A Study on Key Delivery Message System of Digital Cinema Design

Fang Lu

Academy of Fine Arts, Dalian University, Dalian, China, 116622

E-mail:shining_112@live.cn

Keywords: Digital cinema;Design;DCDM;KDM; Security information.

Abstract. Digital Cinema Initiatives released a set of technical specifications and requirements for Digital Cinema. The KDM (Key Delivery Message) has been designed to deliver security parameters and usage rights between D-Cinema content processing centers. We propose a KDM system that covers the end-to-end process of KDM for D-Cinema content protection. It provides the end-to-end process of KDM from Mastering server to D-Cinema play server.

Introduction

Digital Cinema Initiatives, LLC (DCI) has established uniform specification for Digital Cinema. It covers technical specifications and requirements for the mastering of, distribution of, and theatrical playback of Digital Cinema content [1, 3, 6].

The protection of intellectual property of Digital Cinema is a critical aspect of the design of the system [4, 5]. The Key Delivery Message (KDM) has been designed to deliver security parameters and usage rights between D-Cinema content processing centers [8]. It contains security keys for decrypting Digital Cinema Package (DCP) from digital cinema servers [2, 3, 7, 9].

We propose a KDM system that covers the end-to-end process of KDM for D-Cinema content protection. Proposed KDM system provides a scheme how the KDM is generated from Mastering server, how KDM is issued from KDM server and how KDM is handled in D-Cinema play server [10].

Digital Cinema Using Case Scenario

Digital Cinema content for distribution is generated at the mastering time. The mastering process produces DCP (Digital Cinema Package) from DCDM (Digital Cinema Distribution Master) which is the output of the Digital Cinema postproduction process and is a collection of image, audio and subtitle files. Once the DCDM is compressed, encrypted and packaged, it is considered to be DCP. The mastering process also produces security information like AES-128 keys used to encrypt image, audio and subtitle of DCP [3,4,5,6].

After the mastering process, DCP is delivered to Contentserver to distribute it to a theater and security information is delivered to KDM server to issue KDM to D-Cinema playserver.

If a theater requests DCP from content server and KDM for the DCP, content server will deliver DCP to the theater through network, satellite, or hard-disk. And, KDM server will issue a KDM which is specific to the D-Cinema play server. It will be delivered through e-mail, USB, or network[6].

After DCP is transported to the theater, it is stored on a file server in the theater until playback. D-cinema play server will play DCP with the KDM. During the playback and projection, digital cinema content plays out in real time[5].

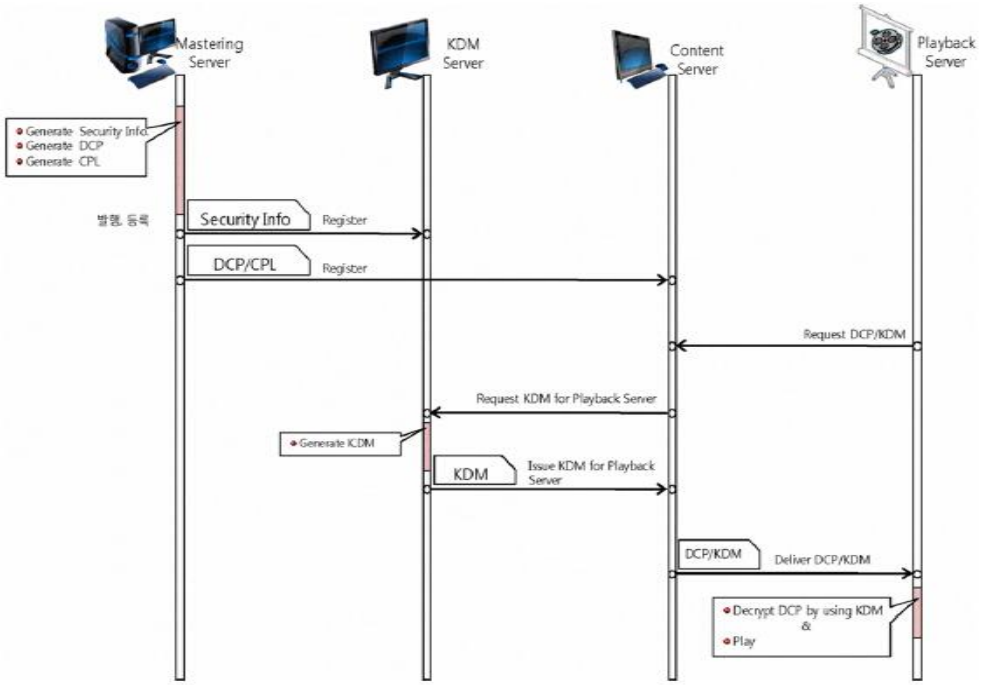

Figure1. Use case scenario of Digital Cinema

Proposed KDM System

Proposed KDM system defines the entities which involve in delivery of security information and KDM. The distribution is implemented by the following step:

a) First, D-Cinema content server generates 128 bit-long AES cryptographic keys of D-Cinema content and use K_c to package the content to an AES encrypted format. Video file, audio file and subtitle file use different keys, and in addition, each video file or audio file can be divided into several reels, each of which is encrypted using a unique key, for the purpose of increase the encryption strength. Thus the original D-Cinema content C is packaged to C'.

$$C'=E_{K_C}(C) \quad (1)$$

b) D-Cinema content server lists the encrypted content in the available folder, and then distributes it to subscriber, either via online data transfer or physical offline delivery.

c) Link all the content keys using to the movie in a format as indicated in equation (2) and thus form a key list,

$$KL=KeyID\|K_C\|\cdots\|KeyID\|K_C \quad (2)$$

where the notation $\|$ denotes the concatenation operation, and KeyID which stands for the identity of key, is used as the index relating D-Cinema reel and the relevant key. The encrypted data package of each reel includes the KeyID of relevant content key, which facilitates the project device to search the appropriate content key K_C to decrypt the encrypted package.

d) KL is encrypted by the public key of license management server PK_1 formatted into key delivery message KDM_{c21}sent to the license management server. Once the license management server receivesKDM_{c21}, KL will be decrypted from it and stored in the database of content keys.

$$KDM_{c21}=E_{PK1}(KL) \quad (3)$$

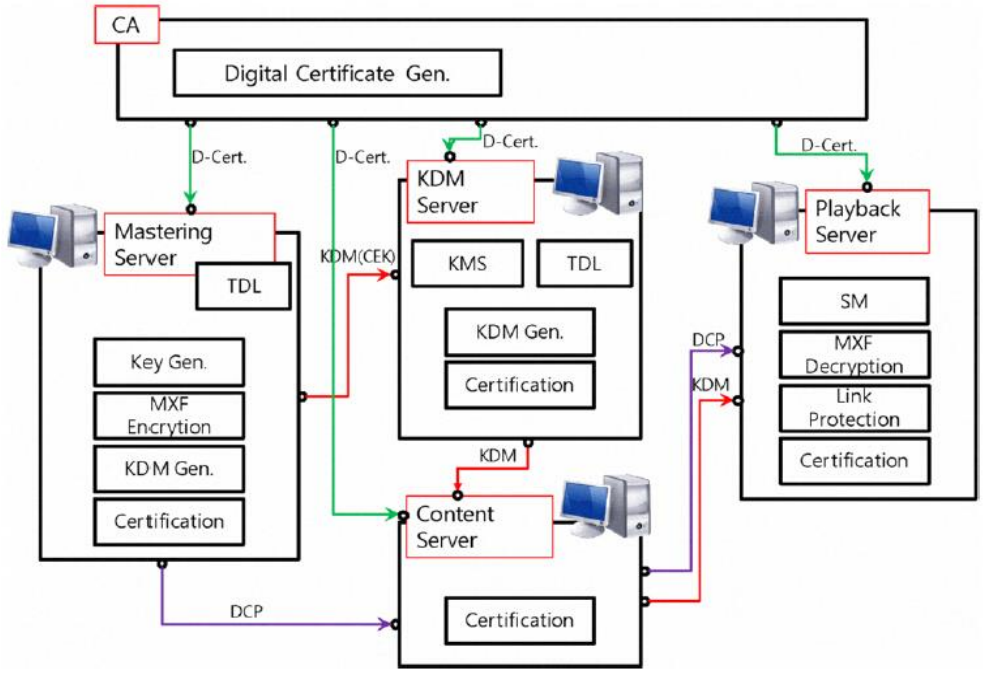

Figure 2. Overall architecture of KDM System

Security Analysis

The forgery of KDM system can be detected by its certificate. The entities of KDM system can authenticate each other using the other's certificate to determine whether it is a legal entity. Mastering server and KDM server can respectively verify whether KDM server and D-Cinema play server are legal entities to which a KDM can be given and confirm that the KDM to be issued goes to correct entity but others. And KDM server and D-Cinema play server can respectively verify thatthe sender of the KDM is a legal Mastering server and KDMserver.

An attack on CEK during delivery from sender, Mastering server or KDM server, to receiver, KDM server or D-Cinema play server, is prevented because CEK is encrypted with the public key of receiver and delivered to receiver. Thus, CEK is decrypted by only receiver who has a secret key and not the others. Illegal recovery of original content from DCP is prevented because the resource like image, audio and subtitle is encrypted by CEK which can be only decrypted by receiver, and KDM can be digitally signed by the sender.Thus receiver can check whether it has been changed or not.

Conclusions

Digital Cinema Initiatives released a set of technical specifications and requirements for the mastering of, distribution of, and theatrical playback of Digital Cinema content. DCI explicitly pointed out that a set of regulations for movie content based on DRM should be set up to regulate the security of D-cinema. The KDM has been designed to deliver security parameters and usage rights between D-Cinema content processing centers. It contains security keys for decrypting DCP on D-Cinema servers.

Acknowledgement

This work was supported by the Liaoning Provincial Education Department (W2013280); Scientific Research Foundation for the Returned Overseas Chinese Scholars, State Education Ministry; Research Fund for the Doctoral Program of Dalian University.

References

[1] Digital Cinema Initiatives, L., "Digital Cinema System SpecificationV1.2", March 07,2008.

[2] H. Zhaoting, G. Qiang, L. Yiguang, "A digital right management systembased on smart card for digital cinema", Communications andNetworking in China, 2008. ChinaCom 2008. Third InternationalConference on 25-27 Aug. 2008 Page(s):829 - 833

[3] J. A. Bloom, "Security and rights management in digital cinema",Acoustics, Speech, and Signal Processing, 2003. Proceedings. (ICASSP'03). 2003 IEEE International Conference on Volume 4, 6-10 April2003 Page(s):N - 712-15 vo1.4

[4] J. A. Bloom, "Digital Cinema Content Security and the DCI",Information Sciences and Systems, 2006 40th Annual Conference on 2224March 2006 Page(s):1176 - 1181

[5] Zhen-Song Wang, Ling Li, Xi-Shuang Wang, Ke Zhang, Kai Wang,Ping Yao, Wen-Dong Cao, Huang-HuiShen, " A Digital CinemaPlayback system compliant with the DCI specification", Picture CodingSymposium, 2009. PCS 2009, 6-8 May 2009 Page(s):l - 4

[6] P. Micanti, F. Frescura, G. Baruffa, "Digital Cinema packagetransmission over wireless IP networks", Wireless CommunicationSystems. 2008. ISWCS '08. IEEE International Symposium on 21-24Oct. 2008 Page(s):154 - 158

[7] SMPTE 430-1-2006, D-Cinema Operations - Key Delivery Message,October 3, 2006

[8] SMPTE 430-2-2006, D-Cinema Operations - Digital Certificate,October 3, 2006

[9] SMPTE 430-3-2006, D-Cinema Operations - Generic Extra TheaterMessage Format, March 3, 2008

[10] Digital Cinema System Specification Compliance Test Plan Version 1.1,May 8, 2009