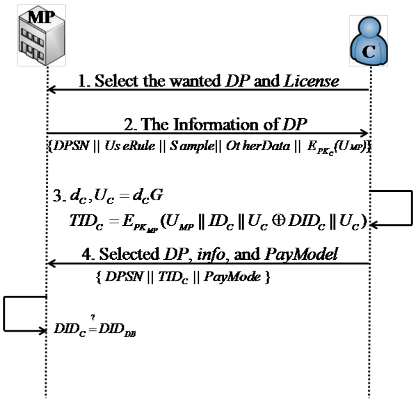
MP
C
1. Select the wanted DP and $License$
2. The Information of DP
$\{DPSN \,||\, UseRule \,||\, Sample \,||\, OtherData \,||\, E_{PK_C}(U_{MP})\}$
3. $d_C, U_C = d_C G$
$TID_C = E_{PK_{MP}}(U_{MP} \,\|\, ID_C \,\|\, U_C \oplus DID_C \,\|\, U_C)$
4. Selected DP, $info$, and $PayModel$
$\{ DPSN \,||\, TID_C \,||\, PayMode \}$
$DID_C \overset{?}{=} DID_{DB}$

Figure 3. The processes of Publication Selecting and Authentication Phase

checking if TID_C consists in Database (DB). The process could keep anonymity for customer C by using temporary identity without containing personal information. Fig. 3 shows the detailed processes.

4. Flexible Payment Phase
   Customers could buy licenses from online services after authentication. Fig. 4 shows the detailed processes. MP decides temporary private key d_{MP} and generates public key U_{MP} with ECDH after C requests the wanted digital publication. Then, MP selects a random number r and generates session key K between MP and C by hashing. After that, MP sends the encrypted messages to C. C could generate the same session key K by using the parameter sent by MP and check validity after receiving message from MP. After checking the validity of K, C returns related message as response to MP. Next, MP sends the related message to BK for payment, including the serial number of the publication, payment mode, identity, and payment amount. When the transaction completed, BK sends the serial number of the publication, the customer's identity and the message of transaction to MP. Then, MP sends the profit distribution agreed by MP and PP to BK for processing the transaction. In addition, the $TradeOK_C$ contains a hash of serial number of the publication, the customer's identity, and the timestamp. And the above messages are signed with BK's private key.

5. License Issuing Phase
   After payment, the customer can request the license to enjoy the publication. The detailed processes are shown as Fig. 5. C sends $TradeOK_C$ to MP for requesting the license. At the same time, they start to agree using the session key K. After MP checks the valid $TradeOK_C$, it issues the license encrypted with K to C. Then, C decrypts the message and gets the license. Next, C hashes identity of C's device and the license as a token for checking validity in the future. Finally C sends the token to MP. In order to protect user privacy, the personal information does not write in the license. Further, it is impossible for users to change the grants or other information because the licenses are signed with MP's private key.

6. Tracking Phase
   Regardless of online or offline patterns, DRM controller must record and trace the processes of how users enjoy publications for protecting the publications. Fig. 6

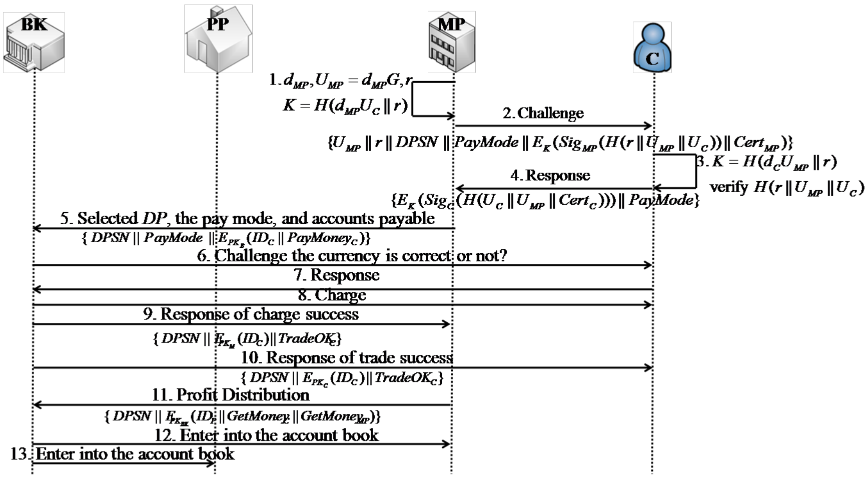
BK
PP
MP
C
1. $d_{MP}, U_{MP} = d_{MP}G, r$
$K = H(d_{MP}U_C \| r)$
2. Challenge
$\{U_{MP} \| r \| DPSN \| PayMode \| E_K(Sig_{MP}(H(r \| U_{MP} \| U_C)) \| Cert_{MP})\}$
3. $K = H(d_C U_{MP} \| r)$
verify $H(r \| U_{MP} \| U_C)$
4. Response
$\{E_K(Sig_C(H(U_C \| U_{MP} \| Cert_C))) \| PayMode\}$
5. Selected DP, the pay mode, and accounts payable
$\{DPSN \| PayMode \| E_{PK_B}(ID_C \| PayMoney_C)\}$
6. Challenge the currency is correct or not?
7. Response
8. Charge
9. Response of charge success
$\{DPSN \| E_{PK_M}(ID_C) \| TradeOK_C\}$
10. Response of trade success
$\{DPSN \| E_{PK_C}(ID_C) \| TradeOK_C\}$
11. Profit Distribution
$\{DPSN \| E_{PK_{BK}}(ID_P \| GetMoney_P \| GetMoney_{MP})\}$
12. Enter into the account book
13. Enter into the account book

Figure 4. The processes of Flexible Payment Phase

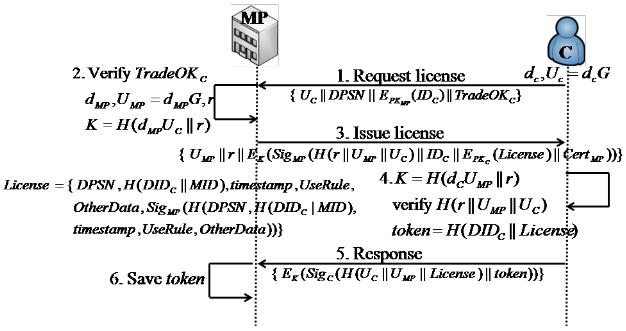
MP
C
1. Request license
$d_c, U_c = d_c G$
$\{U_C \| DPSN \| E_{PK_{MP}}(ID_C) \| TradeOK_C\}$
2. Verify $TradeOK_C$
$d_{MP}, U_{MP} = d_{MP}G, r$
$K = H(d_{MP}U_C \| r)$
3. Issue license
$\{U_{MP} \| r \| E_K(Sig_{MP}(H(r \| U_{MP} \| U_C)) \| ID_C \| E_{PK_C}(License) \| Cert_{MP})\}$
$License = \{DPSN, H(DID_C \| MID), timestamp, UseRule, OtherData, Sig_{MP}(H(DPSN, H(DID_C | MID), timestamp, UseRule, OtherData))\}$
4. $K = H(d_C U_{MP} \| r)$
verify $H(r \| U_{MP} \| U_C)$
$token = H(DID_C \| License)$
5. Response
$\{E_K(Sig_C(H(U_C \| U_{MP} \| License) \| token))\}$
6. Save $token$

Figure 5. The processes of License Issuing Phase

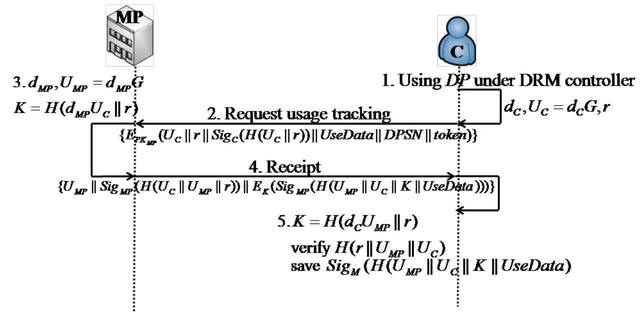
MP
C
1. Using DP under DRM controller
$d_C, U_C = d_C G, r$
2. Request usage tracking
$\{E_{PK_{MP}}(U_C \| r \| Sig_C(H(U_C \| r)) \| UseData \| DPSN \| token)\}$
3. $d_{MP}, U_{MP} = d_{MP} G$
$K = H(d_{MP} U_C \| r)$
4. Receipt
$\{U_{MP} \| Sig_{MP}(H(U_C \| U_{MP} \| r)) \| E_K(Sig_{MP}(H(U_{MP} \| U_C \| K \| UseData)))\}$
5. $K = H(d_C U_{MP} \| r)$
verify $H(r \| U_{MP} \| U_C)$
save $Sig_M(H(U_{MP} \| U_C \| K \| UseData)$

Figure 6. The processes of Tracking Phase

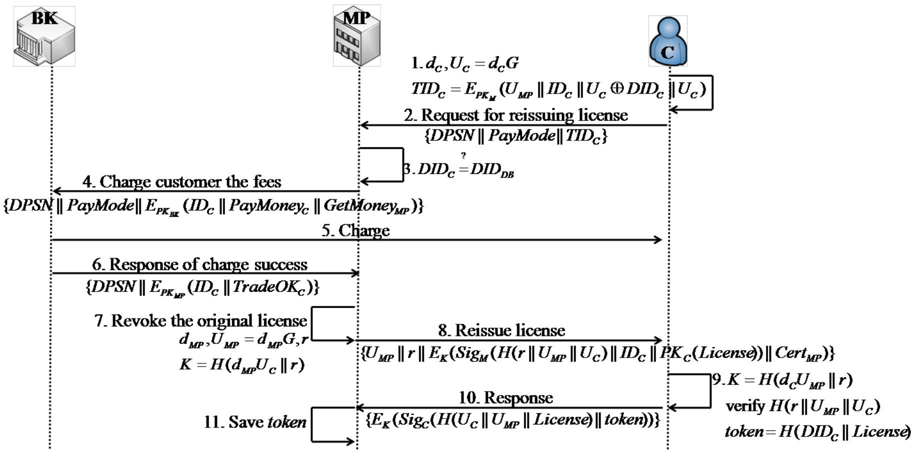
BK
MP
C
1. $d_C, U_C = d_C G$
$TID_C = E_{PK_M}(U_{MP} \| ID_C \| U_C \oplus DID_C \| U_C)$
2. Request for reissuing license
$\{DPSN \| PayMode \| TID_C\}$
3. $DID_C \overset{?}{=} DID_{DB}$
4. Charge customer the fees
$\{DPSN \| PayMode \| E_{PK_{BK}}(ID_C \| PayMoney_C \| GetMoney_{MP})\}$
5. Charge
6. Response of charge success
$\{DPSN \| E_{PK_{MP}}(ID_C \| TradeOK_C)\}$
7. Revoke the original license
$d_{MP}, U_{MP} = d_{MP} G, r$
$K = H(d_{MP} U_C \| r)$
8. Reissue license
$\{U_{MP} \| r \| E_K(Sig_M(H(r \| U_{MP} \| U_C) \| ID_C \| PK_C(License)) \| Cert_{MP})\}$
9. $K = H(d_C U_{MP} \| r)$
verify $H(r \| U_{MP} \| U_C)$
$token = H(DID_C \| License)$
10. Response
$\{E_K(Sig_C(H(U_C \| U_{MP} \| License) \| token))\}$
11. Save token

Figure 7. The processes of License Reissuing Phase

shows the detailed processes. When customers connect with the Internet and enjoy the digital publications at the same time, DRM controller will verify the validity of the user and usage. DRM controller sends request for identifying, including token, using data, and information of key exchanging. After MP receives the request and identifies the validity, it sends the information, which contains current state of information and are signed with MP's private key, to C. Then, C saves above information.

7. License Reissuing Phase
   Customers may lose their licenses. This mechanism allows customers to request license reissuing. The detailed processes are shown as Fig. 7. C decides the temporary private key d_C and generates temporary public key U_C with ECDH. Then, C computes the temporary identity TID_C and sends serial number of the publication, the payment mode for reissuing, and TID_C to MP for requesting license reissuing. MP checks the validity of DID_C by searching its DB after receiving the request. Next, MP notifies BK that will pay the amount of fees. Then, BK processes the transaction and sends message of transaction completed to MP. MP revokes C's original license and computes the session key K after receiving the message showing the transaction is completed. Next, MP reissues the license and encrypts it with K. Then, MP sends above to C. C computes session key and then generates token. After that, C sends token to MP. MP saves token after receiving it.

8. Customers' License Transferring Phase

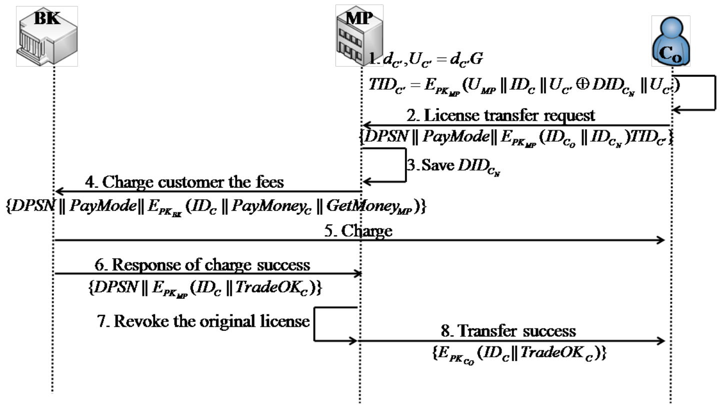
BK
MP
Co
1. $d_{C'}, U_{C'} = d_{C'}G$
$TID_{C'} = E_{PK_{MP}}(U_{MP} \| ID_C \| U_{C'} \oplus DID_{C_N} \| U_{C'})$
2. License transfer request
$\{DPSN \| PayMode \| E_{PK_{MP}}(ID_{C_O} \| ID_{C_N})TID_{C'}\}$
3. Save DID_{C_N}
4. Charge customer the fees
$\{DPSN \| PayMode \| E_{PK_{BK}}(ID_C \| PayMoney_C \| GetMoney_{MP})\}$
5. Charge
6. Response of charge success
$\{DPSN \| E_{PK_{MP}}(ID_C \| TradeOK_C)\}$
7. Revoke the original license
8. Transfer success
$\{E_{PK_{CO}}(ID_C \| TradeOK_C)\}$

Figure 8. The processes of Customers' License Transferring Phase

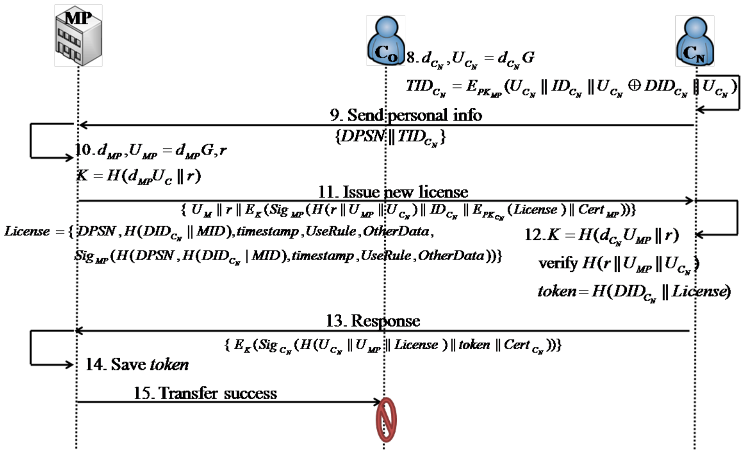
MP
Co
CN
8. $d_{C_N}, U_{C_N} = d_{C_N}G$
$TID_{C_N} = E_{PK_{MP}}(U_{C_N} \| ID_{C_N} \| U_{C_N} \oplus DID_{C_N} \| U_{C_N})$
9. Send personal info
$\{DPSN \| TID_{C_N}\}$
10. $d_{MP}, U_{MP} = d_{MP}G, r$
$K = H(d_{MP}U_C \| r)$
11. Issue new license
$\{U_M \| r \| E_K(Sig_{MP}(H(r \| U_{MP} \| U_{C_N}) \| ID_{C_N} \| E_{PK_{C_N}}(License) \| Cert_{MP}))\}$
$License = \{DPSN, H(DID_{C_N} \| MID), timestamp, UseRule, OtherData,$
$Sig_{MP}(H(DPSN, H(DID_{C_N} | MID), timestamp, UseRule, OtherData))\}$
12. $K = H(d_{C_N}U_{MP} \| r)$
verify $H(r \| U_{MP} \| U_{C_N})$
$token = H(DID_{C_N} \| License)$
13. Response
$\{E_K(Sig_{C_N}(H(U_{C_N} \| U_{MP} \| License) \| token \| Cert_{C_N}))\}$
14. Save *token*
15. Transfer success

Figure 9. The processes of Customers' License Transferring Phase (Cont.)

In order to handle various modes of transactions, we support license transferring services for flexible use of valid licenses. Fig. 8 and 9 show the detailed processes.Original Customer C_O computes temporary private key and public key; then generates the temporary identity with KryptoKnight. The following step is sending information to MP to request license transferring, including the device identity of new customer C_N, identity of C_N, payment mode, and serial number of the publication. MP decrypts the request and saves. Then, MP notifies BK that will pay the amount of fees. Next, BK processes the transaction and sends successful message to MP. After that, MP revokes the license of C_O, and then sends both the successful message and revoking message to C_O. To request license, C_N sends temporary identity to MP. After MP receives the request, it verifies validity of C_N and computes session key K. Then, MP sends the license and related information, which are encrypted with K to C_N. C_N computes K and identifies its validity. Then, C_N generates token of the license and sends it to MP. Finally, MP saves the token and then notifies C_N that the license transferring phase is complete.

9. Customers' License redeeming Phase

To provide customers with more service related licenses, this mechanism supports

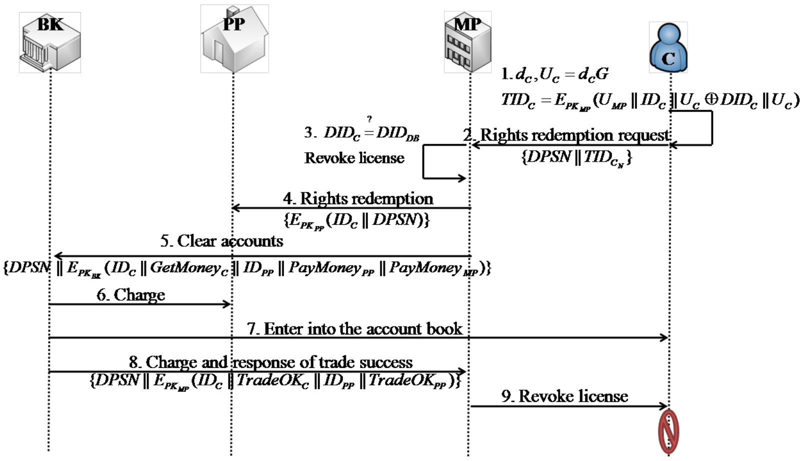
BK
PP
MP
C
1. $d_C, U_C = d_C G$
$TID_C = E_{PK_{MP}}(U_{MP} \| ID_C \| U_C \oplus DID_C \| U_C)$
3. $DID_C \overset{?}{=} DID_{DB}$
Revoke license
2. Rights redemption request
$\{DPSN \| TID_{C_N}\}$
4. Rights redemption
$\{E_{PK_{PP}}(ID_C \| DPSN)\}$
5. Clear accounts
$\{DPSN \| E_{PK_{BK}}(ID_C \| GetMoney_C \| ID_{PP} \| PayMoney_{PP} \| PayMoney_{MP})\}$
6. Charge
7. Enter into the account book
8. Charge and response of trade success
$\{DPSN \| E_{PK_{MP}}(ID_C \| TradeOK_C \| ID_{PP} \| TradeOK_{PP})\}$
9. Revoke license

Figure 10. The processes of Customers' License redeeming Phase

license redeeming. Moreover, customers will refund customers' remaining amount and they can buy other publications. The detailed processes are shown as Fig. 10. C decides the temporary private key and computes its public key first. Next, C computes his temporary identity TID_C, and then he sends the request to MP, including serial number of the publication and TID_C. After MP receives the request, MP verifies the validity of C and then sends the license redeeming to PP. At the same time, MP computes settlement amount and notifies BK with the amount. Until BK completes the transaction, BK sends the message of transaction completed to MP. Finally, MP revokes license of C.

10. Payment for Offline Use

In order to offer customers the convenience of offline services, this section presents the processes. Because the protection of offline mode only relies on DRM controller, there are more restrictions to customers. The restrictions may be use times, print times, and effective duration, etc. Moreover, the licenses will be invalid as soon as customers reach termination conditions. Fig. 11 shows the detailed processes. After C requests wanted publication by sending the serial number of the publication, the license type, and the payment mode to MP, MP notifies BK that the amount paid by C and the amount received by MP. Next, BK processes the transaction and sends the message of transaction completed to MP. Finally, MP sends the contents to C, including the license and the protected publication. Moreover, the detailed operations of clients are shown in the section of implementation.

11. Rights Transferring Phase

There are various business models in commercial circumstances. Considering the demands of providers, they may transfer their rights to others. For example, some enterprises may find business opportunities from some digital publications and then buy out them. Moreover, the transferred target must be the member of this mechanism. The detailed processes are shown as Fig. 12. Original provider PP_O requests MP to transfer the rights by sending serial number and the payment mode which are encrypted with the public key of MP. Then, MP saves above information and notifies BK how to allocate the amount. After BK completes the transaction and sends the successful message to MP, MP transfers the rights to new provider PP_N

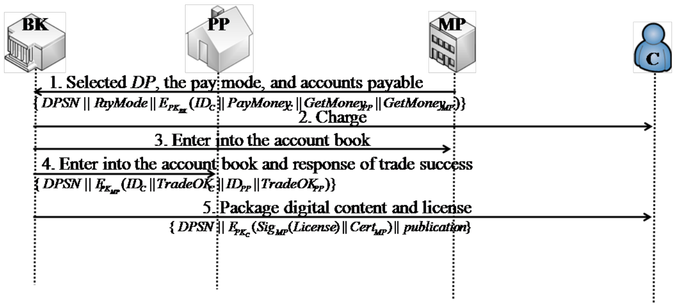
BK
PP
MP
C
1. Selected DP, the pay mode, and accounts payable
$\{DPSN \| PayMode \| E_{PK_{BK}}(ID_C \| PayMoney_C \| GetMoney_{PP} \| GetMoney_{MP})\}$
2. Charge
3. Enter into the account book
4. Enter into the account book and response of trade success
$\{DPSN \| E_{PK_{MP}}(ID_C \| TradeOK_C \| ID_{PP} \| TradeOK_{PP})\}$
5. Package digital content and license
$\{DPSN \| E_{PK_C}(Sig_{MP}(License) \| Cert_{MP}) \| publication\}$

Figure 11. The processes of Payment of offline use Phase

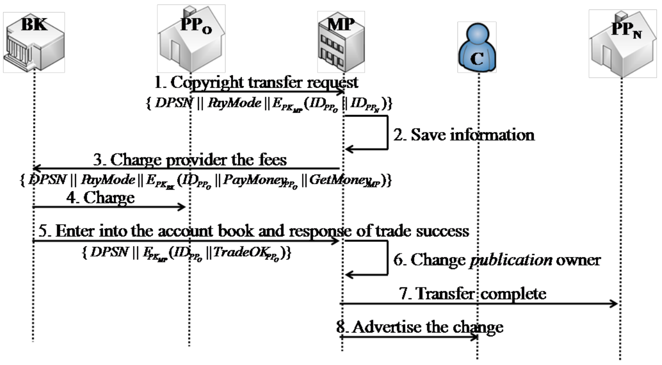
BK
PP_O
MP
C
PP_N
1. Copyright transfer request
$\{DPSN \| PayMode \| E_{PK_{MP}}(ID_{PP_O} \| ID_{PP_N})\}$
2. Save information
3. Charge provider the fees
$\{DPSN \| PayMode \| E_{PK_{BK}}(ID_{PP_O} \| PayMoney_{PP_O} \| GetMoney_{MP})\}$
4. Charge
5. Enter into the account book and response of trade success
$\{DPSN \| E_{PK_{MP}}(ID_{PP_O} \| TradeOK_{PP_O})\}$
6. Change publication owner
7. Transfer complete
8. Advertise the change

Figure 12. The processes of Rights Transferring Phase

and advertises the information to all clients who buy the licenses about the PP_O.

12. Rights Redeeming Phase
    Providers may want to off shelve the digital publications and then request rights redeeming. Fig. 13 shows the detailed processes. The Provider PP decides the temporary private key d_{PP} and computes his public key U_{PP}. Then, he generates temporary identity and sends both TID_C and serial number of the publication to MP for requesting rights redeeming. MP decrypts the request and verifies the validity of PP. Next, MP stops selling the publication and revokes the licenses. Then MP settles the amount of each customer who buys the publication. After that, MP notifies BK of processing transaction and advertises all customers who buy the publication. Finally, BK sends the message of transaction completed to MP.

3.2 Implementation

This research implements a sample of DRM system for protecting digital publications. The implementation contains following features: reaching integrity and security by wrapping; monitoring processes by API HOOK; describing digital rights language with XrML. Moreover, this system allows various authentications, including both online and offline authentication with device identity of hardware or smart card. This section displays the architecture of this system.

There are four functional modules in this system shown as Fig. 14 and 15 , including Digital Content (DC) Management, DC Package, DC Wrapper, and DC Rights Exchange

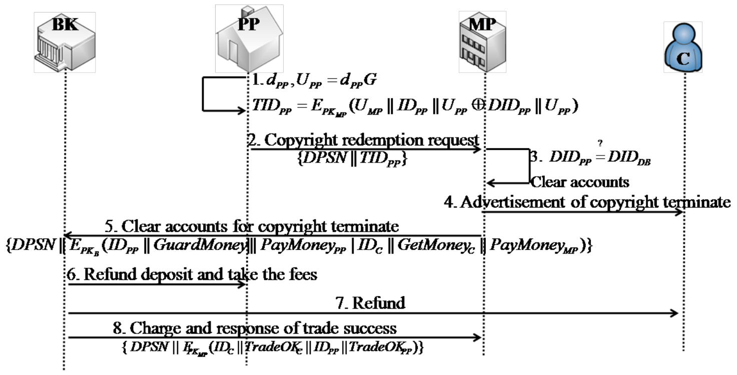
BK
PP
MP
C
1. $d_{PP}, U_{PP} = d_{PP}G$
$TID_{PP} = E_{PK_{MP}}(U_{MP} \| ID_{PP} \| U_{PP} \oplus DID_{PP} \| U_{PP})$
2. Copyright redemption request
$\{DPSN \| TID_{PP}\}$
3. $DID_{PP} \overset{?}{=} DID_{DB}$
Clear accounts
4. Advertisement of copyright terminate
5. Clear accounts for copyright terminate
$\{DPSN \| E_{PK_B}(ID_{PP} \| GuardMoney \| PayMoney_{PP} | ID_C \| GetMoney_C \| PayMoney_{MP})\}$
6. Refund deposit and take the fees
7. Refund
8. Charge and response of trade success
$\{DPSN \| E_{PK_{MP}}(ID_C \| TradeOK_C \| ID_{PP} \| TradeOK_{PP})\}$

Figure 13. The processes of Rights Redeeming Phase

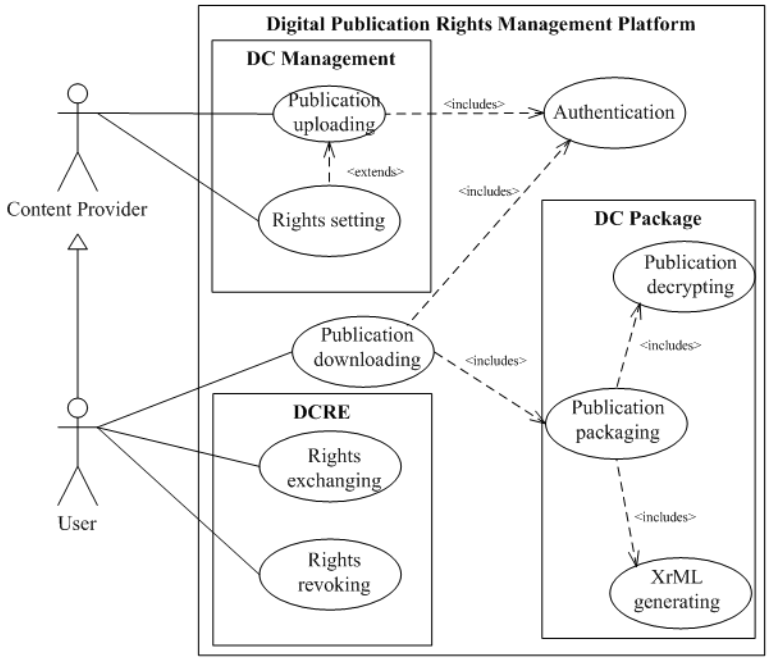

Figure 14. The modules and functions in digital publication rights management platform

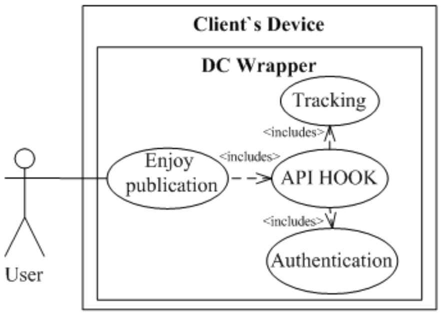

Figure 15. The functions of DC Wrapper

(DCRE). Furthermore, DC Management, DC Package, and DCRE are the modules of digital publication rights issuing management platform. DC Wrapper is the module of clients and it starts when they use the services of digital publications. The followings describe the functions of each module:

1. DC Management
   This module provides publication uploading and rights setting, such as the print right, use times, and use durations, etc.

2. DC Package
   What the providers hope are distributing their publications effectively and make money. Furthermore, customers must be authenticated and paid for their publications. This system decrypts digital publications for avoiding unauthorized use. Moreover, we package the contents to a new file, including decrypted publication, copyright information, rights expression language, and API HOOK module. In addition, we support marketing grants and basic grants for supporting superdistribution. In addition, above makes rights exchanging and rights revoking more easily. Besides, this implementation provides convenience of user-friendly interface under API HOOK by adopting MFC.

3. DCRE
   This system supports rights exchanging and rights revoking. As mentioned above, this research allows providers think more about business

4. DC Wrapper
   We adopt API HOOK to monitor processes. Customers need not to install plug-in and change their habits.

4 Analysis

This section compares the functions between this research and related literatures [11, 13, 14, 15, 19, 21] shown in Table 2, including basic services, business model, and implementation.

Table 2. Comparisons of related researches

	[15]	[14]	[13]	[21]	[19]	[11]	Ours
				Basic Services			
Description	Yes	Yes	x	x	Yes	x	Yes
Identifying	Yes	Yes	x	x	Yes	x	Yes
Transaction	Yes	Yes	x	Yes	Yes	x	Yes
Protection	Yes	Yes	Yes	x	Yes	x	Yes
Monitor	Yes	Yes	No	x	Yes	x	Yes
Tracing	No	No	No	x	Yes	x	Yes
				Business Model			
Super-distribution	No	No	No	Yes	No	No	Yes
				Implementation Information			
Format supporting	Almost all	WMA, WMV, ASF	x x	x x	x x	x x	Almost all
License issuer	No	License Server	License Server	License Server	License Server	License Server	License Server
License type	CP	ID	ID	ID	No	Ticket	CP,ID
Encryption	No	No	Yes	Yes	No	x	Yes
Portable	Yes	No	Yes	x	Yes	x	Yes
Offline use	Yes	No	No	x	Yes	x	Yes
Authentication methods	Online, MC, SC	Online Online	SC SC	x x	Online Online	x x	Online, MC, SC

CP: Combined with Publication.
ID: Independence.
MC: Machine Code.
SC: Smart Card.
x: Non-mentioned.

4.1 Basic Services

As Table 2 shows, most of the researches focus on some areas. Therefore, they don't satisfy the basic services proposed by Rosenblatt [6]. Some researches reply on making assumptions to reach some basic services. This research extends study of Liaw et al. [15] and improves the monitor modules. Therefore, we reach all the functions of basic services.

4.2 Business Model

In order to improve the development of DRM, DRM needs to support suitable business models according to Zhaofeng [26]. There are the models of m2m and m2c in the research of Liu et al. [2], but they are similar to superdistribution. Moreover, Liu et al. do not implement their system. However, the implementation of our research proves our research can support the business model of superdistribution.

In addition, Osterwalder [27] proposes business model including value proposition, target customer, capabilities, activity configuration, partner network, resources and assets, customer relationship, information strategy, feeling and service (distribution channels), and trust and loyalty. Supporting superdistribution of this research brings the following benefits: providing more distributed channels; expanding the partner work for everyone may be a distributor; reducing the cost since distributing digital publications through superdistribution reduces the burden of servers.

4.3 Implementation Information

We can find out following features through implementation information: supporting which type of file format; supporting which type of authentication method, and how to support superdistribution. This mechanism extends study of Liaw et al. [15] and supports superdistribution by departing basic grants and marketing grants.

5 Conclusion

In this paper, we proposed a novel digital publication issuing mechanism, which supports business model, and implemented the system. In this mechanism, we adopted API-HOOK to avoid changing habits of customers. The mechanism inherits all advantages of the research of Liaw et al. [15]. In addition, we proposed the concept of DRM controller, such that Digital publication could be distributed effectively and securely under such protection.

References

[1] Ku, W., Chi, C.: Survey on the technological aspects of digital rights management. Information Security (2004) 391–403

[2] Liu, Z., Wang, B., Lee, B., Han, M.: Security license distribution mechanism for rights delegation models of group distribution between consumers. In: Computational Science and its Applications, 2007. ICCSA 2007. International Conference on, IEEE (2007) 144–152

[3] Mori, R., Kawahara, M.: Superdistribution: the concept and the architecture. IEICE TRANSACTIONS **1976** (1990)

[4] Liu, Q., Safavi-Naini, R., Sheppard, N.: Digital rights management for content distribution. In: Proceedings of the Australasian information security workshop conference on ACSW frontiers 2003-Volume 21, Australian Computer Society, Inc. (2003) 49–58

[5] Iannella, R.: Digital rights management (drm) architectures. (2001)

[6] Rosenblatt, B., Trippe, B., Mooney, S.: Digital rights management: business and technology. New York (2002)

[7] Jamkhedkar, P., Heileman, G., Martinez-Ortiz, I.: Middleware services for drm. In: Communication Systems Software and Middleware, 2007. COMSWARE 2007. 2nd International Conference on, IEEE (2007) 1–8

[8] Coyle, K.: Rights expression languages. (2004)

[9] Filho, F., de Albuquerque, J., de Geus, P.: A service-oriented framework to promote interoperability among drm systems. Autonomic Management of Mobile Multimedia Services (2006) 124–127

[10] Wang, B., Lee, B.: A study for license distribution mechanism using accumulated device identifier in drm system. In: Multimedia and Ubiquitous Engineering, 2007. MUE'07. International Conference on, IEEE (2007) 1118–1123

[11] Sun, M., Laih, C., Yen, H., Kuo, J.: A ticket based digital rights management model. In: Consumer Communications and Networking Conference, 2009. CCNC 2009. 6th IEEE, IEEE (2009) 1–5

[12] Nishimoto, Y., Baba, A., Ogawa, K.: Advanced conditional access system for digital broadcasting receivers using metadata. In: Consumer Electronics, 2006. ICCE'06. 2006 Digest of Technical Papers. International Conference on, IEEE (2006) 111–112

[13] Sun, H., Hung, C., Chen, C.: An improved digital rights management system based on smart cards. In: Digital EcoSystems and Technologies Conference, 2007. DEST'07. Inaugural IEEE-IES, IEEE (2007) 308–313

[14] Yang, C.T.: Design of multimedia digital rights management mechanism based on xrml. Master's thesis, Department of Computer Science and Information Engineering of National Chung Cheng University (2005)

[15] H.T. Liaw, J.F. Lin, W.L.S.L., Lin, C.: Digital publication right issuing management practice mechanism. Journal of e-Business **9** (2007) 321–352

[16] H.T. Liaw, M.H. Guo, W.L., Hsiao, L.: Digital right issuing management mechanism and implementation strategy. Journal of Computer Science and Application **3** (2007) 23–42

[17] Nadah, N., de Rosnay, M., Bachimont, B.: Licensing digital content with a generic ontology: escaping from the jungle of rights expression languages. In: Proceedings of the 11th international conference on Artificial intelligence and law, ACM (2007) 65–69

[18] Muhlbauer, A., Safavi-Naini, R., Salim, F., Sheppard, N., Surminen, M.: Location constraints in digital rights management. Computer Communications **31** (2008) 1173–1180

[19] Kirovski, D., Jain, K.: Off-line economies for digital media. In: Proceedings of the 2006 international workshop on Network and operating systems support for digital

audio and video, ACM (2006) 20

[20] Conrado, C., Kamperman, F., Schrijen, G., Jonker, W.: Privacy in an identity-based drm system. In: Database and Expert Systems Applications, 2003. Proceedings. 14th International Workshop on, IEEE (2003) 389–395

[21] Sheppard, N., Safavi-Naini, R.: Protecting privacy with the mpeg-21 ipmp framework. In: Privacy Enhancing Technologies, Springer (2006) 152–171

[22] Cattelan, R., He, S., Kirovski, D.: Prototyping a novel platform for free-trade of digital content. In: Proceedings of the 12th Brazilian Symposium on Multimedia and the web, ACM (2006) 79–88

[23] Damiani, E., Fugazza, C.: Toward semantics-aware management of intellectual property rights. Online information review **31** (2007) 59–72

[24] Barker, E., Johnson, D., Smid, M., of Standards, N.I., (US), T.: Recommendation for Pair-wise Key Establishment Schemes Using Discrete Logarithm Cryptography:(revised). National Institute of Standards and Technology (2007)

[25] Molva, R., Tsudik, G., Van Herreweghen, E., Zatti, S.: Kryptoknight authentication and key distribution system. Computer SecurityESORICS 92 (1992) 155–174

[26] Zhaofeng, M., Yixian, Y., Xinxin, N.: Secure and flexible digital rights management in a pervasive usage mode. In: Computational Intelligence and Security, 2007 International Conference on, IEEE (2007) 863–867

[27] Osterwalder, A., Pigneur, Y.: An ontology for e-business models. Value creation from e-business models (2004) 416