Implementation of KDM System based on DCI

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— **The Key Delivery Message(KDM) has been designed to deliver security parameters and usage rights between Digital Cinema content processing centers. We implement KDM system that consists of KDM server which can issue KDM to D-Cinema play server and content server which can receive a KDM request from D-Cinema play server and request KDM server to issue KDM for the D-Cinema play server. Proposed KDM system provides how it securely receives the KDM related information from mastering server, how it handles the KDM information in KDM server and content server, and how it issues KDM to D-Cinema play server.**

.

Keywords— **KDM, Digital Cinema, DCI**

I. INTRODUCTION

Digital Cinema Initiatives released a set of technical specifications and requirements 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 implement a KDM system that consist of KDM server and content server. KDM server receives information to construct KDM from master server and issue KDM to D-cinema play server. Content server receives a request to KDM issue from D-cinema play server and send the request to KDM server.

Proposed KDM system provides how it securely receives the KDM related information from mastering server, how it handles the KDM information in KDM server and content server, and how it issues KDM to D-Cinema play server.

II. KDM SERVICE MODEL AND USE CASE SCENARIO

Mastering server generates DCP and KDM information for the distribution of Digital Cinema content 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 theatre to play it on D-cinema play server and KDM information is delivered to KDM server to issue KDM to D-Cinema play server.

KDM server receives KDM information from mastering server and stores it in its local DB to generate KDM for a corresponding DCP.

If a theatre requests DCP and KDM to content server, content server will send DCP to the theatre through network, satellite, or hard-disk and request KDM server to issue the KDM of the DCP for the theatre. KDM server will issue the KDM which is specific to the D-Cinema play server which is already verified and registered in TDL of KDM server. It will be downloaded through network by the theatre.

After the DCP and KDM is transported to the theatre, it is stored on a file server of the theatre. D-cinema play server will play DCP with the KDM. During the playback and projection, digital cinema content plays out in real time. Figure 1 shows KDM service model which consists of mastering server, KDM server, content server and D-Cinema play

server and Figure 2 shows the use case scenario that presents how KDM and DCP is handled in the proposed model.

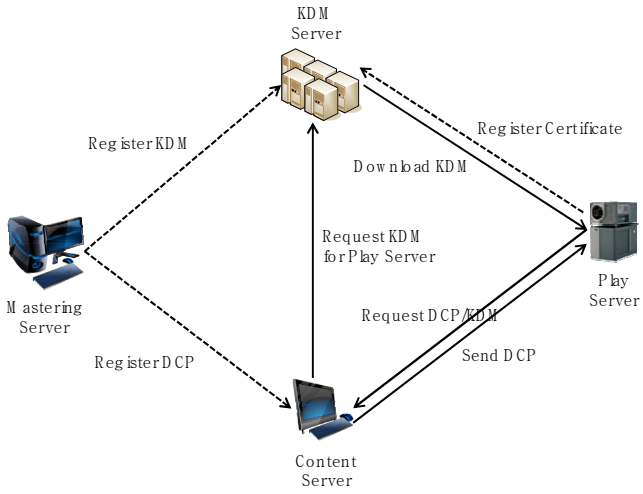


Figure 1. KDM service model which consists of masering server, KDM server, content server and play server

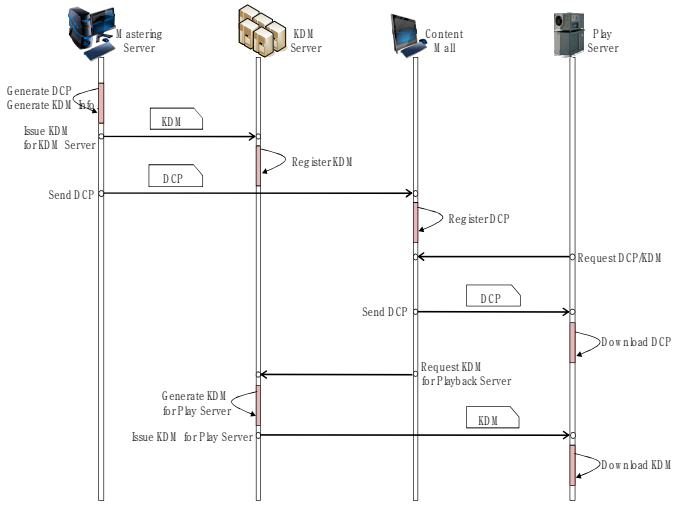


Figure 2. KDM use case scenario which consists of masering server, KDM server, content server and play server

III. KDM MESSAGE

The KDM carries all the critical information required to enable content decryption according to a baseline interoperable security standard[1,7]. KDM server uses KDM message to send KDM information to D-Cinema play server. We also use KDM message to deliver KDM information from mastering server to KDM server. It can provide secure transfer of KDM information from mastering server to KDM server. Figure 3 and 4 show the KDM information flow of the proposed KDM system.

KDM server receives KDM information from mastering server by using KDM message, the issuer and recipient of which are mastering server and KDM server respectively. It contains the AES-128 keys encrypted 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.

KDM server issues KDM to D-Cinema play server by using the KDM message that received from mastering server. KDM server decrypts cipher data in the KDM with its private key. It replaces 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 the new KDM with its private key.

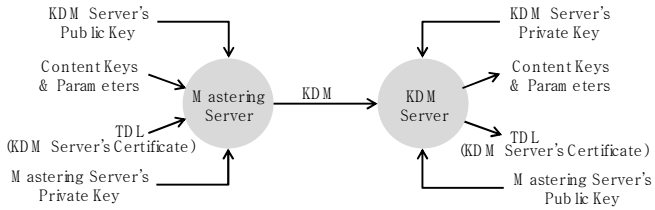


Figure 3. KDM information flow from masering server to KDM server

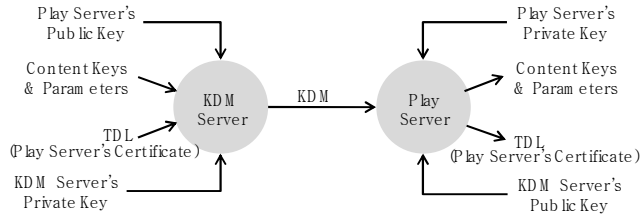


Figure 4. KDM information flow from KDM server to D-Cinema play server

KDM is particular instance of the generic XML security wrapper defined by D-Cinema ETM(Extra Theatre Message) format[7,9]. The ETM consists of the AuthenticatedPublic, AuthenticatedPrivate and Signature element.

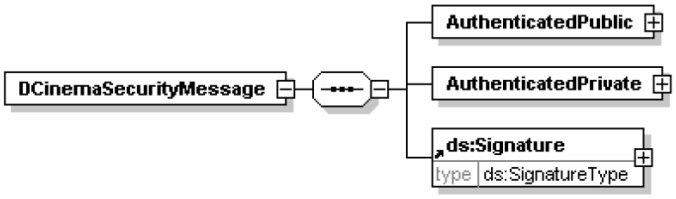


Figure 5. XML Diagram for ETM

KDM server replaces some child elements of the AuthenticatedPublic element which includes information that must be visible without decryption in order to properly handle the KDM within D-Cinema systems. MessageId is newly generated. IssueDate is changed with current issuing time. Signer is KDM server and Recipient is D-Cinema play server. ContentKeysNotValidBefore and ContentKeysNotValidAfter is changed with the requested usage rights for the D-Cinema player server from content server. CertificateThumbprint is that of D-Cinema play server's certificate.

The AuthenticatedPrivate element contains encrypted keys which are encrypted for the recipient before being transmitted. It means that through encryption only a specified recipient is allowed to view this information. So, KDM server decrypts the encrypted keys with its private key. After that, it replaces the values of ContentKeysNotValidBefore and ContentKeysNotValidAfter of CipherValue element with the requested usage rights and re-encrypts CipherValue element with D-Cinema play server's public key.

Signature element which shall contain two reference fields, one for the new AuthenticatedPublic and one for new AuthenticatedPrivate provides the integrity of the KDM by using KDM server's certificate.

IV. KDM System

A. KDM Server

KDM server is divided in KDM management, TD management and KDM issue module. KDM management manages KDM information. It registers the KDM which is generated 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 theatre. KDM management stores the KDM with KDM information like CPL Id, title, usage rights and issued date in the authenticated public area of the KDM.

Figure 6. KDM management

TD management manages certificates of D-Cinema play server. It registers the certificate of D-Cinema play server. Then It is possible to check whether the D-Cinema play server is verified one or not with TDL in the TDL database when the KDM request to a specific play server occurs from content server.

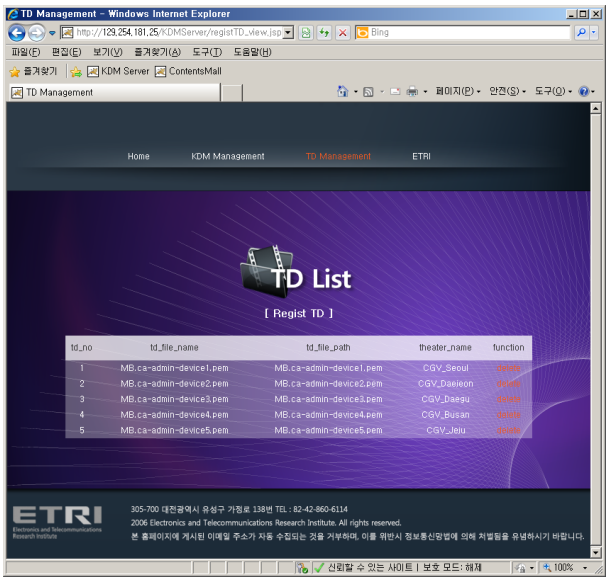


Figure 7. TDL management

KDM issue module issues KDM to a specific D-Cinema play server by using the data of KDM management and TDL management. If request to issue a specific KDM for a D-cinema play server occurs, KDM issue module will receive D-Cinema play server's thumbprint, CPL Id corresponding to the KDM and rights usage from content server. It verifies the requested usage rights is available according to the usage rights of the KDM which is stored in its local DB. It also verifies D-Cinema play server is verified one or not with TDL in the TDL database. After that, KDM issue module issues new KDM for the D-Cinema player server .

B. Content Server

Content server receives a request to issue KDM for a specific DCP and send the request to KDM server. The inputs of the request are D-Cinema play server's thumbprint, CPL Id to be issued for the specific KDM and rights usage. Theatre can input D-Cinema play server's thumbprint by choosing the theatre name, CPL Id by movie and rights usage by the period. After that, it can download the KDM file on the web page.

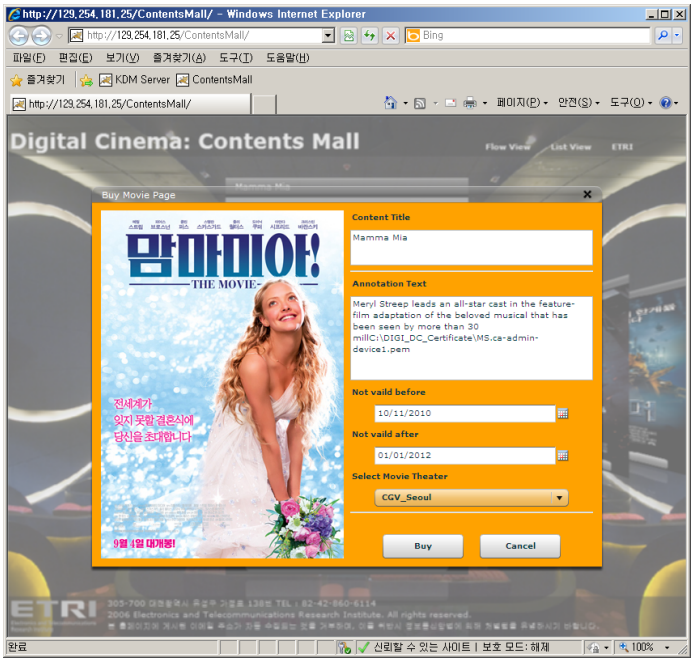
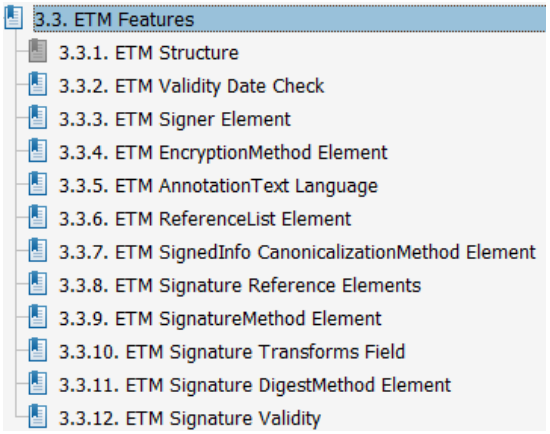


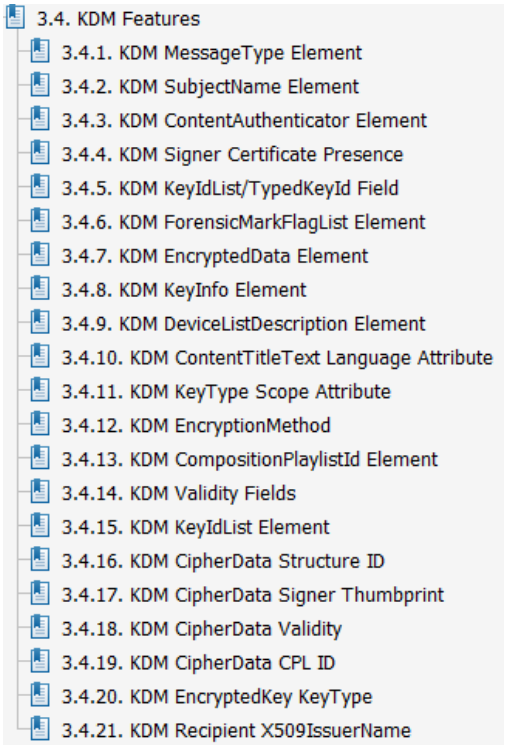
Figure 8. Content server

V. COMPLIANCE TEST

Compliance Test Plan (CTP) was developed by DCI to provide uniform testing procedures for d-cinema equipment[10]. We test KDM which is issued from KDM server according to the CTP. And, we succeeded the test of 12 items of ETM feature and 21 items of KDM feature in the CTP. It ensures the KDM issued to a D-Cinema play server will work properly at a theatre.



(a) ETM Features



(b) KDM features

Figure 9. (a) ETM and (b) KDM feature in CTP

VI. CONCLUSIONS

We implement KDM server and content server to provide KDM service to a D-Cinema play server for a specific digital cinema content. Content server receives a request to issue KDM for a digital cinema content from a D-Cinema play server and request KDM server to issue the corresponding KDM. KDM server manages KDM information of the content and issues KDM to a specific D-Cinema play server by using the information of the KDM and D-Cinema play server. We test 12 items of ETM feature and 21 items of KDM feature in the CTP to ensure KDM compliance.

Proposed KDM system provides how it securely receives the KDM related information from mastering server, how it handles the KDM information in KDM server and content server, and how it issues KDM to D-Cinema play server.

ACKNOWLEDGMENT

This work was supported by the IT R&D program of MCT/KOCCA[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