Design of KDM System for Digital Cinema

Yeonjeong Jeong, Jungsoo Lee, Kisong Yoon

Content Distribution Team, ETRI, 161, Gajeong-dong, Yuseong-gu, Daejeon, Korea

yjjeong@etri.re.kr, jslee2365@etri.re.kr, ksyoon@etri.re.kr

***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.**

***Keywords*— D-Cinema, KDM**

I. 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. The Key Delivery Message(KDM) has been designed to deliver security parameters and usage rights between D-Cinema content processing centers. 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.

II. DIGITAL CINEMA USE 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 post-production 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 Content server to distribute it to a theater and security information is delivered to KDM server to issue KDM to D-Cinema play server.

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].

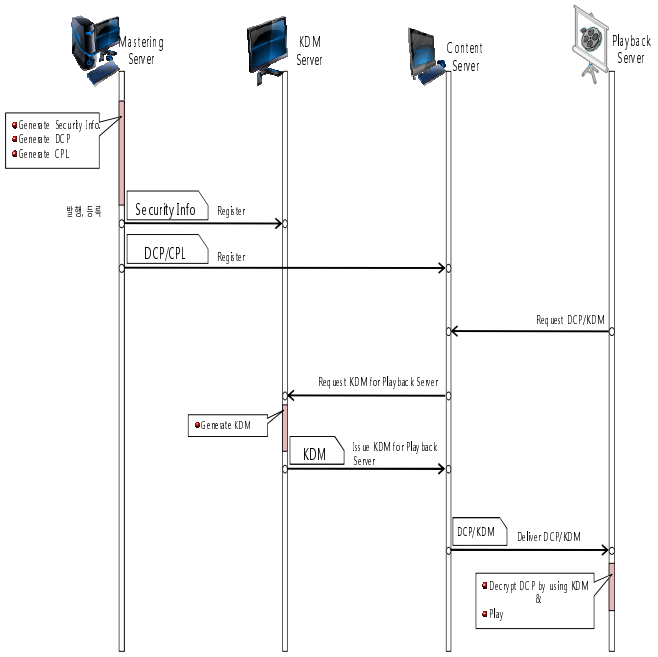

Figure 1. Use case scenario of Digital Cinema

III. PROPOSED KDM SYSTEM

Proposed KDM system defines the entities which involve in delivery of security information and KDM. It consists of CA server, modules in Mastering server, KDM server and modules

in D-Cinema play server. CA server provides digital certificate to each server. Modules in Mastering server which are key generation module, MXF encryption module and KDM generation module. KDM server provides KDM to D-Cinema play server. Modules in D-Cinema play sever which are KDM decode module and MXF decryption module provide security information like the cipher keys which are used to decrypt D-cinema content and forensic mark, and usage rights.

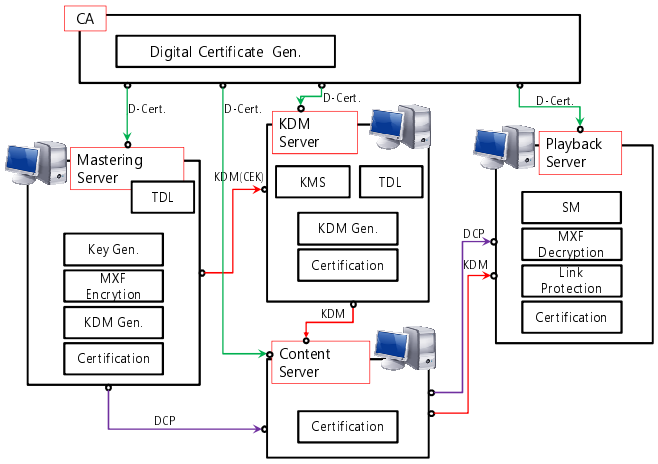

Figure 2. Overall architecture of KDM System

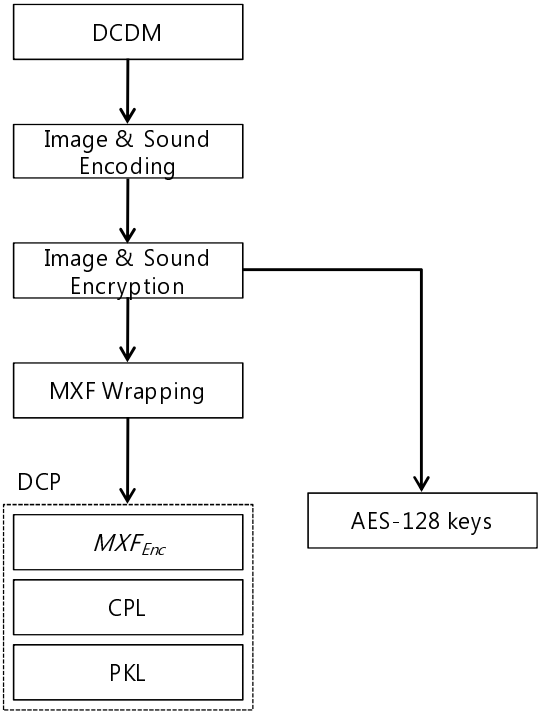

Figure 3. Digital cinema mastering process

A. KDM modules in Mastering server

The Mastering server produces DCP(Digital Cinema Package) from DCDM(Digital Cinema Distribution Master) which contains all of the digital material needed for projection. The images and sound of DCDM are then compressed, encrypted, and packaged to form a DCP. A DCP consists of several reels, each of which has image track, sound track and subtitle track. The security information like AES-128 key used to encrypt the image, sound and subtitle track is generated during the mastering process. The figure 3. shows the mastering process of digital cinema.

We design that mastering sever includes KDM generation module to produce KDM from the security information. MXF wrapper request a AES-128 key to Key generation module. The generated key is used to encrypt a track file only but other track file. MXF wrapper sends the key, J2K frame and plaintext offset to MXF encryption module. Then it encrypts the J2K frame from the offset by using the encryption key. MXF wrapper will call MXF encryption module with the same key until the whole j2k frames of the track file are encrypted. After the MXF wrapping, DCP and security information to generate KDM are produced. KDM generation module gets the AES-128 keys, corresponding key id to the key and CPL Id from MXF wrapper module. It encrypts the AES-128 keys with KDM server's public key and singed with Mastering server's private key. After all, KDM for a KDM server is generated and delivered to the KDM server.

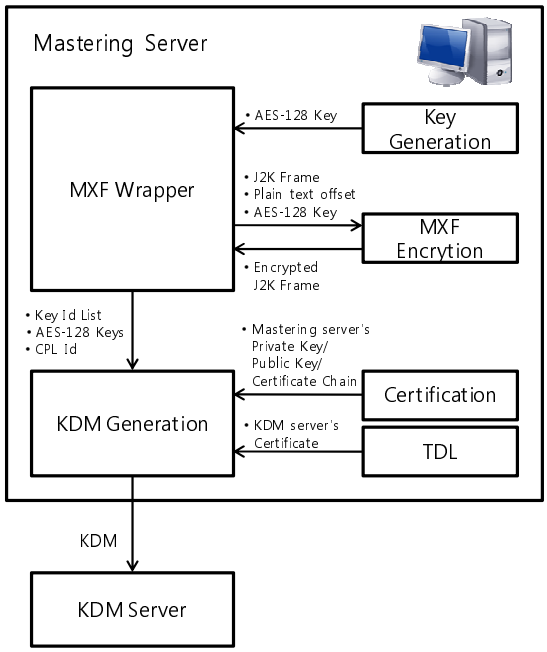

Figure 4. KDM module structure in Mastering server

B. KDM server

We design that KDM server issue KDM to a specific D-Cinema play server by using the KDM which is generated from Mastering server. The KDM from Mastering server is encrypted by using KDM server's public key. After it is decrypted with KDM server's private key, it can be encrypted with a specific D-Cinema play server's public key.

KDM server registers the KDM from Mastering server after it verifies the KDM according to the KDM decoding behavior[10]. It ensures the KDM issued to a D-Cinema play server will work properly at a theater. KMS module stores the KDM with its information like CPL Id, title, usage rights and issued date in the authenticated public area of the KDM.

If request to issue a specific KDM for a D-cinema play server occurs, KDM issue module will receive D-Cinema play server's device Id, CPL Id for the specific KDM and rights usage from content server. Then It checks whether the D-Cinema play server is verified one or not with TDL in the TDL database. It also verifies the requested usage rights is available according to the usage rights of the KDM which is stored in its local DB.

KDM decryption module decrypts cipher data in KDM with its private key. KDM issue module replaces the usage rights with the requested usage rights for the D-cinema player server, encrypts the decrypted the encrypted data with the D-Cinema play server's public key, and digitally signs new KDM with its private key.

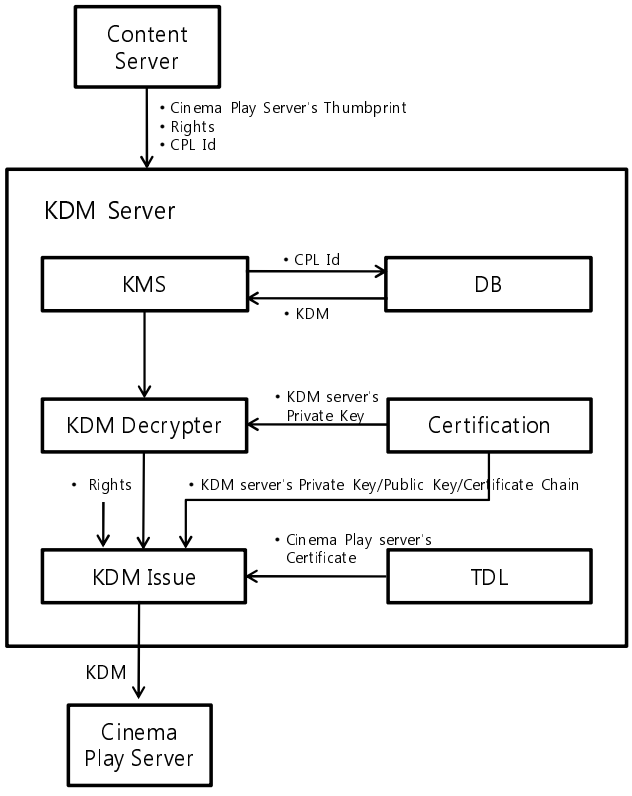

Figure 5. KDM server structure

C. KDM modules in cinema play server

The D-Cinema play server converts the packaged, compressed and encrypted data, DCP, into raw image, sound and subtitles. KDM decode module validates and decrypts KDM and verifies it has all cipher keys necessary for DCP. Then it sends all cipher keys to media block which are responsible for converting DCP into raw image, sound and subtitles. MXF decryption module decrypts J2K frame from plain text offset by using the cipher key. Media block will call MXF decryption module with the same key until the whole j2k frames of a track file are decrypted.

KDM decode module also sends forensic mark key to forensic mark module. forensic mark module will use the key as seed of forensic mark.

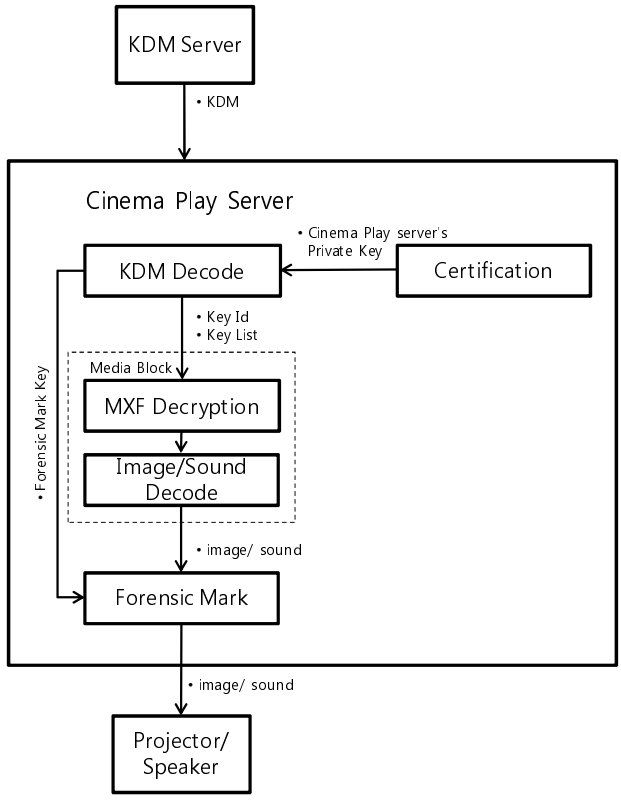

Figure 6. KDM module structure in D-Cinema play server

IV. 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 that

the sender of the KDM is a legal Mastering server and KDM server.

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.

V. CONCLUSION

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.

We propose 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. It provides the end-to-end process of KDM from Mastering server to D-Cinema play server.

ACKNOWLEDGMENT

This work was supported by MCST(Ministry of Culture, Sports & Tourism)/KOCCA(Korea Culture and Content Agency)(2-09-1205-001-10987-09-001 Development of DCI compliant digital cinema distribution management and copyright protection technology).

REFERENCES

[1] Digital Cinema Initiatives, L., "Digital Cinema System Specification V1.2", March 07, 2008.

[2] H. Zhaoting, G. Qiang, L. Yiguang, " A digital right management system based on smart card for digital cinema", Communications and Networking in China, 2008. ChinaCom 2008. Third International Conference 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 April 2003 Page(s):IV - 712-15 vol.4

[4] J. A. Bloom, "Digital Cinema Content Security and the DCI", Information Sciences and Systems, 2006 40th Annual Conference on 22-24 March 2006 Page(s):1176 - 1181

[5] Zhen-Song Wang, Ling Li, Xi-Shuang Wang, Ke Zhang, Kai Wang, Ping Yao, Wen-Dong Cao, Huang-Hui Shen, " A Digital Cinema Playback system compliant with the DCI specification", Picture Coding Symposium, 2009. PCS 2009, 6-8 May 2009 Page(s):1 - 4

[6] P. Micanti, F. Frescura, G. Baruffa, "Digital Cinema package transmission over wireless IP networks", Wireless Communication Systems. 2008. ISWCS '08. IEEE International Symposium on 21-24 Oct. 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 Theater Message Format, March 3, 2008

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