*2011 International Conference on Computer and Automation Engineering (ICCAE 2011)*
***IPCSIT vol. 44 (2012) © (2012) IACSIT Press, Singapore***
*DOI: 10.7763/IPCSIT.2012.V44.9*

# Architecture Design for Drm System of Digital Television

Dayun Lin[a+] and Xingshu Chen[b]

Network and Trusted Computing Institute, Computer College of Sichuan University
Chengdu Sichuan, China

**Abstract**. With the development of Internet and broadband communications technology, Digital TV on a global scale, especially in developed countries has been widely applied. However, there is a huge challenge, which is how to manage a large number of digital content. Digital Rights Management is such a system that strengthen the protection of digital audio and video content copyright. In this paper, we first reviewed the related works in this area and introduced the DRM technology. Then we designed the architecture for "CHKT-DRM". Finally, we introduced all details of this DRM system's core processes.

**Keywords**: Digital TV; DRM; Architecture; digital certificate; Set-top box

## 1. Introduction

With the development of Internet and broadband communications technology, Digital TV on a global scale, especially in developed countries has been widely applied, at the same time, with the gradual progress of network convergence in China, More and more Chinese households will use digital televisions.

Compared with traditional TV, the prominent feature of digital TV is interactive and real-time, However, the spread of digital television is digital content, which can easily be copied, modified and spread, and then cause great economic loss to authors, publisher and distributors, it dampened their enthusiasm of developing new digital products, hindering the develop of digital products and dissemination of information, undermine the healthy growth of digital TV industry. Besides, with the diversified development of digital TV, charging for digital content to make inevitable trend. How to protect digital content from violation and how to manage the charging for content have become an important issue in the development of digital TV. So it is quite necessary and significant to have a theoretical research on this field.

The architecture for DRM system is designed in this paper, which includes content protection, TV programs management, fees collecting management, and then this paper details the entire process of this system. The CHKT-DRM system supports quick publishing for digital content while focus on rights management and user rights management, it realized cluster server technology to carry out the streaming and distribution of digital content. Finally, the architecture gives an effective and security solution to the digital rights management problem of digital TV.

## 2. Related Works

In recent years, DRM makes international broadcasting industry, the academic field and government departments extraordinarily pay attention to. Standardization work has been carried out in some countries. There are three DRM standards which are internationally-recognized: IPMP, OMA DRM and DMP. In China, AVS workgroup(Audio Video Coding Standard Workgroup) designed AVS-DRM in 2004, which supports some important information applications, such as high-resolution digital audio broadcasting, high-density

[+] Email: [a] jefferent@tom.com, [b] chenxsh@scu.edu.cn laser technology of digital storage medium, wireless broadband multimedia communication systems, broadband network streaming, etc.

On research directions, scholars did much research work on rights expression, usage control, reasonable use, conversion privilege, trusted execution and layer architecture for DRM.

The system which provides DRM features is usually very perplexing and has a variety of functions[1]. A wide array of demands and the complexity issues new challenges to the development of DRM[2]. One of the biggest challenges DRM face is dispersion of the solution, there is no common global framework, a universal DRM system that could provide a platform which gathers all DRM service[3]. In the field of the digital right protection, there are many techniques to realize right protection, such as safety container, digital watermark, encryption technology, digital certificate, trusted computing platform, all of these technology have taken huge strides forward. Although DRM varies the objects of protection, business model and technology used, their core idea is the same: through the use of digital certificates to protect the copyright of digital content. Additionally, the architecture for DRM based on Trusted Computing Base(TCB) and the technology of trace illegal redistributors are the focus of related research[4,5].

This paper designs the architecture for DRM system of digital TV, and based on this architecture we develop a experimental system that is called "CHKT-DRM", which pays more attention to the layer structure and integrates the technology of content encryption, authentication, secure communication, rights management, server clustering to ensure that DRM system have specific properties of high safety and high availability.

## 3. DRM Technology

DRM technology is an integral mechanism which define, describes, protects and monitors the rights of the parties involved in the process of creating, broadcasting and playing digital content. DRM is the chain of hardware and software services and technologies governing the authorized use of digital content and managing any consequences of that use throughout the entire life cycle of the content[6]. Its goals are to ensure legitimate use through the life cycle of digital content, protect the intellectual property rights of digital content, protect the trade channel of digital content, protect the interests of authors, publisher and distributors and the legitimate right of end-users. Finally, achieving the goal of keeping the balance of the interests among all parties, stimulating digital content product's development and prosperity. Figure1 shows the common framework of digital TV[7].

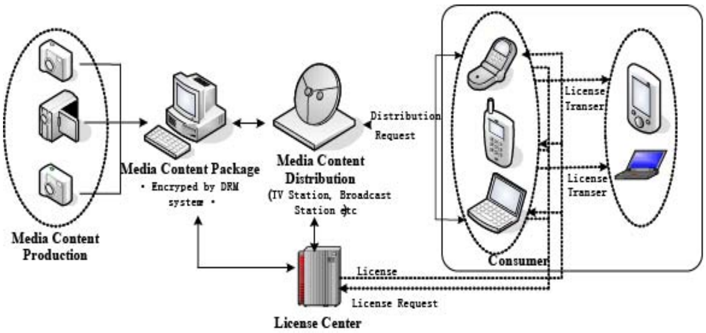

Fig.1. DRM framework of Digital TV

### 3.1. Requirements of Digital Rights Management

A complete DRM system should be an appropriate balance between provider and user. To satisfy these needs, DRM system offers a series of key technologies and functions, which means it develops and maintains a safe work environment to conduct interactions between content providers and end-users. DRM system should achieve the following functions:

#### 3.1.1. Content protection and secure transmission

DRM should guarantee secure transmission on insecure common channel between content providers and end-users. Generally speaking, DRM employs encryption algorithms to secure digital content, only the man who get the keys could decrypt the data.

### 3.1.2. Secure publishing

Once after digital content has been packed by DRM, all end-users can access protected contents, but if there is no use permit, it cannot use digital content normally, and therefore ensure secure publishing, control usage mode and using objects of digital content.

### 3.1.3. Identify the authenticity of content

In order to ensure the truth of content, DRM employs unilateral hashing function and digital watermarking technology. Get and store content summarization when publish the digital content; or divide the original content into multiple blocks that embedded different digital watermark. If user wants to identify integrality and authenticity of digital content, he/she could compare the original with the current summarization; or detect the watermark signal of each blocks.

### 3.1.4. Non-repudiation of the trading

Whether in the real world or in virtual market, the proof of trading is important for all participants of the transaction.

### 3.1.5. Identity authentication

DRM system must identify the ID of all participants first. In general, DRM uses digital certificates technology to ensure authenticity of participants.

## 3.2. Functional Architecture of DRM

Any DRM architecture is composed of a standardized set of different building blocks. DRM system uses digital certificates to protect the copyright of digital content. After user has got the digital content, he/she can play the content with digital certificate[8]. Figure2 shows the typical DRM system with DRM functional architecture, it includes: Content Server, License Server and Client[9].

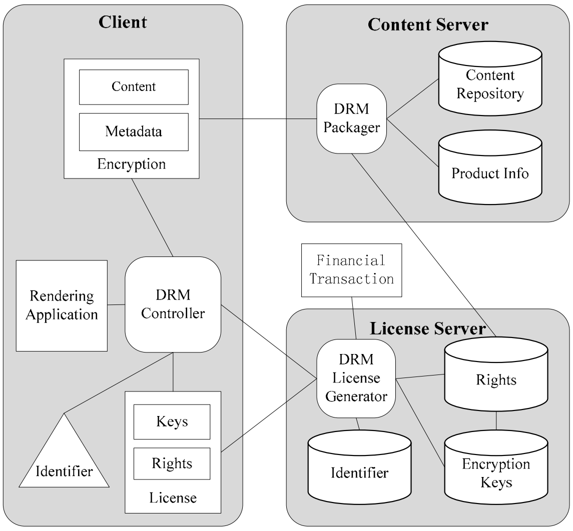

Fig.2 Generic DRM Functional Architecture

## 3.3. Rights Expression Language

Rights Expression Language(REL) is one of the most key technologies in the DRM. DRM system makes identification and interpretation of digital content, and thus using the technology for rights management. The digital content is described by REL[10].Figure3 shows REL entities model:

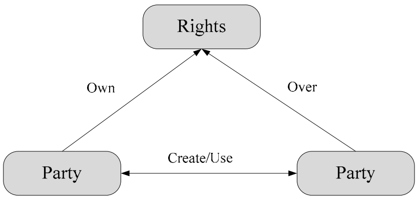

Fig.3. REL Entities Model

## 4. Architecture Design For CHKT-DRM

CHKT-DRM system can encrypt and pack streaming and static files which base on mp4 format, and then be published by content publishing server. When the end-user receive the contents, he/she cannot decode the contents and watch them until he get the decryption key and be authenticated.

Figure4 shows the architecture of CHKT-DRM, the system includes six modules: CA, DRM Center, Content Provider, Streaming Server Cluster, Set-top Box and File Storage Management. Different modules can be achieved on different physical node(server), different DRM system can be comprised of different modules according to the business requirements of target DRM system.

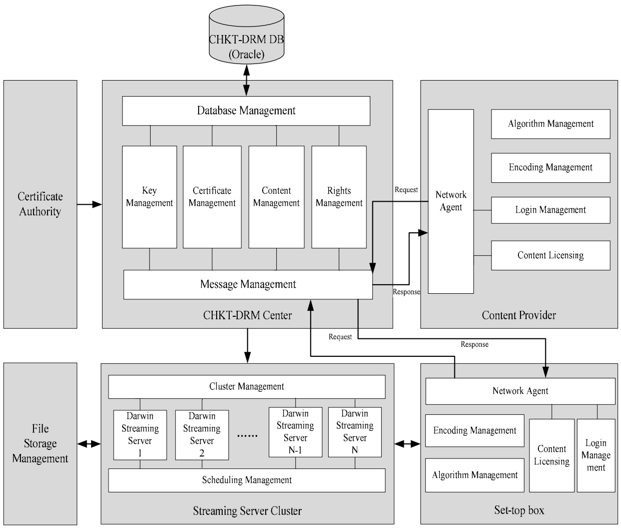

Fig.4. Architecture of CHKT-DRM

### 4.1. System Architectural Components

The system mainly consists of six modules, each is described in detail below:

- *CA*: This module is responsible for certificate generation, distribution and management, authenticating the identity of the terminal, providing certificate status queries. It maintains an open communication with rights management system to assist to manage access right of end-users.
- *DRM Center*: This module is responsible for maintaining and managing keys and providing query services to rights management system, besides, it is responsible for managing digital content, it sends encrypted content to Streaming Server Cluster.
- *Content Provider*: This module is responsible for packaging and encrypting digital content, and sending the results to the content distribution system.
- *Streaming Server Cluster*: This module is responsible for publishing content, accepting and dispatching content request from the terminal and managing all Darwin Streaming Server[11].
- *Set-top Box*: This module is responsible for decrypting digital content with the decryption key.
- *File Storage Management*: This module is responsible for storing content and establishing of the content index.

### 4.2. System Work Flow

Figure5 shows the work flow of CHKT-DRM, including the following steps:

- Publisher uploads the plaintext digital content to Content Provider Server;
- Content Provider Server encrypts the digital content, and passes it to Streaming Server Cluster;
- Content Provider Server stores the information of programs and keys into database;
- Set-top Box gets program list from Streaming Server Cluster, and requests the program which the user wants to watch;
- When Set-top Box finds the steaming is encrypted, it initiates authentication request to CA, and the CA processes this request and verifies the identity of the requester;
- CA submits a query request to Rights Management Server, checks the rights of this end-user;
- If certification is correct and this end-user has the corresponding rights, Set-top Box will request the decryption key from Key Management Server, and then Set-top Box can decode the encrypted Streaming and play it. Otherwise, if there are some errors during this process, it will prompt the user the error information.

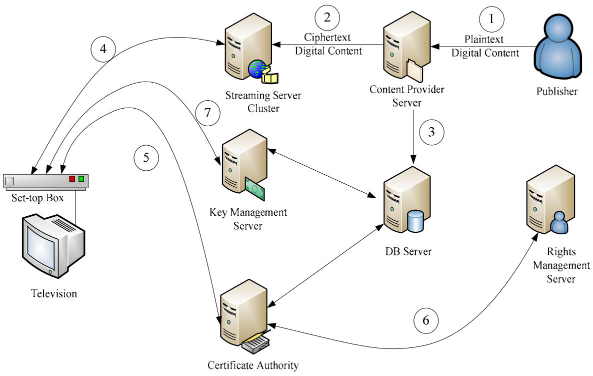

Fig.5. Work Flow of CHKT-DRM

## 4.3. System Business Process

### 4.3.1. Key Management Process

Key Management System is such an important part of DRM system and is responsible for managing keys. It provides query services to Rights Management System, and maintains the mapping relationship between keys and digital content. In order to support business expansion, Key Management System can control the keys validity period, and attach the validity period with rights entity.

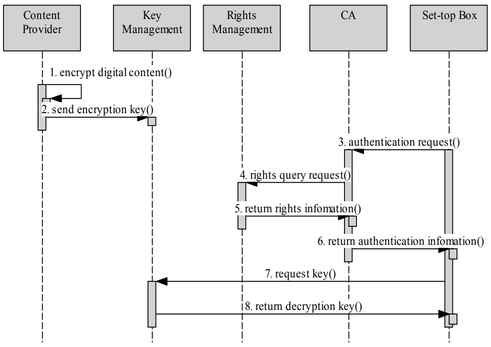
Content
Provider
Key
Management
Rights
Management
CA
Set-top Box
1. encrypt digital content()
2. send encryption key()
3. authentication request()
4. rights query request()
5. return rights infomation()
6. return authentication infomation()
7. request key()
8. return decryption key()

Fig.6. Key Management Process

Figure6 shows Key Management Process of CHKT-DRM, the actualizing process falls mostly into eight steps:

- Content Provider encrypts the digital content;
- Content Provider sends the encryption key to Key Management System;
- Set-top Box sends authentication request to CA, CA processes this request and verifies the identity of the requester;

- CA submits a query request to Rights Management Server, checks the rights of this end-user;
- Rights Management Server returns rights information;
- CA returns authentication information to Set-top box;
- Set-top Box requests the decryption key from Key Management Server;
- Key Management Server returns the decryption key to Set-top Box.

### 4.3.2. Program Publishing Process

Program Publishing includes two parts: Content Provider Server and Streaming Server Cluster. Content Provider Server is responsible for encrypting plaintext digital content and Streaming Server Cluster is responsible for translating digital content into streaming and publishing the content. CHKT-DRM system uses Darwin Streaming Server(DSS) as publishing server, and uses server clustering technology to manage all DSS.

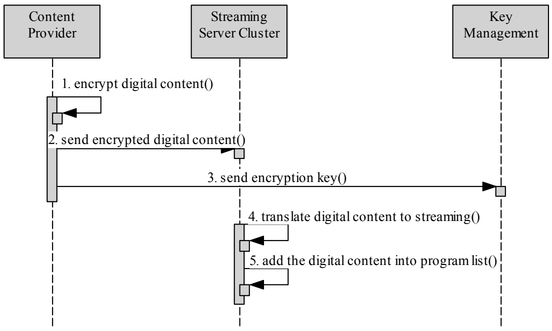
Content Provider
Streaming Server Cluster
Key Management
1. encrypt digital content()
2. send encrypted digital content()
3. send encryption key()
4. translate digital content to streaming()
5. add the digital content into program list()

Fig.7. Program Publishing Process

Figure7 shows Program Publishing Process of CHKT-DRM, the actualizing process falls mostly into five steps:

- Content Provider encrypts the digital content;
- Content Provider sends encrypted digital content to Streaming Server Cluster;
- Content Provider sends the encryption key to Key Management System;
- Streaming Server Cluster translates digital content into streaming;
- Streaming Server Cluster adds the digital content into program list.

### 4.3.3. Certification Authority and Rights Management Process

This is an important part of DRM system, the security of CHKT-DRM is determined by this module. CA is responsible for certificate generation, distribution and management, authenticating the identity of the terminal, providing certificate status queries. Rights Management System is responsible for managing rights of all end-users, and supplies rights query services to CA.

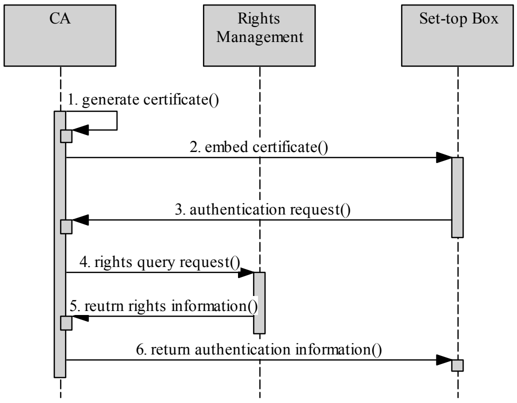
CA
Rights Management
Set-top Box
1. generate certificate()
2. embed certificate()
3. authentication request()
4. rights query request()
5. reutrn rights information()
6. return authentication information()

Fig.8. Certification Authority and Rights Management Process

Figure5 shows Certification Authority and Rights Management Process of CHKT-DRM, the actualizing process falls mostly into six steps:

- CA generates certificate for end-user;
- The certificate is embedded into Set-top box;
- Set-top Box sends authentication request to CA, CA processes this request and verifies the identity of the requester;
- CA submits a query request to Rights Management Server, checks the rights of this end-user;
- Rights Management Server returns rights information;
- CA returns authentication information to Set-top box;

### 4.3.4. Request Program Process

Request Program is the ultimate embodiment of CHKT-DRM, end-users watch TV programs through Set-top Box.

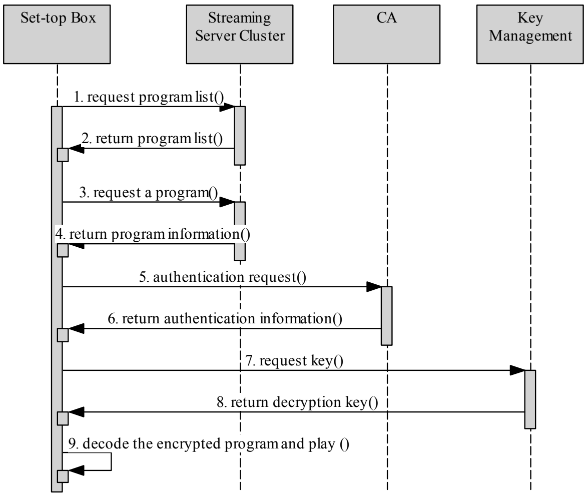
Set-top Box
Streaming Server Cluster
CA
Key Management
1. request program list()
2. return program list()
3. request a program()
4. return program information()
5. authentication request()
6. return authentication information()
7. request key()
8. return decryption key()
9. decode the encrypted program and play ()

Fig.9. Request Program Process

Figure9 shows Request Program Process of CHKT-DRM, the actualizing process falls mostly into nine steps:

- Set-top Box requests program list from Streaming Server Cluster;
- Streaming Server Cluster returns program list to Set-top Box;
- Set-top Box requests a program from Streaming Server Cluster;
- Streaming Server Cluster returns the program to Set-top Box;
- Set-top Box sends authentication request to CA, CA processes this request and verifies the identity of the requester;
- CA returns authentication information to Set-top box;
- Set-top Box requests the decryption key from Key Management Server;
- Key Management Server returns the decryption key to Set-top Box;
- Set-top Box decodes the encrypted Streaming and play it.

## 5. Conclusion

This paper designs the architecture for DRM system of digital TV, introduces all details of this DRM system’s core processes, and based on this architecture we develop CHKT-DRM system, which pays more attention to the layer structure and integrates the technology of content encryption, authentication, secure communication, rights management, server clustering to ensure that DRM system have specific properties of high safety and high availability. Finally, the architecture solves the content rights management problem of digital TV safety and high efficiency.

## 6. Acknowledgment

This work was supported by the major state basic research development program of China(973 program) under grant No.2007CB311106. The authors wish to thank all members of Network and Trusted Computing Institute of Sichuan University, and thank project team members for their help when the authors write this paper.

## 7. References

[1] D.K.Mulligan,Special Issue:Digital Rights Management and fair use by design,Communications of the ACM,2003,46(4).

[2] Sam Michiels,Towards a software architecture for DRM,Proceedings of the 5th ACM workshop on Digital rights 2005,pp.65-74.

[3] Jamkhedkar Pramod A., Heileman Gregory L. DRM as a layered system. In Proceedings of the Fourth ACM Workshop on Digital Rights Management, 2004, pp. 11~21.

[4] Reid J F，Caelli W J．DRM，Trusted Computing and Operating System Architecture．Australasian Information Security Workshop 2005(AISW2005)．Newcastle．Australia.

[5] QIU Gang, WANG Yu-lei,ZHOU Li-hua. “Study on the Interoperability of DRM Based on Trusted Computing”, Computer Science, vol. 36, Jan 2009.

[6] Dahl Joshua and Kevorkian Susan, Understanding DRM Systems, An IDC Research White Paper, 2001.

[7] Song Yonghao. Research on Content Protection of Digital Television;Shanghai Jiao Tong University,2008, pp.23-24.

[8] Fromm M, Gruber H, Schutz M. Evaluation of digital rights management systems, Vienna University. Seminar Paper, 2003.1.

[9] Rosenblatt W., Trippe W., Mooney S. Digital Right s Management: Business and Technology. New York: M &T Books, 2002.

[10] Guth S., Rights expression languages, In Digital Rights Management: Technological, Economic, Legal and Political Aspects. Lecture Notes in Computer Science 2770 , Berlin, 2003, pp.101~112.

[11] Hua Bafeng, ZhongMing, Yang Chuanjun, et a.l Research and application of the darwin streaming server[J]. Computer Engineering, 2004, 30(19):1342135