# A Proposal on Open DRM System Coping with Both Benefits of Rights-Holders and Users

Akiko Seki
Graduate School of Global Information and Telecommunication Studies, Waseda University
Tokyo, Japan
Email: akiko@ruri.waseda.jp

Wataru Kameyama
Graduate School of Global Information and Telecommunication Studies, Waseda University
Tokyo, Japan
Email: wataru@waseda.jp

***Abstract*— This paper proposes a rights management processing system which is independent from any usage environments and enables flexibility, re-using, and redistribution of contents with the rightful consent between right-holders and users. An implementation is also shown to evaluate both the secureness and flexibility of the proposed system, as well as the comparison with other existing systems.**

## I. Introduction

While digital rights management (DRM) systems are needed for contents distribution services, the present contents distribution systems are in closed environments that generally involve limited number of rights-holders, where the contents and the right information are severely managed by rights-holders. In such environments, contents are distributed one-way from rights-holders to users, and users can not provide their contents to the contents market. Moreover, it is difficult to get rights information of contents, and users cannot process rights for re-use and re-distribute of contents. In future contents distribution environments, many users will create and distribute contents to networks with improvement of digital contents creating technologies and networks. In such situations, the contents distribution should be bi-directional flow among rights-holders and users. In this bi-directional contents distributing environment, a user may become a rights-holder, and vice versa.

For this reason, an open DRM system is desired, which respects the safe distribution of contents, the positive rights-processing, and the open of the market to users. In an open DRM system, everyone may enable to provide their contents in a safe way, and to set rights information of these contents. In this sense, this paper proposes a new DRM system to achieve the open rights management as mentioned above. The goal of this system is to provide an infrastructure to facilitate the distribution of contents under a rightful consent between rights-holders and users.

## II. Overview of Proposed System

The proposed system has the following four features in order to enable rightful and smooth use of contents.

### A. Open Management of Rights Information

The existing DRM systems such as broadcasting system and DVD system [1], provide contents in limited usage conditions and usage environments. These DRM systems don't open rights information of contents, make these information closed, and manage them by themselves. Many Web contents don't open their rights information, either, since it is difficult to find out such rights information of contents and hard to get consent to reuse or redistribution of them. For this reason, to enable a smooth rights-processing and a smooth use of contents, every contents should open their rights information to everyone.

In addition, as many existing DRM systems lack interoperability, users have to use different DRM systems depending on contents providers. Therefore, in the proposed system, the rights information is described in an XML-based language, i.e. the eXtensible rights markup Language (XrML) [2], in the form which can be processed by any systems. Anyone enables to describe rights information easily, and they are distributed in the open format. By this, rights information can be processed independent from platforms, and users are enabled to get and to see distributed rights information anytime easily.

### B. Flexible Contents Use

As for the many existing DRM systems which put weight on right protection of a rights-holder, flexibility of contents use like free contents and private use under rightful consent are not possible. In the proposed system, a rightful user has a License Certificate File, which is created after a rights-processing and manages usage consent of users. By using a License Certificate File, a rightful user enable to use purchased contents, except for pay-per-view contents, for private use, such as copy, move, edit, etc., without making additional rights-processing and the application of consent. A License Certificate File is possible to identify the rightful user with appropriate usage consents. Therefore, only the rightful user can use purchased contents.

### C. Flexible Rights Processing

The existing DRM systems manage rights information and contents in the service provider's databases. And users access this database to do rights-processing when they purchase contents as in the Copymart model which is proposed to realize a smooth rights transaction [7]. These systems are suitable for strict management of rights, but they need some cost for managing them, and the user mobility is rather ignored. So, in the proposed system, a user has all rights-processing

functions locally, in an Open DRM System, such as the functions of a rights-processing, a protecting of contents, and a decryption of contents. And, it generates a different key for each content, which is used by contents protection and unprotection. Therefore, a contents provider does not need to manage rights information, contents, and cipher keys. A user receives License File and contents, as inputs to a local Open DRM System which performs rights-processing and generates a cipher key. Therefore, a user does not need to access the contents provider's database at the time of using contents.

### *D. Flexibility of Secondary Contents Use*

For smooth distribution of contents, a DRM system requires to enable distribution of original contents safely and smoothly, as well as to enable the secondary use of contents under rightful consents. The Superdistribution model in [4] and [5] has been proposed to realize the former, and the IntelligentPad model [8] and Transcopyright model [3] have been proposed to realize the latter. However, these models are not taking account of secondary contents or derived contents distribution for private use.

In the proposed system, a user is possible to create secondary contents as for private use and to distribute it. When such secondary contents or derived contents are distributed to other users, they cannot use it without rights-processing, however, the secondary contents can be used if a receiver does the rights-processing to original contents and gets rights to view them. A secondary contents creator may also distribute the secondary contents after rights-processing for re-distribution, under rights information in a License File.

The proposed system is possible to divide, merge, and transfer rights. Therefore, a secondary contents creator can turn into a new rights-holder of the secondary contents. And, a user is possible to do some partial rights-processing when a user wants to listen to only a music of compound contents that are composed of music, images, and texts. Moreover, a purchased content is possible to transfer to an other user with License Certificate File.

## III. SYSTEM DETAILS

### *A. Concept of Proposed System*

Fig.1 depicts the conceptual diagram of the proposed system. At the time of providing contents (Fig. 1. a), the contents owner inputs contents and the rights information into the DRM system. Then, the system outputs protected contents and License Files describing the right information associated with the contents. And at the time of the first use (Fig. 1. b), a user inputs the protected contents and its License File into the DRM system. the system performs rights-processing, then reproduces contents and outputs License Certificate File describing the usage consent of contents. At the time of the use after the rights-processing (Fig. 1. c), a rightful user inputs this License Certificate File instead of License File, then contents can be used without additional rights-processing.

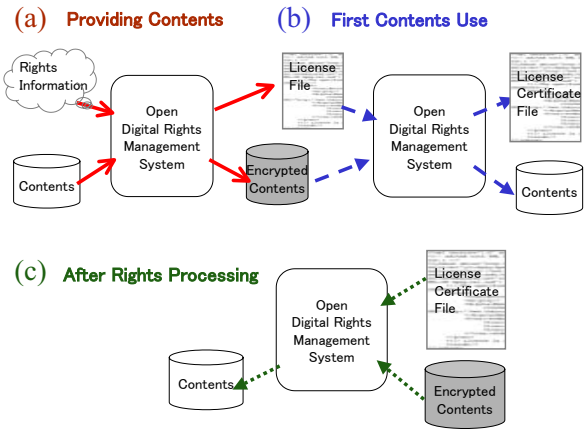


Fig. 1. The Processing Flow of Open DRM System

### *B. System Architecture*

This system is designed to allow users to use and reuse contents under rightful consents among rights-holders and users, in order to manage various usage conditions of contents, and to replay contents even in different equipments and locations. Fig.2 shows the proposed system architecture. As this system is to enable the offline rights-processing, rights-processing functionalities are embedded in user equipments.

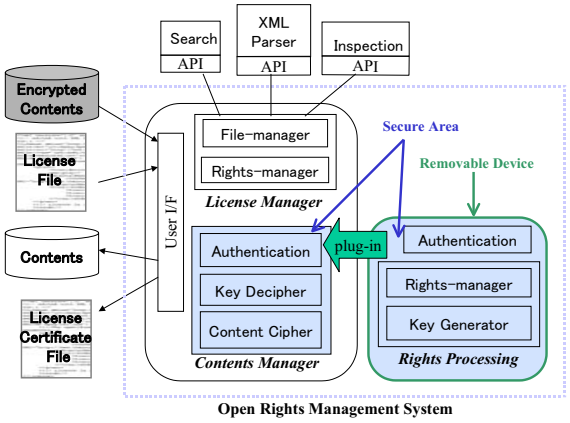


Fig. 2. Open DRM System Architecture

### *C. License File*

The License File describes right information, such as Content ID, rights-holders information, creator's information, purchasing conditions, several usage conditions, etc. These informations are important for rights-holders and need to be processed by all DRM systems. Therefore, License File is described in the XML-based digital rights description language, XrML. A License File is exposed and distributed as in the plain format, and it is possible to copy to anyone. The rights-processing is performed based on the rights information described in the License File. If such information is altered, the alteration can be detected in the Open Rights Managements

System by digital signature. The Open Rights Managements System verifies the digital signature using the verification key which is added to contents, and checks the justice of the rights information. For this reason, the License File is highly interoperable. And, any users enable to browse rights information in the License File. So, users of other DRM systems may also enable to get some usage information. Moreover, Content ID is described in a License File, which locates the corresponding content one-to-one basis. Thus the user can search contents based on Content ID described in the License File, and vice versa. Since License Files are distributed independently from contents, users get License Files first, and look for the favorite usage condition, then receive contents. The License Files is prepared not only for pay contents but also for free contents. By doing so, every content can be checked with the usage condition, when a user wants to reuse and redistribute it. Shareware-type contents distributions are also allowed by this model.

### *D. License Certificate File*

The License Certificate File is created by the Open Rights Management System after the first rights-processing. It describes the processed rights information and consent information in the same format as the License File. The processed rights informations are Content ID, consent information of user, a part of content information and rights-holder's information, and the rights-processing conditions chosen at the time of the first rights-processing by user. The consent information, which is an agreed license conditions of a content between a user and a rights-holder, includes licensed user identification and usage conditions, that the user obtains by the first rights-processing.

The License Certificate File is used by the DRM system to confirm the license of a user when the user uses the same contents repeatedly. As the License Certificate File includes the licensed user's identification, it can verify the user's rights in the rights management system. Thus, the system prevents fraudulent use of License Certificate File of others. After the system checks the consent information and the validity of a user, the user can use the content without additional rights-processing. And as a rightful user has a License Certificate File, the user can use of contents for copy, remove, edit, etc. without additional rights-processing. Such secondary contents or derived contents are used by only the rightful user who is the owner of the License Certificate File.

This file may be kept outside of the open rights management system. A user may transfer purchased contents to friends using a License Certificate File. And rights or consents can be divided, exchanged or merged.

### *E. Open Rights Management System*

It consists of four components, User I/F, License Manager, Contents Manager, and Rights Processing as shown in Fig.2. For example, when a user is going to use a protected content of movie, the system searches and retrieves the License File from Content ID in the contents. Then it performs rights-processing with License File and deciphers contents, and shows the contents. The functionalities of these components are detailed below:

- User I/F
  This component passes a request from application or a user to the system. The inputs are Content ID, License File, Contents, License Certificate File, and some user's commands.
- License Manager
  This component has two functions, File-manager and Rights-manager. The File-manager uses some tools' APIs, and searches License Files or Contents, validates the digital signature, and parses the rights information from the License File. The Rights-manager manages rights information. It exchanges rights information and license information between this and the Rights Processing, and it creates a License Certificate File and stores these information to it.
- Contents Manager
  This component manages protection of contents. It protects, unprotects and reproduces contents, and watches the entire use of contents. And it keeps the protected contents even after use of contents. This component has three functions, Authentication, Key Decipher, and Content Cipher. The Authentication exchanges information with the Authentication of Rights Processing to verify the validity of Contents Manager and Rights Processing. The Key Decipher deciphers an encrypted Content Key. And the Content Cipher deciphers or enciphers contents.
- Rights Processing
  This component has tree functions, Authentication, Rights-manager, and Key Generator. The Authentication checks the input data and its signature with verification keys. The Rights-manager does the rights-processing and issues usage consents. And the Key Generator creates Content Key and enciphers the Content Key with Protect Key, which is different for each Rights Processing of a user. Thus this component is built in a secure removable device like a smart card, to enable the user mobility.

### *F. Prototype System*

A prototype system is implemented in order to confirm the proposed system functionalities. The detail of the data processing procedure is described below as well as in Fig.3.

1) User I/F sends user's request.
2) File-manager searches, validates, and parses License File.
3) Return rights information, and the user selects the usage information to process rights.
4) Send the license information to the Rights Processing.
5) Rights-manager of Rights Processing checks usage rule, and clearance of licenses, selects the accounting information and sends it to Accounting.
6) After the complete payment, the Accounting notifies it to Key Generator.
7) Send license information to Key Generator.
8) Generate a Content Key, and enciphers it.

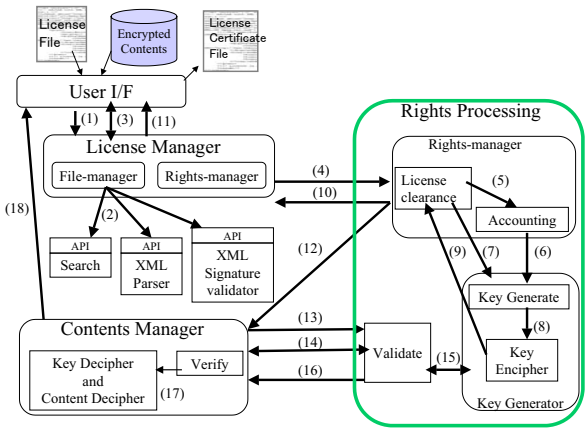


Fig. 3. Prototype System

9) Send back encrypted Content Key by Protect Key.
10) Send back processed rights information, license information, encrypted Content Key, and signature to the License Manager.
11) Create License Certificate File.
12) Send encrypted Content Key.
13) Send request to get Protect Key, with a authenticate signature
14) Both components exchange session keys.
15) Encipher Protect Key with session key.
16) Send back encrypted Protect Key.
17) Decipher encrypted Protect Key with session key, decipher encrypted Content Key with it, and decipher content with deciphered Content Key.
18) Finally the content shows to user's application.

When using rights-processed contents in the above-mentioned Procedure 2, the License Certificate File is used for rights-processing instead of the License File. In the Procedure 5, the Rights-manager in the Rights Processing checks a license information and signatures in the License Certificate File, then the Rights-manager notifies it to the Key Generator, and jumps into Procedure 11. Here, when license information is not valid, rights-processing from Procedure 2 should be performed again with the original License File.

## IV. Management of Content Key

### A. Generating Content Key

The Content Key is generated by Key Generator in the Rights Processing, at the time of protecting of content by contents owners and performing of rights-processing by users. The Key Generator has a key generate function, which has volatile unidirectional function like a SHA-1 algorithm [9]. When a user inputs license data described in the License File, to the Open DRM System, the license data and the common key of Key Generator are inputted to the key generate function, then the Content Key is generated. After that, the Content Key is enciphered with a Protect Key. And the encrypted Content Key is managed in the License Certificate File when the user performed rights-processing.

This license data is including a digital signature of the rights-holder. When a rights-holder generates Content Key for content protection, a rights-holder inputs private key to the Open DRM System to generate a digital signature. The Open DRM System generates digital signature of the rights-holder from a part of rights information, and inputs it to the key generate function. These license data is unique for each contents. Therefore, Key Generator enables to generate various different Content Keys. And, a tampered or a spurious License File does not generate the correct Content Key.

### B. Usefulness of License Certificate File

When a user uses purchased content repeatedly, the user inputs License Certificate File to the Open DRM System instead of License File. The License Certificate File has an encrypted Content Key and license information. The encrypted Content Key is passed to Contents Manager. And the license information is passed to Rights Processing.

The license information consists of two digital signatures to be checked, i.e. a signature of license data and a signature of licensed user. The Rights Processing checks a signature of rights information at the Authentication with verification key. Then, it checks a signature of licensed user with user's private key, and verifies whether a user has rightful License Certificate File. These keys are managed as secret by the Rights Processing, and no one knows these keys. And the user's private key is different for each Rights Processing of user. These are possible because the License Certificate File is used by only rightful owner of this file. After the validation of two signatures, the Rights Processing notifies the validity to the Key Generator. Therefore, this process enables to validate the rightful owner of the License Certificate File and enables to get a deciphered Content Key.

### C. Deciphering of Content Key

At the Contents Manager, it must decipher the encrypted Content Key to use. The Protect Key, which is used to decipher the Content Key, is managed in the Rights Processing. Thus, the Contents Manager needs to get the Protect Key. When the Contents Manager needs to use Content Key, it requests to send a Protect Key to the Rights Processing with a digital certificate. The digital certificate is approved by a certificate authority which might be established as a center by agreement of society. The Authentication of Rights Processing has a validation key, which should be embedded at the time of manufacturing this component. And the Rights Processing validates the digital certificate and signature form Contents Manager. Then, both components exchange a session key, and the Rights Processing enciphers a Protect Key with the session key to be sent to the Contents Manager. The Contents Manager deciphers the Content Key with the Protect Key.

Therefore, the Protect Key can be sent and received between Rights Processing and Contents Manager with a different session key each time generated.

## V. EVALUATION

The features of the proposed system are compared with other five existing system models.

A : Broadcasting System with CAS
B : Superdistribution (Type1) [4], [5]
C : Superdistribution (Type2) [6]
D : Copymart [7]
E : IntelligentPad [8]
F : Proposed System

On the above-mentioned models, the evaluation from viewpoints of users, rights-holders and contents distribution is done as shown in Fig.5, where 1-4 are evaluation categories and each has four sub-categories to be marked either of 0, 1 or 2, from different perspectives of smooth contents distribution, users benefits, and rights-holders benefits, as shown in Fig.4:

1 The environment of rights processing
  1-1) Is the platform provided in hardware or software?
  1-2) Is the network connection needed for rights processing?
  1-3) Is the content purchase limited only to members?
  1-4) Is the rights information managed in a server?
2 The usage condition of content
  2-1) Is the usage environment depending a certain type of hardware?
  2-2) Is the redistribution allowed?
  2-3) Is the private use, as copy, move and edit, allowed?
  2-4) Is the rights information provided for reusing content?
3 The management of safety
  3-1) Is the safety of the system depending on hardware, software, or both?
  3-2) Is the renewal of a system possible?
  3-3) Is the charge of use trustworthy?
  3-4) Is the detail contents distribution informed to rights-holders?
4 The management of rights information
  4-1) Is the right information provided to users environments?
  4-2) Is the variety of right information possible?
  4-3) Is the renewal of rights information possible?
  4-4) Is the rights processing for secondary content possible?

| 1 | | SCD | UB | RHB | 2 | | SCD | UB | RHB |
|---|---|---|---|---|---|---|---|---|---|
| 1-1) | Hardware | 1 | 0 | 1 | 2-1) | Dependent | 0 | 0 | 2 |
| | Software | 1 | 2 | 1 | | Independent | 2 | 2 | 1 |
| 1-2) | Online | 1 | 0 | 1 | 2-2) | Allowed | 2 | 2 | 1 |
| | Offline | 1 | 2 | 0 | | Not allowed | 0 | 0 | 2 |
| 1-3) | Members-only | 0 | 0 | 2 | 2-3) | Allowed | 2 | 2 | 1 |
| | Anyone | 2 | 2 | 0 | | Not allowed | 0 | 0 | 2 |
| 1-4) | Server | 1 | 1 | 2 | 2-4) | Provided | 2 | 2 | 1 |
| | Local | 1 | 1 | 1 | | Not provided | 0 | 0 | 2 |
| 3 | | SCD | UB | RHB | 4 | | SCD | UB | RHB |
| 3-1) | Hardware | 2 | 1 | 2 | 4-1) | Provided | 2 | 2 | 1 |
| | Software | 1 | 1 | 1 | | Not provided | 1 | 0 | 2 |
| 3-2) | Renewable | 2 | 1 | 2 | 4-2) | Possible | 2 | 2 | 2 |
| | Not renewable | 0 | 0 | 0 | | Impossible | 0 | 0 | 0 |
| 3-3) | Trustworthy | 2 | 1 | 2 | 4-3) | Renewable | 2 | 2 | 2 |
| | Not trustworthy | 0 | 1 | 0 | | Not renewable | 0 | 0 | 0 |
| 3-4) | Informed | 2 | 1 | 2 | 4-4) | Possible | 2 | 2 | 2 |
| | Not informed | 1 | 1 | 0 | | Impossible | 1 | 0 | 1 |

Note : SCD: Smooth Contents Distribution, UB: Users Benefits, RHB: Rights-Holders Benefits
0 … poor 1 … fair 2 … satisfactory
Some Intermediate values are used for imperfect functionalities

Fig. 4. Values for Evaluation Categories

From Fig.5, it is apparently that the model D, E and F have many attractive functions for contents distribution. And the evaluation from viewpoints of users and rights-holders shows that the model A and C are unbalanced in both benefits, while the model E and F are well balanced.

Therefore, it can be said that the proposed system has many desirable functions which promote contents distribution and keep the nearly same level of capability against other systems, as well as respecting both users and rights-holders benefits.

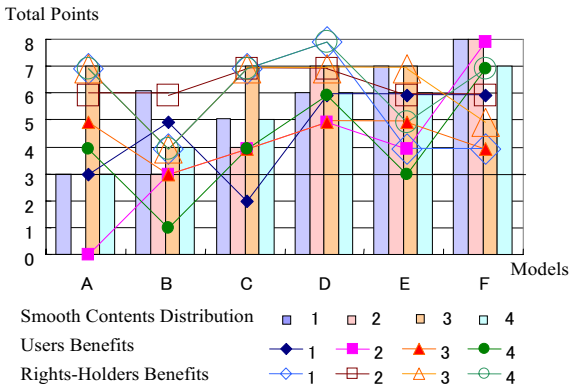


Fig. 5. Compared with Other System

## VI. CONCLUSION

In this paper, an Open DRM System is proposed. The proposed system utilizes various rights information of contents in XrML. Thus, the rights information enable to be processed independently from any platforms. And users enable to transfer rights information to do smooth rights-processing, and to promote re-use and redistribution of contents. This proposed system is secured from the attack of illegal access by verifying a signature as an input value to Rights Processing, and well-protected by enciphering. And user mobility is highly respected with presenting License Certificate File that can be processed off-line as well as allows the private user of contents.

It is can be concluded from the evaluation results that the proposed system enables smooth contents distribution. And the proposed system has some advantages while keeping the nearly same level of capability as seen in other systems, but respecting both rights-holders and users benefits. As for the more sophisticated secondary contents distribution, to process and manage rights information of original and derived are further studies.

## REFERENCES


[1] Jean-Paul Linnartz, Joop Talstra, Ton Kalker, and Maurice Maes, "System Aspects of Copy Management for Digital Video", *Proc. of IEEE ICME* 2000, 0-7803-6536-4
[2] The XrML website. [Online]. Available: http://www.xrml.org/
[3] Theodor H. Nelson, "Transcopyright: Dealing with the Dilemma of Digital Copyright", *in Educom Review* 32(1), 32-5, January/February 1997.
[4] R. Mori and M. Kawahara, "Superdistribution: The Concept and the Architecture", *Trans. IEICE*, Vol.E73, No.7, pp.1122-1146, July 1990.
[5] R. Mori and M. Kawahara, "Superdistribution: An Electronic Infrastructure for the Economy of the Future", *Trans. IPS. Japan*, Vol.38, No.7, pp.1465-1472, July 1997.
[6] H. Imai and T. Suematsu, "An SD System Based on SD Label Distribution Which is Able to Protect User's Privacy", *Trans. IEICE*, Vol.J81-A, No.10 pp.1377-1385, October 1998. [in Japanese]
[7] Kitagawa, "Copymart: A new concept-An Application of Digital Technology to the Collective management of Copyright", *WIPO Worldwide Symposium*, 1993, pp.139-147.
[8] Tanaka, Y. and Imataki, T."IntelligentPad: A Hypermedia System allowing Functional Composition of Active Media Objects through Direct Manipulations", *Proc. of th IFIP 11th World Computer Congress, San Francisco* (1989), pp.541-546.
[9] National Institute of Standards and Technology website. [Online]. Available: http://csrc.nist.gov/cryptval/shs.html