A DRM System Based on PKI

Lili Zhang ,ZhiYong Zhang, Dan Mei Niu , Sen Shen, Chuan Qi Ye
Electronic Information Engineering College
Henan University of Science and Technology
Luoyang, China
lillyzh@126.com xidianzzy@126.com

Abstract—**A DRM system scheme based on PKI is proposed and designed in this paper, which can achieve secure distribution and use of digital content. The system architecture, secure mechanism, workflow are described. At last the system simulation test and analysis are presented, test and analysis results show that the scheme is feasible and effective.**

Keywords- DRM; PKI; CA ;authentication

I. INTRODUCTION

With the rapid development of internet and digital technology, digital products including digital music, digital TV,E-Book and other various forms are more widely used. These digital products significantly facilitate people's daily use, but they are easily pirated or illegally tempered and used because of their easy to transfer digital contents and characteristics of non-destructive copy. so content providers of digital products, need a technology to protect their digital products away from illegal use. Digital Rights Management (DRM) [1][2]arises to solve the problem [3] [4] [5]. It enables digital products to be used in the permissions granted by digital content provider.

A DRM system based on PKI is designed in this paper, Public Key Infrastructure（PKI）technology[6][7] to solve large-scale open network environment, information security problems is most feasible and most effective measure. It uses the basic theory of public key cryptography for network applications such as authentication, authorization, encryption, decryption, digital signatures and other security services and is a new information security technology and specification. Use of PKI can establish a secure network environment, enabling users to easily use encryption and digital signature technology in a variety of application environments to ensure data confidentiality, integrity, effectiveness and anti-denial.

II. SYSTEM ARCHITECTURE

DRM system architecture designed in this paper is illustrated in Figure1. The System is mainly composed of Certification Authority（CA）, the Server (S) and User Domain (UD), constituting a standard tripartite system of PKI.

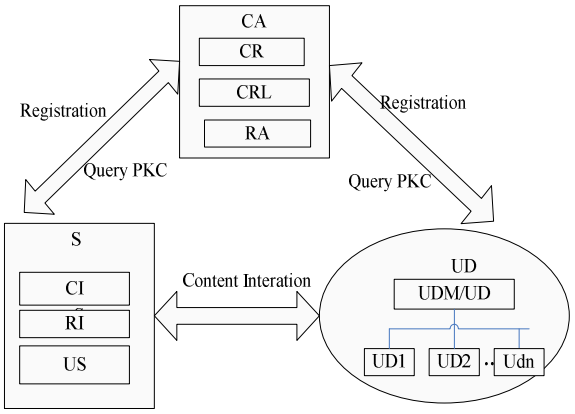

Figure 1 DRM system architecture

A. CA

CA integrates Certificate Repository（CR）,Certificate Revocation list(CRL)and Registration Authority（RA）.As the authority, CA receives and verifies the application information submitted by S and UD, then generates a unique Public Key Certificate (PKC) for the suitable entity, meanwhile backups and issues it. In addition, CA provides the inquiry service of PKC.

B. S

S consists of many servers. S is a provider of digital content and the issuer of corresponding DRM rights, the manager of UD as well. At least S includes the Content Issuer(CI), Right Issuer(RI), User Server（US),CI provides the business of digital content's distribution and download ,RI is responsible for the generation and distribution of rights, US is used to store, update and manage the UD information.

C. UD

UD is composed of equipments owned by the user, meanwhile it accepts the services from S as separate entity. User Device Manager (UDM) is one of the member devices in UD.

III. SYSTEM SECURITY MACHANISM

Authentication mechanism, confidential mechanism, integrity protection mechanism for digital content are described in this part.

978-0-7695-4281-2/10 $26.00 © 2010 IEEE
DOI 10.1109/ICGEC.2010.136

A. *Authentication Mechanism[8]*

DRM system authentication mechanism is based on PKI authentication protocol and implemented via PKC service provided by CA.

Trust model used in this paper is authentication model based on the third-party ,which is that the every party of the communication selects a common trust anchor and they establish two-way trust relationship through the trust anchor。

S and UD confirm each other's identity by mutually verifying CA's digital signature.CA first open its own PKC so that S and UD acquire CA's public key.

when S and UD communicate, they obtain each other's PEK in two ways: one is downloading each one's PKC according to ID information provided by the opposite; the other one is that the opposite directly provides PKC. After obtaining PKC, the verifier verifies the identify of the provider. Firstly it is made sure CRL is up to date before verifying the opposite identity ， if necessary download the latest CRL. P stands for provider ,V stands for verifier, the validation process is shown in figure 2.

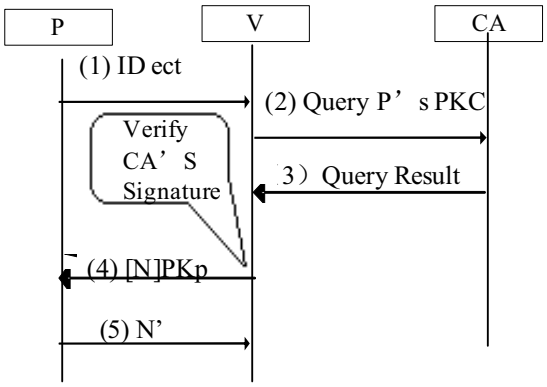

Figure 2 . DRM system authentication process

- P sends ID and other information to V.
- V queries P's PKC from CA by P's ID.
- CA sends query results to V.
- After obtaining the public key PKp ,V encrypts the random number N and send the encrypted content to P.
- After obtaining encrypted content, P decrypts it with its secret key SKp and gets N', and sends N' to V.

B. *Confidential Mechanism for Digital Content*

The confidential mechanism of DRM system is implemented via content encryption key (CEK) generated by S and the public key of UD. S encrypts dates with CEK, while CEK is encapsulated in the right object (RO) and is encrypted with the UD's public key. Thus, only those users with permission of the DRM content can decrypt CEK in RO with their own secret key. The core content of RO includes digital content ID, authorized users' ID, UD information, authorizer's ID, DRM rights (including operating permits, terms of use, range of use, effective date, authority transfer details), RO effective period, CEK encrypted by the user's the public key, S' signature on the RO's Hash value. After obtaining RO, UD must first verify S's signature to ensure RO real and effective.

C. *Integrity Protection Mechanism for Digital Content*

DRM system's integrity protection mechanism for digital content is implemented by message checksum Hash function and digital signature together. S makes signature on RO's hash value with its own secret key and attaches signature dates to the back of RO content .After receiving RO,UD verifies the signature of RO and executes hash operation with the same hashing algorithm, and compares acquired hash value and the signed hash value It is proved .that the content of RO is intact if the same.

IV. SYSTEM WORKFLOW

Workflow system is divided into the following three steps.

A. *Obeject Entity Registration*

It is mainly that S and UD register in CA and receive the PKC service of CA. both registration process is identical. Figure 3 is an example of UD's registration process.

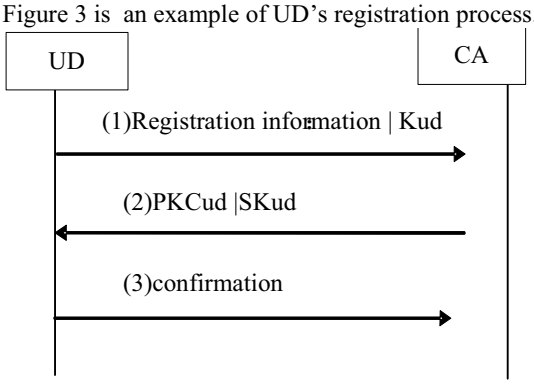

Figure 3 UD registration process

- After obtaining the PKC of CA ,UD first send registration information (the core message is the UD' ID)and registration key Kud to CA. and Kud is symmetric key randomly generated by UD.UD encrypts Kud with the CA's public key PKca and send encrypted datas to CA.
- After receiving the registration information and Kud from UD, CA checksr related information provided by UD. If they meet the condition of the service, CA generates PKC and secret key SKud for UD, and stores them in the Certificate Repository(CR), CA decrypts protected keys with its secret key and gets Kud.CA signs name with its secret key SKca and encrypts it with Kud, and send it to UD with PKCud togethe.
- After receiving PKCud and encrypted SKud, UD decrypts SKud with Kud. UD verifes the CA's signature on PKCud and SKud , then send confirmation message to CA after making sure. Registration process ends.

B. *Query Cerficate*

CA provides public key certificate query service to the outside world, the process is as following: queerer submits a query application (core information is the ID of query object); CA queries in CR and returns query result , If queried Certificate exists and is valid, it is returned. Otherwise "certificate does not exist" or "certificate has been revoked," is returned.

C. S and UD Communicate

S communicates with UD according to the following steps:

- UD obtains S's PKC (query from the CA or S open their own PKC).
- UD sends its own ID information and content of request signed with its secret key,the content is [ID| ContentRequest] SKud .
- After receiving the message from UD, S queries UD'S PKC in CA (UD can also provides PKC). After obtaining UD's PKC, UD and S conduct two-way authentication based on PKC.
- After successful authentication, S verifies the UD's signature on the content request information and makes DRM content and the corresponding RO according to the UD's content request information and purchases conditions of the queried content.
- S can send DRM content to UD, and then send RO to UD after receiving UD's Confirmation and request information for RO. S can also send DRM content and RO together to UD.

V. SYTEM SIMULATION AND IMPLEMENT

DRM system designed in this paper is simulated based on Visual c + + software development platform. DES algorithm is selected as the symmetric cipher algorithm for the realization of the protection key and generation of content encrytion key CEK; RSA algorithm is selected as non-symmetric cipher algorithm for public key certificates service, content key protection, digital signature and verification functions. Simulation system is shown in Figure 4.

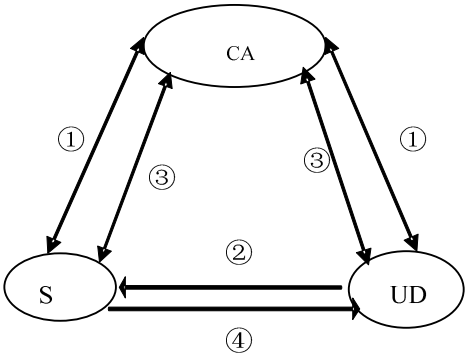

Figure 4 system simulation processes

A. Simulation Process

1) Registration process

UD's registration process is as follows: UD sends registration information to CA; CA conducts the registration business for UD, generates PKC and feedbacks; UD verifies and stores the PKC and the private key.

2) UD applies for digital content from S

UD applies for digital content and provides its ID information.

3) S and UD verify each other's identify

S and UD inquiry and get each other's PKC through CA , makes a certificate validation, completes authentication and protection of the RO (core is protection of content key CEK).

4) UD receives digital content and RO from S

UD receives digital content and RO from S and properly use them.

B. Test Results and Analysis

Several detailed tests are implemented on the running of DRM simulation system, MP3 music file used for the test can reach UD and be decrypted correctly. The decrypted file is identical with the original file. This shows that digital content has no data loss in the process of encryption, decryption and transmission. Digital content is distributed and used properly, achieving the expected goal of the simulation system.

Key Indicators of simulation system are the core algorithm program efficiency and data security under the premise that digital content is distributed and use correctly.

1) Algorithm program efficiency

DES algorithm: the symmetric encryption algorithm used by simulation system is tripleDES algorithm, Tests show the actual encryption speed is about 0.15MB / S and is within an acceptable range of the simulation system.

RSA algorithm: in simulation system key generation, encryption and decryption and signature verification algorithms use RSA algorithm because RSA algorithm is far less than the speed of DES, RSA is mainly used for the signature on public key certificate and the protection of core information on the RO. because of the small amount of encrypted data, the speed is acceptable. In the actual test, the key generation, encryption,decryption , signature and verification all are in 2 seconds or less time-consuming.

2) Important datas security

In this simulation system the core dates such as PKC and responding secret key, digital content, RO, protecting methods and cryptographic algorithms for core dates is shown in table1 . It can clearly be seen that related core data have been protected well , RSA and DES algorithms are currently the most widely used algorithm and their security has been proved in practice long ago.

TABLE I. PROTECTING METHODS AND CRYPTOGRAPHIC ALGORITHMS FOR IMPORTANT DATES

Inportant Dates	Protection Modes	Cryptography Algorithms
PKC	Digital Signature	RSA
Secret Key	Encryption	Triple DES
Digital Content	Encryption	Triple DES
RO	Digital Signature Encryption	RSA

VI. CONCLUTION

The test results show that DRM systems designed in this paper is feasible and effective, in addition, the prevalence of PKI technology, makes this scheme also have a good security mechanism for the universal.

ACKNOWLEDGEMENTS

The work was sponsored by National Natural Science Foundation of China Grant No.61003234 & No.60803150, China Postdoctoral Science Foundation Grant No.20100471611, Henan Province Key Technologies R & D Program Grant No.092102210295, and Henan University of Science & Technology Young Scholar Fund Grant No.2008QN010.

REFERENCES

[1] Zhiyong Zhang, Qingqi Pei, Jianfeng Ma, Lin Yang, "Establishing Multi-Party Trust Architecture for DRM by Using Game-Theoretic Analysis of Security Policies," Chinese Journal of Electronics, 2009, 18(3):pp. 519-524.

[2] Zhiyong Zhang, Qingqi Pei, Jianfeng Ma, Lin Yang, "Security and Trust in Digital Rights Management: A Survey," International Journal of Network Security, Vol.9, No.3, 2009, pp. 247-263.

[3] INDICARE, "Consumer Survey on Digital Music and DRM," http://www.indicare.org, May 2005.

[4]OMA (Open Mobile Alliance) 2.0, http://www.openmo-bilealliance.org, September 2007.

[5] Younggyo Lee Jeonghee Ahn, Seungjoo Kim Dongho Won, A PKI System for Detecting the Exposure of a User's Secret Key, Public Key Infrastructure, Springer Berlin / HeidelbergVolume 4043,pp.248-250,June 2006.

[6] Jae-Pyo Park, Hong-jin Kim, Keun-Wang Lee, and Keun-Soo Lee Based Digital Rights Management System for Safe Playback Lecture Notes in Computer Science Springer Berlin / Heidelberg,Volume 3645, pp.801-810, September 2005.

[7] Yun-kyung Lee,Hong-il Ju Jee-hye,User authentication mechanism using authentication server in homnetwork Advanced Communication Technology, 2006. ICACT 2006. The 8th International Conference Phoenix Park, pp.504-506,August 2006.

[8]Fumiaki Sato,Hirohisa Takahira, Tadanori Mizuno, Message authentication scheme for mobile ad hoc networks, Parallel and Distributed Systems, 2005. Proceedings. 11th International Conference on vol.1, IEEEComputer Society Washington, DC, USA ,pp.50-56,Janury 2005.