PAPER

A Trust Distributed DRM System Using Smart Cards

Ming-Kung SUN[†a)], **Michael CHANG**[†], ***Nonmembers***, **Hsiao-Ching LIN**[†], ***Student Member***, **Chi-Sung LAIH**[†,††], ***and*** **Hui-Tang LIN**[†,††], ***Nonmembers***

SUMMARY Digital Rights Management (DRM) ensures that the usage of digital media adheres to the intentions of the copyright holder and prevents the unauthorized modification or distribution of media. Due to the widespread adoption of digital content use, DRM has received a fair amount of attention and has seen implementation in many commercial models. Although many DRM schemes have been introduced in the literature, they still suffer from some security issues and may not guarantee the quality of performance. In this paper, we propose a trust-distributed DRM model to provide improvements for realistic DRM environments to bring more functionality to users. We use the features of the smart cards to provide an option of anonymity for the consumer while continuing to protect the rights of the copyright holder and the financial interests of the media industry. We also classify the security criteria of DRM systems and show that our proposed smart card based DRM scheme satisfies all of these criteria.

key words: *anonymous consumption, digital rights management, privacy, public key infrastructure, smart card, ticket card*

1. Introduction

In January 1994, the concrete concept of Digital Rights Management (DRM) for protecting intellectual property was proposed in a Network Multimedia Environment conference [1]. One definition of DRM [2] is *a system for protecting the copyrights of data circulated via the Internet or other digital media by enabling secure distribution or disabling illegal distribution of the data*. DRM systems play significant roles in processes concerning the flow of content [3]–[5]. When a provider furnishes content, they inherently control the ability to grant usage rules to that content. DRM aims to protect digital contents from illegal or unauthorized access [6]. The main goal of DRM is to protect digital media from illegal copy, and uses public key infrastructure (PKI) to facilitate this end. Many companies or organizations such as InterTrust [7], Microsoft [8], and Open Mobile Alliance (OMA) [9] have developed DRM systems.

Because of the rapid development of the Internet, digital content can now be disseminated quickly and easily to be used on or off-line. The openness of the Internet allows individual users to contribute towards digital content creation or modification. Among these users, some may wish to copyright their works for financial profit. Thus, some research [10] proposed copyright protection systems for content which can be modified by multiple users. At the same time, digital multimedia related technologies have grown in capability. New products with high storage capacity and high mobility form factors have spawned new business models and corresponding DRM systems to protect content. For example, devices such as mobile phones now have the capacity to store large amounts of media and provide the ability to use that media while mobile. A model such as [11] may provide a viable DRM framework to distribute and protect copyrighted media for a mobile cellular environment.

DRM embodies certain specific requirements. DRM needs *persistent safeguarding*, which is protection that stays with the contents. Conceptually, DRM can be envisioned as *remote control* for content. Not only is protection required during delivery of this content, but content controls must be enforced after delivery. A DRM system needs to incorporate several components, such as control flows, monitoring mechanisms, media identification, tracing mechanisms, and conditional access. To meet such requirements, a DRM system employs many cryptographic technologies [6], [12], [13] such as encryption/decryption, authentication, signatures, access control, and key management. There are two main functions of a DRM system. One is to prevent users from unauthorized access during the complete life cycle of digital content, and the other is to efficiently manage various kinds of usage rules.

The contribution of this paper can be described in two parts. First, we focus on the issue of anonymous consumption. Most existing DRM models do not support anonymous consumption, so we propose a model using smart cards to provide this capability. Second, the adoption of smart cards also supports other important DRM issues. One is *portability* which is an open issue for DRM related efforts. A user must purchase new licenses for other devices even though they have already purchased the media rights on another platform. This unreasonably hinders the concept of fair use and increases inconvenience. This can be alleviated by the portability property of the smart card based scheme. These smart cards also solve the issues of trust and regional restrictions. We will explain how the smart card concept works in the latter part of this paper.

This paper is organized as follows: in Sect. 2, we survey related research concerning DRM systems. A modified

Manuscript received September 27, 2011.
Manuscript revised July 1, 2012.

[†]The authors are with the Institute of Computer and Communication Engineering, National Cheng-Kung University, Tainan, Taiwan.
[††]The authors are with the Electrical Engineering Department National Cheng-Kung University, Tainan, Taiwan.
a) E-mail: morgan@crypto.ee.ncku.edu.tw

DOI: 10.1587/transinf.E95.D.2991

DRM model is proposed in Sect. 3 which improves on the properties introduced. Section 4 describes the capabilities and achievements of our model. A comprehensive security analysis and comparison of our system and other DRM solutions is presented. Finally, we provide some closing remarks in Sect. 5.

2. Related Work

In this section, we review related research in regards to five attributes: anonymity, portability, privacy, regional restrictions, and trust issue.

2.1 Anonymity

In existing DRM systems, a consumer has to reveal their identity to obtain a license for protected content. Some researchers [14], [15] have spotlighted the need to use digital content without disclosing any personal information. A DRM system should provide the capability to extend anonymity to their consumers. Previous research [16] stated the problem scope is larger than only privacy concerns about personal data and illustrated the management of intellectual property rights. In order to remedy this issue, the DRM system should allow anonymous consumption. This allows the option of privacy and anonymity if elected by the consumer.

2.2 Portability

In a DRM system, security is the key factor. For current applications, these requirements rely on a tamper-proof device to play protected content according to the content usage rules. These systems are classified as device based DRM systems [8], [9]. In this model, every license is bound to a unique playback device, so the license stored in one device cannot be shared by another. If a user has more than one device and wishes to use the same content on all their devices, they have to purchase licenses for every device. This is undesirable and illustrates the problem concerning portability.

In contrast, identity based DRM systems, such as Project DReaM [17], provide more flexibility to users. Sun Microsystem's Project DReaM aimed to produce "interoperable DRM architecture implementing standardized interfaces and processes for the inter-operability of DRM systems." Instead of device based mechanisms, they adopted an identity based method to authenticate legitimate users. Identity based DRM systems allow use of digital contents anywhere and anytime on compliant devices. Based on this concept, a number of identity based DRM systems [18], [19] have been proposed. By their design, identity based DRM systems do not inherently account for privacy anonymity or considerations. Other work concentrate on frameworks using quantification theory (predicate logic) [20] or adopting a systems based approach along with defined formal semantics [21] to provide ubiquitous license inter-operability.

2.3 Privacy

DRM is widely adopted to guard intellectual property for content owners but consumer privacy is not heavily considered. In current DRM systems, the DRM client module knows what media users consume, and the license server knows what content users have obtained licenses for. Another commonly unaddressed issue of DRM is the safeguarding of personal privacy. Although many privacy protection schemes [22]–[24] have been proposed, they only focus on protecting customer privacy from misuse from outsiders, and do not provide safeguards against abuse by the service providers themselves. This lapse allows service providers to acquire personal data to profile user habits. This often overlooked practice violates consumer privacy.

2.4 Regional Restrictions

A digital content provider may serve customers who reside in various global regions. For commercial reasons, providers may wish to divide their market into several areas to offer value added services such as languages, or subtitles suitable to that region. DRM can provide this functionality. Greveler proposed a scheme [25] of enforcing a DRM system that allows for region-dependent licensing policies. The DVD market is an example of regional restrictions. DVD products are divided into six regions, and the players in one region can only play DVDs according to the region code allowed. The same concept is applied here for digital contents.

2.5 Trust Issue

Current DRM systems focus on content protection from malicious consumers based on the assumption that the servers themselves are trustworthy. The issue of trust concerns the possibility of malicious elements within the DRM system. Researchers [26], [27] have suggested the need to secure DRM servers against each other. The concept of least privilege should be followed in case a server is compromised. Safeguards can be designed into the DRM model to mitigate these issues.

To the best of our knowledge, no system exists that simultaneously addresses the DRM issues described in this section. Note an earlier incarnation of this model was outlined in previous work [28]. The model has evolved to include added functionality from refined communication and details the specifics of security interaction between roles. A comprehensive security analysis of model has been provided. This work can be regarded as a successor and realization of the author's earlier research.

3. The Proposed Smart Card Based DRM Model

The DRM framework is well defined though implementations vary. The general model has been detailed through previous DRM research [14], [29], [30]. There are three major

roles in most existing models. They are the content server, license server and consumer. To design a DRM system which addresses the issues in Sect. 2, we propose a DRM model which provides confidentiality for the digital content while simultaneously protecting user privacy.

This section is composed of three parts. In the first part, we will provide some assumptions and supporting concepts for our DRM system. In the second part, we will define the roles involved in the proposed DRM model. Lastly, we dissect the system process flow.

3.1 Preliminaries and Assumptions

We include some build upon prerequisites to support our DRM model. The DRM scheme assumes the open availability of Internet access until the point when the client device receives the content decryption key. After this, the content can be used off-line. As emphasized in Sect. 1, digital content must be protected from unauthorized access. To this goal, the proposed DRM model is supported by the underlying concepts of public key infrastructure (PKI) technology including the use of encryption/decryption, digital signatures, message authentication codes (MAC), and implies the availability of an authoritative entity such as a certificate authorities (CA). To send a message under the PKI solution, the sender signs it[†] with its private key before sending and includes the CA's certificate as follows:

$$S \rightarrow R : M, Sig_{PrK_S}(h(M)), Cert_S(PuK_S) \quad (1)$$

where S designates the sender, R represents the receiver, M is the sending message, PrK_S/PuK_S is the private/public key pair of the sender that used to generate its signature to prove the message is actually sent by the claimed sender, $h(*)$ is a one-way hash function which receives input M to create the message digest $h(M)$, and $Cert_S$ is the public key certificate of sender. The receiver of the message has to extract and verify the public key of S using the certificate and verify the sender's signature using its certified public key. The receiver ensures message integrity during the transmission by inputting the received M into the pre-shared hash function, and checks if the output is the same as the received $h(M)$ using

$$h(M) \stackrel{?}{=} V_{PuK_S}(Sig_{PrK_S}(h(M))) \quad (2)$$

where $V_{PuK_S}(*)$ represents using the public key of S to verify if the hash of the message $h(M)$ was signed by S's private key. In order to complete the verification process, the receiver needs the public key of the CA. For example, assuming keys are certified by a CA, the certificate $Cert_S(PuK_S)$ of a sender should include the following:

$$Cert_S(PuK_S) = PuK_S \parallel Sig_{PrK_{CA}}(PuK_S \parallel ID_{CA}) \quad (3)$$

where $\parallel$ is the concatenation operator, PrK_{CA} is CA private key and ID_{CA} is the unique ID of the CA. These cryptographic concepts will be considered as a foundation and utilized when required but will not be otherwise detailed in the process flow.

3.2 Supporting Components

In order to build the proposed smart card DRM model, some foundational concepts and components are required. The following supporting concepts are adopted in this design:

- *Ticket card.* In [28], we proposed a ticket based DRM model. In this current research, we apply the ticket concept to smart cards. Any smart card with CPU able to support PKI functions (such as those adhering to ISO-7816) can be employed in this model. The ticket card is a stored value container purchased from a retailer. This ticket card can be registered and linked to the consumer's identity or can be used anonymously. Anonymous ticket cards differ from registered ticket cards only in the additional act of registration before payment. There is no physical or technical difference between the two kinds of ticket cards. When purchased without identification registration, this card facilitates anonymous consumption and in the case of registered ticket cards, refunds of lost cards.
- *Tamper-Proof Device.* The use of secret information such as keys or right objects necessitates the use of a Tamper-Proof Device (TPD) in each client. In addition to deal with secret information, this device will be also responsible for PKI operations. To reduce risk of compromise by attackers, the device should be tamper resistant. As its name implies, the TPD contains a set of sensors that detect hardware tampering and erase all stored sensitive data to prevent compromise. Access to the TPD should be restricted to authorized smart cards and the client device is assumed to be trusted.
- *Rights Object.* The Rights Object (*RO*) enables use of content by permitting the DRM client device to utilize the protected content. The *RO* contains the usage rules outlined by the content provider. The distributor is responsible for management of these usage rules.
- *Revocation List.* Where *RO* permits usage of content, the Revocation List (*RL*) denies use of ticket cards based on a retailer maintained database of revoked cards. Whether ticket cards are registered or anonymous, every card has a unique identifier. The *RL* is maintained by the retailer in order to ensure that the TPD does not provide validation to the malicious ticket cards with revoked IDs to play digital content.
- *metadata.* In addition to providing digital content, the provider catalogs *metadata* for their products. This *metadata* contains information related to the content such as artist or cast information, format, description, playing time, price, subtitles, and so on.

3.3 DRM Scheme Stakeholders

Figure 1 illustrates the basic components of DRM architec-

[†]The message is assumed hashed before signing.

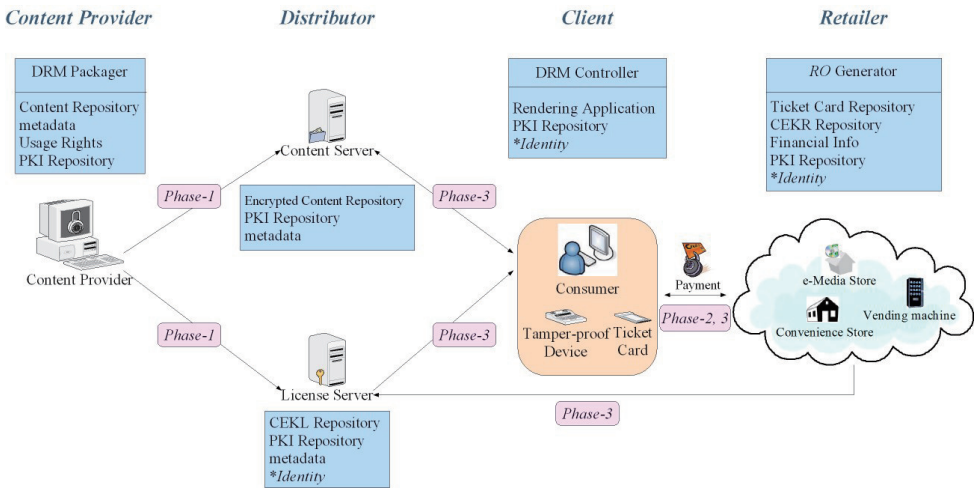

Fig. 1 The proposed DRM reference architecture.

ture. There are four main roles in the proposed scheme. They are content provider, distributor, retailer and client. We will define them as follows:

3.3.1 The Content Provider

The content provider is an entity such as a book publisher, music company or movie studio which releases digital content and inherently own the rights to that media. Because they own the content, they also dictate the way the content can be used. They also provide supplementary data complementing the digital content they release in the form of *metadata*. We consider the content provider as a trusted role in our model.

3.3.2 The Distributor

The distributor is responsible for storing the protected contents and associated usage rules uploaded by the content provider and delivering this content to satisfy consumer requests. Based on authority granted by the content provider, the distributor may grant part of content encryption key to the consumer for using the content. The distributor consists of two types of servers which are the content server and the license server.

- The content server is in charge of dealing with protected contents uploaded by the content provider. It also delivers the digital content to the consumer according to client requests.
- The license server manages the licenses for the digital content. It grants licenses according to the usage rules set by the content provider. Usage rules consist of device information and *metadata*. According to the usage rules established by the content provider, the license server generates *RO* which contain the terms and conditions related to usage of the content. There are diverse usage rules like expiration date, starting date, ending date, playback counts and device types.

3.3.3 The Client

The client is a combination of the consumer and a media device. The device is assumed to be trusted and tamper-proof. The consumer operates this device utilizing a secure platform which is able to download protected content and obtain a license from the distributor to use that content. Licenses are granted based on remittance according to the business model of the content provider and distributor. Using a ticket card for the authentication process, the device will obtain a *RO* which grants permission to play digital content. The user will then be able to use the digital content according to the associated usage rules enforced by the DRM client controller. The purpose of the ticket card is to hold value to exchange for the usage rules granted in the form of a *RO*. It contains pre-shared keys in order to allow the client device to be authenticated by the retailer.

3.3.4 The Retailer

A payment procedure is supported by our model. In the proposed scheme, the ticket card may contain tokens for the device to get usage rules. Consumers can purchase ticket cards from retailers such as electronic or e-media stores, convenience stores or vending machines. Both anonymous and identity based ticket cards can be sold to consumers. Consumers can also reuse the ticket card by recharging it with additional value.

3.4 The Proposed DRM Process Flow

The proposed DRM model employs a ticket card to redeem a content license without revealing user identity. Due to the un-traceability of the ticket card, knowledge of issued usage rules does not provide ability to identify the user yet can still support license revocation. The following is a description of the three phases (upload, purchase, play) involved in providing content to the client. The notation for describing the

Table 1 Notations of the proposed DRM model.

Name	Description
CEK	symmetric content encryption key
$CEKL$	portion of CEK, belonging to L
$CEKR$	portion of CEK, belonging to R
$E_K(*)/D_K(*)$	encrypt/decrypt * with key K
C	ID of content server
L	ID of license server
P	ID of content provider
R	ID of retailer
T	ID of ticket card
i	ID of digital content
IP	Internet Protocol address
K_1, K_2	symmetric key pre-shared by R, T
K_3, K_4	calculated *nonces*
M	unencrypted digital content
m	*metadata* associated with the M
Payment	digital payment
PuK_C/PrK_C	public/private key of C
PuK_L/PrK_L	public/private key of L
PuK_P/PrK_P	public/private key of P
PuK_R/PrK_R	public/private key of R
PuK_T/PrK_T	public/private key of T
r_1, r_2	random secret generated by T, R
Region	regional code, belonging to DRM device
RO_i	rights object of digital content ID i
UR_i	usage rule of digital content ID i

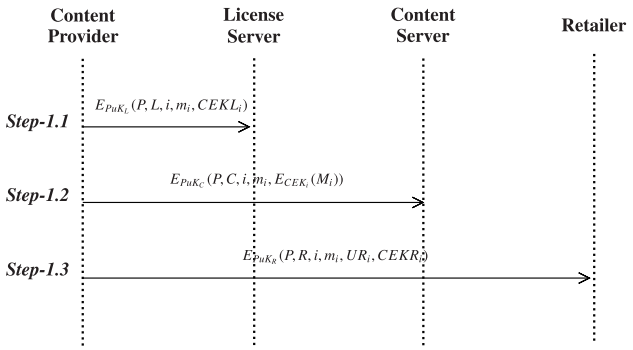

Fig. 2 Upload phase.

detailed process flow is provided in Table 1.

3.4.1 Upload Phase

In this phase, raw content will be encrypted with a portion of the Content Encryption Key (CEK) then uploaded by the provider to the content server. Also, the content provider will upload the usage rules to the license server which is responsible for generating the content license as a response to client requests. Figure 2 illustrates the upload phase and its related flows of steps. The content provider generates the necessary parameters for the corresponding digital content, including M, m, $CEKL$, and $CEKR$. In real implementations, the distributor's servers may be controlled by separate entities. More importantly is that these entities may be malicious or compromised.

To prevent damage from this situation, we divide the full content encryption key CEK into subkeys $CEKL$ and $CEKR$ which can be sent separately to the license servers and the retailer. If one of the servers is malicious, the separation of subkeys keeps any one party from getting the entire content encryption key. Since CEK is split into two subkeys, effective CEK strength relies on the strength of the individual subkeys. Selection of suitable subkey strength can ensure an adequate level of security. Subkey security may be influenced by division method. However, selecting a suitable symmetric encryption method that is not weak towards partial key exposure (such as AES) would mitigate this issue.

The communication steps below rely on PKI for secure transfers.

- *Step-1.1*: The content provider encrypts its own ID P and the ID of the license server L along with the *metadata* m, the content ID i and a portion of the content encryption key $CEKL$ with the public key of the license server, and then sends it to the license server.
- *Step-1.2*: The content provider sends encrypted content containing P, C, $E_{CEK}(M_i)$, m, and i all encrypted with the public key of the content server.
- *Step-1.3*: The content provider encrypts the P, R, i, *metadata* m and a portion of the content encryption key $CEKR$ with the public key of the retailer, and then sends it to the retailer.

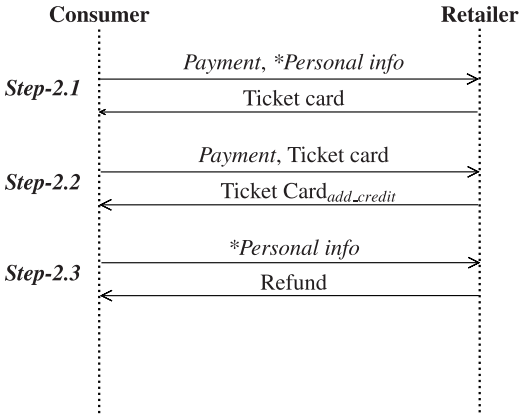

Fig. 3 Purchase phase.

3.4.2 Purchase Phase

This step describes physical interaction between the consumer and a retailer to obtain a ticket card. The ticket card is a token holder for the client device. There are two roles in this phase, the client and the retailer. Whether the ticket card is implemented as anonymous or registered, the consumer can add value to it and use it to obtain the RO and the corresponding CEK from information provided by the license server and retailer. The steps of the purchase phase are illustrated in Fig. 3.

- *Step-2.1*: The consumer buys the ticket card from the retailer via some form of payment. Depending on

the consumer requirement, the registration procedure is optional. The consumer can either choose to provide their identity information for ticket card registration, or they can elect to purchase it anonymously. However, if the consumer chooses anonymity, they will not be able to ask for refund service in case of loss since there is no way to determine the original purchaser.

- *Step-2.2*: A consumer adds value to the ticket card through payment.
- *Step-2.3*: If the consumer has lost their ticket card, they may ask the retailer for refund service by providing personal identification. Once refunded, the ticket card ID will be added to the revocation list by the retailer, preventing future access to the *RO*.

3.4.3 Play Phase

This phase is based on the Universal Electronic Payment System [31] scheme that builds a chain of trust between the communicating parties. U.E.P.S. builds this trust by encrypting messages with information from the previous message so each message doubles as a authenticator for all preceding. This scheme is particularly well suited for smart cards because required computation power is relatively low. Four roles are involved in the play phase, including the content server, the license server, the retailer and the client.

The play phase is divided into four steps. First, the consumer inserts the ticket card into the device, and downloads the desired DRM content. The content server checks if i is valid. If the content ID passes the check, the consumer downloads the desired DRM content freely from the content server via network. In order to have the right to decrypt and play the content, the device requires the *RO* and the complete CEK. So the device authenticates with the retailer. The retailer checks if the ticket card ID is not in the retailer's revocation list and grants authentication. The client can then requests rights to the content by sending various parameters. The retailer responds with the *RO* associated with the desired content to the client. Lastly, the retailer sends a message to the license server and in response the license server sends information including $CEKL$ to the client. Notice the CEK has been separated into two parts, which are held by separate parties to satisfy the trust concerns detailed in Sect. 2. This prevents use of the content by unauthorized parties. The communication in the steps 3.1 and 3.2 are secured by a modified U.E.P.S. scheme and the last step utilizes PKI. Figure 4 illustrates the steps of the play phase:

- *Step-3.0*: The client sends the request and downloads encrypted DRM content $E_{CEK}(M)$ and its corresponding *metadata* from the content server. The *metadata* is signed by the content server's private key. The client uses the content server's public key to verify the the identity of the content server.
- *Step-3.1*: To play the protected DRM content, the client looks up the license acquisition URL and sends the request to the retailer for the corresponding *RO*. The client device sends the ticket card ID in the clear, along with the ticket card ID, the retailer ID and a random number r_1 encrypted first with K_2 and then with K_1. The retailer checks the ticket card *RL* and rejects further interaction with the client if the ticket card is revoked. Since the retailer sold the ticket card, it can easily derive the secret keys K_1 and K_2 from its repository according to the ticket card ID. After receiving the message, the retailer uses K_1 and K_2 to decrypt it and matches the information to confirm the ticket card and retailer ID are correct, then uses the subportion of the message encrypted with K_2. The first 56 bits of this ciphertext $E_{K_2}(T, R, r_1)$ becomes K_3. The retailer then sends the retailer ID, the ticket card ID and another random number r_2 encrypted with K_3 then K_1. Similarly, the client device can easily derive K_3 from $E_{K_2}(T, R, r_1)$ and then decrypts the message from the retailer.

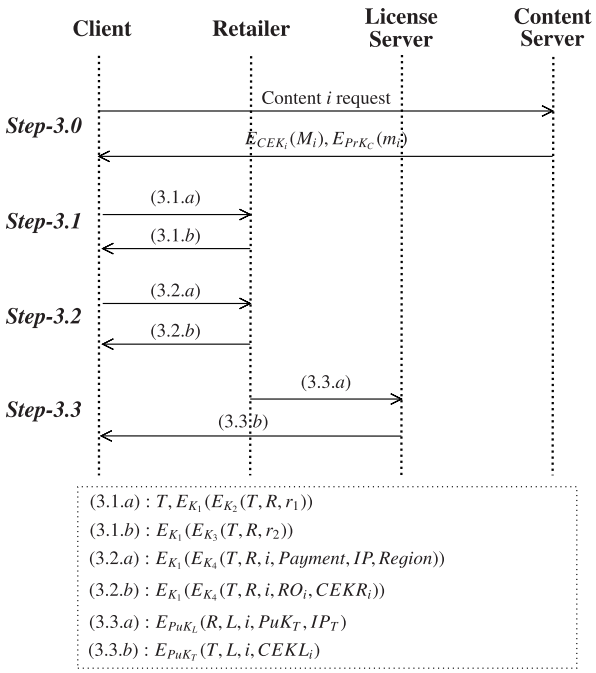

Fig. 4 Play phase.

- *Step-3.2*: The device confirms that T and R are correct and uses 56 bits of the ciphertext $E_{K_3}(T, R, r_2)$ to become K_4. The client device then sends the retailer the card ID, the retailer ID, content ID, the payment, IP address and regional code first encrypted by K_4 then K_1. The retailer use the same method to generate K_4 and uses it and K_1 to decrypt the message from the client device. After checking, the retailer sends the ticket card ID, retailer ID, the digital content ID, the *RO* and a portion of the complete encryption key $CEKR$ encrypted by K_4 then K_1 to the client device.
- *Step-3.3*: The retailer forwards the client request to the license server for the other half of the content encryption key. The retailer's message includes the license

server ID, the retailer ID, the content ID, the public key of the ticket card and the client IP address, all encrypted with the public key of the license server. After receiving the request, the license server uses the public key of the ticket card to encrypt the ticket card ID, the license server ID, the content ID and the content encryption key portion $CEKL$ along with its signature to send to the client device. The client will then be able to assemble the complete CEK to decrypt and play the digital content according to rules dictated by the *RO*.

The computing power and energy resources of the client device may be limited. Notice the client only performs one asymmetric cryptographic action during the play phase. So our model aims for efficiency by minimizing the computing effort of the client device while still providing adequate protection against attackers and malicious servers.

4. Discussions

In this section, we compare our proposed DRM system with several related works and detail the capabilities of the proposed scheme. Following, we provide a security analysis for this scheme.

4.1 Framework Capabilities and Contributions

A comparison between the proposed scheme and several significant DRM systems including Microsoft's DRM system [8] and the OMA DRM system [9] is given in Table 2. Our scheme also addresses more issues compared to other DRM schemes including Conrado et al.'s [18], Lee et al.'s [32], Sun et al.'s [19] and Chen's [11] DRM systems. This model provides great flexibility to accommodate various types of trust inter-relationships. We can see the proposed ticket card based scheme compares favorably to other DRM systems. The following are the achievements of the proposed work.

4.1.1 Anonymous Consumption

During the license acquisition, a consumer's private information is easily revealed through the authentication process. DRM systems can provide a mechanism to protect the consumer's privacy. The ticket card is a substitute for identity which allows the consumer to decide to keep their privacy or not. By using an anonymous ticket card, the retailer cannot correlate consumption of media with an identity. It also allows consumers to give the ticket card as a gift.

4.1.2 Portability

As mentioned in Sect. 2, a DRM system can be divided into two categories of authentication: device based and identity based. Device based DRM systems authenticate the identities of devices, rather than individuals. The simplest way to identify a device is by putting a unique serial number in it. However, when a consumer wants to use digital content on different devices, they must acquire new licenses for every device to enable content consumption. This is inconvenient for consumers to use these types of DRM systems. On the other hand, identity based DRM systems provide a way to solve the issue concerning portability. As long as identity can be determined, they can access content anytime, anywhere, and on any compliant device. Portability is provided in our model by tying usage rules to a ticket card instead of a device freeing the restriction of only being able to use specific devices. This provides identity based DRM benefits without necessarily disclosing privacy related information.

4.1.3 Trust Issue

In a real DRM implementation, various parties are usually controlled by different business entities allow the possibility of one party taking advantage of the other. Separation of duties is designed into the framework to provide the advantage of not explicitly requiring trust between the stakeholders since it is possible these servers may be malicious. In traditional DRM schemes, any malicious server has access to the entire content key and this could lead to abuse of the commercial model. To overcome this problem, the proposed scheme employs the concept of split key where the content key is divided into two parts named $CEKL$ and $CEKR$ which are held by different business entities. They are encrypted with the public key of license server and the retailer, respectively. In addition, a malicious retailer may

Table 2 Comparison to other DRM systems.

	Conrado et al. [18]	Lee et al. [32]	Sun et al. [19]	Chen [11]	Microsoft [8]	OMA [9]	Our DRM system
Technology*	*S*	*S*	*S*	*D*	*D*	*D*	*S*
Roles involved **	*P, U*	*C, L, R, U*	*C, L, U*	*C, L, P, U*	*C, L, U*	*C, L, U*	*C, L, P, R, U*
Encrypted content	No	Yes	Yes	Yes	Yes	Yes	Yes
Anonymity	Yes	Yes	Yes	No	No	No	Yes
Portability	Yes	Yes	Yes	No	No	No	Yes
Trust issue	No	No	No	No	No	No	Yes
Smart card features***	Basic	Basic	Basic	N/A	N/A	N/A	Advanced

*S: Smart Card based, D: Device based
**C: Content server, L: License server, P: Content provider, R: Retailer, U: User
***Basic: Anonymity and Portability
Advanced: Basic functions with additional ticket card assistance features (Sect. 4.1.4)

be able to impersonate the consumer since he has K_1 and K_2. In our model, the license server is aware when a license has been granted since it has to provide the corresponding $CEKL_i$. Even when a retailer masquerades as a client to obtain the full CEK, it is still tied to an individual tamper-proof device. So the license server will charge the retailer regardless which renders this attack without benefit.

4.1.4 Ticket Card Assisted Features

By exploiting the functionalities that ticket cards afford our scheme, the proposed system gains the following capabilities:

- As a rule, consumers are not implicitly trusted. A malicious consumer may attempt to gain access to content he/she is not entitled to. Revocation is integrated into the proposed scheme to protect against fraud from malicious consumers. A accumulated revocation list containing canceled ticket cards is available for retailers to reference. If a ticket card is on the revocation list and requests digital content, the authentication process in the *Step-3.1* will prevent the invalidated ticket card from retrieving any rights object.
- Previous DRM schemes do not account for lost or stolen licenses. Once lost, they are unrecoverable. However, lost ticket cards do not pose a problem for the proposed DRM scheme. Once a ticket card is reported lost and the identity of the owner established, the missing ticket card is added to the revocation list by the retailer. Consequently, a new ticket card is reissued to the registered owner.
- In order to preserve the commercial viability of the content providers, the regional codes are supported in the proposed scheme. During the play phase, the regional code belonging to the device is attached to the authentication message and submitted by the client device during the process of obtaining rights. The design provides great flexibility to the DRM business model. The consumer can carry a ticket card and play the digital content anywhere according to commercial rules. For example, due to the regional restrictions, digital content may not be used in a certain geographical area, but can obtain usage permissions after moving to another area.

4.2 Security Analysis

This research proposes a multi-functional DRM system which is suitable for realistic DRM system implementations to protect digital rights. We now discuss the security criteria for our scheme.

- *Smart card security.* The PuK_T/PrK_T key pair and random numbers r_1/r_2 are paramount in ensuring the security of the ticket card. Since ticket cards are based on smart cards, the maturity of smart card technology can provide protection mechanisms to prevent attackers from compromising information contained within. Hence, these secrets can only be accessed by authorized functions of the ticket card. Even in the case where a ticket card is stolen, the attacker will not be able to access the secret information since the RO, CEK and protected digital content are stored on a tamper-proof device. In addition, whether the smart card is registered or anonymous, an additional authentication check such as a PIN code-like mechanism may be employed to prevent unauthorized access of ticket card.
- *Authentication.* In a DRM business model, it is necessary to ensure that transactions are genuine and messages are generated by legitimate senders. Authentication of messages is provided by digital signature of the sender and the corresponding CA certificate. These mechanisms ensure that outsiders are not able to send forged messages to DRM members. Also, the adoption of U.E.P.S. based communication protocol provides authentication to the communication. In the play phase, a malicious 3*rd* party retailer cannot mislead a device to log into its system without secret keys K_1 and K_2. In *Step-3.1*, when receiving the initial request from the client, the retailer has to decrypt the message and then generate the next secret key K_3.

$$R : D_{K_2}(D_{K_1}(3.1.a)) = \{T, R, r_1\}, \tag{4}$$

$$K_3 = E_{K_2}\{T, R, r_1\}_{56bits} \tag{5}$$

  Since an imposter cannot derive the K_3 (which is *required* to generate the response), the login process will be terminated by the client device. Similarly, when the client sends requests, it has to provide its ID and use the corresponding keys K_1 and K_2 which are issued and stored by the retailer. They can easily authenticate each other since they have a pre-shared secret. For communications between the retailer and the license server, PKI technology is used to validate that all parties involved are actually who they claim. This works because only the true entity has the secret keys required to decrypt the messages intended for them.
- *Confidentiality.* The primary goal of cryptography in DRM is to maintain confidentiality by preventing unauthorized duplication or access to the digital content. Before distributing the raw content, the content provider encrypts it with the CEK.

$$P \longrightarrow C : E_{CEK_i}\{M_i\} \tag{6}$$

  This maintains the confidentiality of the content during distribution. To prevent in-transit disclosure of the CEK, it is separated into two parts, $CEKL$ and $CEKR$ by the content provider and passed to separate entities only to be reassembled at an authorized client device. The separated CEK makes sure neither the license server nor the retailer can obtain the entire CEK. According to Fig. 4, when the $CEKL$ and the $CEKR$

are transmitted over the internet, they are encrypted by K_1 and PuK_T respectively. This ensures only a client with the correct ticket card will be able to decrypt it.

$$C : D_{K_4}(D_{K_1}(3.2.b)) = \{T, R, i, RO_i, CEKR_i\}, \quad (7)$$

$$D_{PrK_T}(3.3.b) = \{T, L, i, CEKL_i\} \quad (8)$$

Consequently, the proposed scheme can provide confidentiality against malicious servers or clients.

- *Integrity.* Integrity signifies that data cannot be modified undetected. Each participating device in the proposed scheme employs PKI technology using a certificate, a public key and the corresponding private key. Transmitted messages are always secured for the receiving entities by encrypting it with keys to make sure it cannot be modified un-detectably. When receiving the CEK, the TPD can ensure the integrity property against any unauthorized manipulation.
- *Access control.* Access control in this scheme is achieved through encryption and PKI. The client is prevented from accessing the digital content by the tamper-proof DRM device until they can obtain the CEK and a *RO* with appropriate rights for that content.
- *Non-repudiation.* A sender should not be able to deny transmission of messages. In the designed protocol, one can easily check the receiving message using the sender's signature. This implies that all parties of transactions cannot deny participating afterwards since the sending and receiving of transaction messages cannot be refuted.
- *No temporal restrictions.* Traditional authentication processes require the clocks of the client and the retailer to be synchronized with each other and the transmission delay time of messages is also limited. To eliminate this restriction, our scheme is based on *nonces* instead of timestamps. Therefore, the proposed DRM implementation has no requirements of clock synchronization or delay time limitations while still providing a suitable level of security.
- *Privacy.* The proper balance between content provider and consumer privacy is a significant challenge in any DRM system. Not only does this model protect consumer privacy from outsiders, the adoption of the ticket card plays the key role in protecting the privacy of the consumers from the service provider. The designed protocol provides the means to adhere to privacy laws against disclosing customer information since all end-to-end data transmissions are protected under security mechanisms.
- *Replay attack prevention.* Replay attacks occur when valid data transmissions are maliciously or fraudulently repeated. If an attacker collects transmission messages to masquerade as a valid client, they still cannot imitate the client completely. In *Step-3.1*, even if an attacker replays the entire message originally sent by the valid client, the attacker still is not able to decrypt the response generated from the retailer.

$$C : \{T, R, r_2\} = D_{K_3}(D_{K_1}(3.1.b)) \quad (9)$$

Since the attacker does not have the pre-shared keys, they do not have K_1 to decrypt the $(3.1.b)$ and then derive the K_3. Thus, attackers will not be able to derive the random secret r_2 generated by the retailer. The same situation happens in *Step-3.2*, even the attacker can replay $(3.2.a)$ to the retailer, he still does not have enough information to decrypt $(3.2.b)$ to obtain the *RO* or $CEKR$. Similarly, the attacker cannot impersonate the retailer since they lack the necessary secrets to accomplish the mutual authentication protocol.

5. Conclusions

In this paper, we propose a trust distributed DRM model based on ticket cards which can provide anonymous consumption and other capabilities. By utilizing the U.E.P.S. protocol, this scheme realizes secure authentication, flexibility, efficiency and practicability for the DRM implementation. Furthermore, a security analysis shows how the system adheres to the tenets of best practices as they apply to different aspects of the system.

Acknowledgment

This paper is dedicated in memory of Chi-Sung Laih, who was Teacher, Advisor, Friend and inspiration to members of his research group. His passion for research lives on in his students. He is sorely missed.

References

[1] P.S. Graham, "Intellectual preservation and electronic intellectual property," Proc. Technological Strategies for Protecting Intellectual Property in the Networked Multimedia Environment, Interactive Multimedia Association, Jan. 1994.
[2] "Webopedia: Digital rights management." http://www.webopedia.com/TERM/D/DRM.html
[3] "Openmhp." http://www.openmhp.org/
[4] E. Diehl, "A four-layer model for security of digital rights management," Proc. 8th ACM workshop on Digital rights management, pp.19–28, 2008.
[5] D. Kundur, C.Y. Lin, B. Macq, and H. Yu, "Special issue on enabling security technologies for digital rights management," Proc. IEEE, vol.92, no.6, pp.879–882, June 2004.
[6] M. Stamp, "Digital rights management: The technology behind the hype," J. Electronic Commerce Research, vol.4, no.3, 2003.
[7] "Intertrust." http://www.intertrust.com/
[8] "Ms-drm: License protocol specification." http://msdn.microsoft.com/en-us/library/cc227964.aspx
[9] "Oma." http://www.openmobilealliance.org/
[10] H. Park and J. Kim, "Copyright protection for modifiable digital content based on distributed environment," IEICE Trans. Inf. & Syst., vol.E91-D, no.5, pp.1390–1397, May 2008.
[11] C.L. Chen, "An "all-in-one" mobile drm system design," International Journal of Innovative Computing, Information and Control, vol.6, no.3A, pp.897–911, March 2010.
[12] D. Alessio and M. Joye, "A simple construction for public-key encryption with revocable anonymity: the honest-sender case," Proc. Nineth ACM Workshop on Digital Rights Management, pp.11–16, 2009.

[13] J.B. Lotspiech, "Broadcast encryption versus public key cryptography in content protection systems," Proc. Nineth ACM Workshop on Digital Rights Management, pp.39–46, 2009.
[14] Q. Liu, R. Safavi-Naini, and N.P. Sheppard, "Digital rights management for content distribution," Proc. Australasian Information Security Workshop Conference on ACSW Frontiers, pp.49–58, 2003.
[15] R. Song and L. Korba, "Pay-tv system with strong privacy and non-repudiation protection," IEEE Trans. Consum. Electron., vol.49, no.2, pp.408–413, May 2003.
[16] S. Palavalli, U.S. Srinivas, and A.R. Pais, "Identity based drm system with total anonymity and device flexibility using ibes," Proc. High Performance Computing & Simulation Conference, 2008.
[17] "Project dream," https://dream.dev.java.net/
[18] C. Conrado, F. Kamperman, G. Schrijen, and W. Jonker, "Privacy in an identity-based drm system," Proc. 14th International Workshop on Database and Expert Systems Applications, pp.389–395, Sept. 2003.
[19] H.M. Sun, C.F. Hung, and C.M. Chen, "An improved digital rights management system based on smart cards," Proc. Inaugural IEEE-IES Digital EcoSystems and Technologies Conference, pp.308–313, Feb. 2007.
[20] K. Fujita and Y. Tsukada, "An analysis of interoperability between licenses," Proc. 10th Annual ACM Workshop on Digital Rights Management, pp.61–72, 2010.
[21] P.A. Jamkhedkar, G.L. Heileman, and C.C. Lamb, "An interoperable usage management framework," Proc. 10th Annual ACM Workshop on Digital Rights Management, pp.73–88, 2010.
[22] B.N. Park, J.W. Kim, and W. Lee, "Precept: A privacy-enhancing license management protocol for digital rights management," Proc. 18th International Conference on Advanced Information Networking and Applications - vol.2, p.574, 2004.
[23] B.N. Park, W. Lee, and J.W. Kim, "A license management protocol for protecting user privacy and digital contents in digital rights management systems," IEICE Trans. Inf. & Syst., vol.E88-D, no.8, pp.1958–1965, Aug. 2005.
[24] J. Zhang, B. Li, L. Zhao, and S.Q. Yang, "License management scheme with anonymous trust for digital rights management," Proc. IEEE International Conference on Multimedia and Expo, p.4, July 2005.
[25] U. Greveler, "Enforcing regional drm for multimedia broadcasts with and without trusted computing," in Digital Rights Management. Technologies, Issues, Challenges and Systems, ed. R. Safavi-Naini and M. Yung, Lect. Notes Comput. Sci., vol.3919, pp.332–340, Springer Berlin / Heidelberg, 2006.
[26] Y. Jeong, K. Yoon, and J. Ryou, "A trusted key management scheme for digital rights management," ETRI J., vol.27, no.1, pp.114–117, 2005.
[27] J. Kim, Y. Jeong, K. Yoon, and J. Ryou, "A trustworthy end-to-end key management scheme for digital rights management," Proc. 14th Annual ACM International Conference on Multimedia, pp.635–638, 2006.
[28] M.K. Sun, C.S. Laih, H.Y. Yen, and J.R. Kuo, "A ticket based digital rights management model," Proc. IEEE 6th Consumer Communications and Networking Conference, pp.1–5, Jan. 2009.
[29] W. Rosenblatt, W. Trippe, and S. Mooney, Digital Rights Management - Business and Technology, M & T Books, 2002.
[30] S. Subramanya and B. Yi, "Digital rights management," Potentials, IEEE, vol.25, no.2, pp.31–34, March-April 2006.
[31] R.J. Anderson, "Ueps - a second generation electronic wallet," European Symposium on Research in Computer Security, pp.411–418, 1992.
[32] W.B. Lee, W.J. Wu, and C.Y. Chang, "A portable drm scheme using smart cards," J. Organizational Computing and Electronic Commerce, vol.17, no.3, pp.247–258, 2007.

Ming-Kung Sun received his B.S. degree in 2001 from Chinese Culture University and his M.S. degree from the Southern Taiwan University in 2003. He is currently working toward his Ph.D. degree in the Institute of Computer and Communications Engineering at National Cheng-K ung University. His research interests include cryptography, network security and wireless networks and digital rights management.

Michael Chang graduated with a degree in Computer Science from the University of Pittsburgh in 1998. Recently, he completed his Masters degree in Electrical Engineering from the Institute of Computer and Communications Engineering of National Cheng-Kung University under Chi-Sung Laih and H.T. Lin. Michael's research interests include practical aspects of Computer and Network Security and finding a fine but accessible Beaujolais in Taiwan.

Hsiao-Ching Lin received his B.S. degree from Yuan Ze University, Taoyuan, Taiwan in 2004, and the M.S. degree from National Kaohsiung University of Applied Sciences, Kaohsiung, Taiwan in 2006. Now he is a graduate student at the National Cheng Kung University (NCKU) pursuing a Ph.D. in EE. His current research interests include cryptography, web application security and MANET.

Chi-Sung Laih received his BS, MS, and Ph.D. degrees all in electrical engineering form National Cheng-Kung University (NCKU) in 1984, 1986, and 1990, respectively. During 1995-2010, he was a professor in the Department of Electrical Engineering at NCKU, located in Tainan, Taiwan. He was the chairman in many international conferences or work-shops, including the general chair in the International Workshop on Applied PKI (IWAP) 2002, program chair in the Asiacrypt 2003 and general chair in the International Systematic Approaches to Digital Forensic Engineering (SADFE) 2005. His research interests include cryptology, information security, error control codes and communication systems.

Hui-Tang Lin received B.S. degree in Control Engineering from National Chiao-Tung University, Taiwan, in 1989, the M.S. and the Ph.D. degrees both in Electrical Engineer-ing from Michigan State University, East Lansing, MI, in 1992 and 1998, respectively. He is currently an associate professor at the Electrical Engineering Department and the Computer and Communication Institute of National Cheng-Kung University, Taiwan. His research interests include QoS of high-speed networks, optical networks, switch architecture, wireless net-works, sensor networks, and network security.